CAPÍTULO IV

MAPEO DE LAS TÉCNICAS DE APRENDIZAJE AUTOMÁTICO USADOS EN FRAUDES CON TARJETA DE CRÉDITO

Fernando Gutiérrez-Portela

Estudiante Doctorado en Ingeniería de la Universidad Autónoma de Bucaramanga. Magíster en Software Libre, Profesor de la facultad de Ingeniería de la Universidad Cooperativa de Colombia Sede Ibagué-Espinal. Integrante del Grupo de Investigación AQUA de la UCC Ibagué-Espinal. Correo: fernando.gutierrez@campusucc.edu.co. Orcid <https://orcid.org/0000-0003-3722-3809>

César Augusto Perdomo-Guerrero

Magíster en Administración. Especialista en dirección financiera y desarrollo organizacional. Administrador de empresas. Profesor de planta del programa de administración de empresas de la Universidad SURCOLOMBIANA. Correo: cesarineiva@hotmail.com.

Mario Heimer Flórez-Guzmán

Doctor en Educación con mención en Gestión de Instituciones Educativas. Profesor investigador de la Corporación Universitaria Remington. Correo: mario.florez@uniremington.edu.co. Orcid: <https://orcid.org/0000-0002-8468-4168>

Ludivia Hernández-Aros

Magíster en Auditoría Internacional. Profesora investigadora de la Facultad de Contaduría Pública de la Universidad Cooperativa de Colombia sede Ibagué-Espinal. Correo: ludivia.hernandez@campusucc.edu.co. Orcid: <https://orcid.org/0000-0002-1571-3439>

Diana Brigitte Quiceno-Castañeda

Estudiante de octavo semestre de Contaduría pública de la Universidad Cooperativa de Colombia Sede Ibagué-Espinal. Correo: diana.quicenoc@campusucc.edu.co. Orcid: <https://orcid.org/0000-0003-0959-4426>

Resumen

El fraude es un acto delictivo que es aprovechado por personas que ven la oportunidad de realizarlo y lo ejecutan, especialmente, en contra de las finanzas de personas naturales o jurídicas. En el caso de las tarjetas de crédito, el fraude está presente en un alto porcentaje de organizaciones financieras y las pérdidas representan alrededor del 5% de los ingresos por

año. Su temprana detección o, en su defecto, identificación en tiempo real, es una necesidad apremiante y exige soluciones eficaces que conserven el prestigio y confiabilidad esperadas por los clientes. Con base en lo expuesto, el presente capítulo de investigación analiza las técnicas de aprendizaje automático usados en fraudes con tarjeta de crédito.

Metodológicamente, es un estudio descriptivo-explicativo de carácter cualitativo, abordando las técnicas que comúnmente se utilizan en los procesos de Aprendizaje Automático en la tipología de fraude en tarjetas de crédito. El resultado del estudio, reflejó el sinnúmero de investigaciones que se han realizado sobre el tema, abarcando grandes avances desde el 2002; así mismo, se observó que algoritmos de aprendizaje como redes neuronales, regresión logística y árboles de decisión, han contribuido a dar solución efectiva frente a la detección oportuna a un fraude con tarjeta de crédito.

Palabras clave: Aprendizaje automático, fraude con tarjeta de crédito, técnicas no supervisadas, técnicas supervisadas.

Abstract

Fraud is a criminal act, which is taken advantage of by people who see the opportunity to do it and execute these facts against the finances of the companies. This crime is present in almost all organizations and losses represent around 5% of income per year, its early detection or failing in real time is a pressing need and requires effective solutions that preserve prestige and reliability for customers. Therefore, this study analyzes the machine learning techniques used in credit card fraud. Methodologically, it is a qualitative descriptive-explanatory study, addressing the techniques commonly used in the Automatic Learning processes in the typology of credit card fraud. The result of this research reflects that there are many investigations that have been carried out on the subject, covering great advances since 2002. It is observed that learning algorithms such as neural networks, logistic regression and decision trees have contributed to give effective solution to the Timely detection of even credit card fraud.

Keywords: credit card fraud, machine learning, unsupervised techniques, supervised techniques.

Estudio derivado de proyecto de investigación «Diseño de estrategias que inciden en los mecanismos de recolección de pruebas en una auditoría forense que propendan por mitigar el riesgo en las organizaciones», asociado al grupo PLANAUDI, AQUA, CACE, adscrito al Centro de Investigaciones del programa de Contaduría Pública de la Universidad Cooperativa de Colombia, sede Ibagué y Cali, y al grupo de investigación Mundo Organizacional de la Corporación Universitaria Remington, «Aplicación de técnicas de aprendizaje automático para la detección de intrusiones en las redes de sensores inalámbricas empleadas en la movilidad inteligente urbana», adscrito al centro de investigaciones del programa de Ingeniería Civil de la Universidad Cooperativa de Colombia, sede Ibagué y de la Universidad SURCOLOMBIANA de Neiva, Huila, Colombia.

Introducción

El fraude, de acuerdo con Crespo (2009), está ocasionado por un individuo que pretende lograr una ventaja deshonesta. Para Ñaupas (2016), el fraude que se realiza de manera electrónica se conoce como el uso indebido de los elementos informáticos que, a través de las redes de sistemas, se manipulan para obtener beneficios económicos ilícitos. Así mismo, Hassan *et al.* (2018), plantean que es importante utilizar herramientas tecnológicas orientadas al control de las operaciones realizadas por las personas y las organizaciones, a fin de mejorar el nivel de confianza y transparencia en las mismas.

En tal sentido, cabe destacar, que la revolución tecnológica ha incrementado la inseguridad al momento de efectuar transacciones electrónicas y, para contenerlo, se implementan sistemas que logren detectar el fraude con tarjeta de crédito para minimizar las pérdidas económicas, tanto para las entidades financieras como para los usuarios. Las técnicas más modernas en inteligencia artificial, seguridad criptográfica, reconocimiento facial, evolucionan para resolver justamente el problema del fraude en tarjetas de crédito (Porto, 2015). El fraude con tarjeta de crédito es aquel uso no autorizado de la tarjeta, para que se realicen compras o retiros de efectivo, que son cargadas a la víctima en su cuenta, considerándose como una de las modalidades de robo de identidad más usadas por hackers (Legal Information Institute, 2018).

En la actualidad, el Aprendizaje Automático (Machine Learning, ML) es una disciplina de la inteligencia artificial que hace posible que las computadoras funcionen sin necesidad de ser programadas, con la facilidad de algoritmos que analizan y procesan los datos para toma de decisiones y/o realizan una predicción sobre un problema real sin ser programados por un humano (González, 2010). Así, en razón a su función, el Aprendizaje Automático ayuda a minimizar los fraudes de tarjetas de crédito que amenazan la seguridad de los datos y, como consecuencia, afectan económicamente a un tercero, que para este estudio es la entidad financiera o el cliente.

Adicionalmente, el Aprendizaje Automático ofrece a los encargados de instaurar los sistemas seguridad en las compañías, técnicas de aprendizaje automático para analizar anomalías en el uso de las tarjetas de crédito que, en su mayoría, conducen a situaciones de riesgos para el usuario. En este contexto, estas técnicas cuentan inicialmente con una base de datos de usuarios genuinos y de usuarios fraudulentos con el objetivo de alimentar la herramienta para que esta pueda clasificar la información y modelar de acuerdo con los patrones y reglas que se hayan determinado y, con ello, establecer en tiempo real si la transacción que se está llevando a cabo es una operación limpia.

Con base en lo expresado, la investigación se compone del análisis del Aprendizaje Automático y sus técnicas supervisadas y no supervisadas, realizando un mapeo de las características de cada una de ellas y su aplicación para la detección de anomalías y prevenir un posible fraude en tarjeta de crédito. La razón que motiva el citado estudio, es dar a conocer las técnicas de Aprendizaje Automático que se han utilizado en la detección de fraudes financieros en tarjetas de crédito, situación que ha representado grandes pérdidas económicas en el sector financiero.

Marco referencial

El Aprendizaje Automático y sus técnicas

El uso del Aprendizaje Automático (Machine Learnig, ML) prepara y crea información mediante el conocimiento y análisis de características o identificación de patrones a partir de un sinnúmero de datos (Prajapati y Jain, 2018; Kumar *et al.*, 2019). Se conocen tres categorías en las que se dividen los algoritmos de ML: 1) Aprendizaje supervisado, 2) No supervisado y, por último, 3) Por refuerzo. A continuación, se detallan:

1. Aprendizaje supervisado

El Aprendizaje Supervisado (Supervised Learning, en inglés), se forma cuando un algoritmo aprende a partir de un conjunto de datos de entrenamiento que consisten en valores numéricos o datos categóricos etiquetados como clases que permiten clasificar o predecir un resultado; para ello, se utiliza otro conjunto de datos de validación y prueba. Esta técnica, se relaciona con el aprendizaje humano que, bajo la enseñanza o entrenamiento de buen instructor, se entregan los mejores casos para que el estudiante los asimile; seguidamente, el aprendiz relaciona mediante estructuras mentales los conocimientos adquiridos y aprende. Cuando el aprendiz recibe nuevos casos, aplica los conocimientos anteriores y genera un resultado acorde con el problema.

El Aprendizaje Supervisado, a su vez, se compone de dos clases de algoritmos, unos de clasificación para valores de respuesta categóricos en los que los datos se pueden separar en “clases” específicas y otros de regresión los cuales generan una respuesta con valores de respuesta continua (Prajapati y Jain, 2018; Kumar *et al.*, 2019; MarthiWorks, s.f). según afirman Mittal y Tyagi (2019), se conocen varios algoritmos de aprendizaje supervisado desde los clásicos hasta los recientes, los cuales incluyen algoritmos basados en árboles, enfoques bayesianos, redes neuronales de aprendizaje clásico y profundo, y algoritmos híbridos.

Algunos de estos algoritmos que permiten detectar situaciones anómalas y que se han usado en diferentes investigaciones, se analizan a continuación:

- a. **Regresión logística:** algoritmo de clasificación que encuentra el mejor parámetro de ajuste para estimar la probabilidad de la respuesta binaria en función de una o más características. En la regresión logística, la variable dependiente es una variable binaria que contiene datos codificados como 1-0, sí-no, abierto-cerrado. Dicha regresión, se usa para estimar la probabilidad de una respuesta binaria basada en uno o más predictores o variables independientes (características); emplea, además, la función sigmoide para asignar valores pronosticados a probabilidades. La razón por la cual la regresión logística es muy utilizada, a pesar de los algoritmos avanzados como las nuevas redes neuronales, se debe a la eficiencia y el bajo requerimiento computacional para su ejecución (Mittal y Tyagi, 2019; González, 2020; Awoyemi, *et al.*, 2017; Dighe, *et al.*, 2018).
- b. **Vecinos K-Vecinos más cercanos:** algoritmo de clasificación K-Nearest Neighbour (KNN). Son métodos de aprendizaje supervisados basados en instancias que clasifican según una medida de similitud como las funciones de distancia

Euclidiana, Manhattan o Minkowski. Dado que el conjunto de datos de la tarjeta de crédito contiene variables continuas, se utiliza la medida de distancia euclidiana. Es un clasificador sólido, usado como punto de referencia para clasificadores más complejos como las redes neuronales artificiales y vectores de soporte, utilizado en diferentes aplicaciones como pronósticos económicos, fraude financiero, genética, entre otros (Awoyemi *et al.*, 2017; González, 2020; Dighe *et al.*, 2018).

- c. **Naïve Bayes:** algoritmo de clasificación con enfoque estadístico basado en la teoría bayesiana, que elige la decisión en función de la probabilidad más alta. La probabilidad bayesiana estima probabilidades desconocidas a partir de valores conocidos. También, permite que se apliquen conocimientos y lógica previos a declaraciones inciertas. Esta técnica, supone una independencia condicional entre las características de los datos. El clasificador Naïve Bayes, se basa en las probabilidades condicionales que se pueden obtener usando la fórmula de Bayes y el resultado es, generalmente, categórico: fraude y no fraude (Mittal y Tyagi, 2019; Awoyemi *et al.*, 2017; Dighe *et al.*, 2018).
- d. **Máquinas de Vectores de Soporte:** algoritmo de clasificación discriminatorio definido formalmente por un hiperplano de separación. En otras palabras, suministrados los datos de entrenamiento etiquetados, el algoritmo genera un hiperplano óptimo que clasifica los nuevos ejemplos en dos espacios dimensionales; este hiperplano, es una línea que divide un plano en dos partes donde cada clase se encuentra en cada lado. De otra parte, los datos se clasifican y analizan linealmente (Mittal y Tyagi, 2019; González, 2020; Mohamad, 2018).
- e. **Árbol de Decisión:** algoritmo para problemas de clasificación, hace referencia a un conjunto de condiciones organizadas con estructura jerárquica para que la decisión se ajuste al cumplimiento de las condiciones desde la raíz hasta sus hojas. Este algoritmo se aplica cuando se requiere detectar las reglas del negocio para ser traducidas al lenguaje neuronal para la construcción de modelos predictivos. A diferencia de los modelos lineales, mapean bastante bien las relaciones no lineales (González, 2020; Dighe *et al.*, 2018; Apapan, 2018).
- f. **Bosque aleatorio:** algoritmo de clasificación que se compone de muchos árboles de decisión. Es muy efectivo cuando hay un mayor número de árboles en el bosque, esto evita que el modelo se sobreajuste. Cada árbol de decisión en el bosque genera algunos resultados, estos resultados, se fusionan para obtener una predicción más precisa y estable (Mittal y Tyagi, 2019; González, 2020; Varmedja *et al.*, 2019).

2. Aprendizaje no supervisado

Las técnicas no supervisadas agrupan registros de datos similares que pertenecen a la misma clase. Son útiles para detección de valores atípicos, registros que no pertenecen a ninguno de los grupos. Por tal motivo, estas técnicas, en el caso particular de fraudes financieros, son muy pocas, situación que se podría ver como una oportunidad de estudios futuros. El aprendizaje no supervisado, realiza inferencias a partir de conjuntos de datos de entrada sin etiquetar. Los algoritmos utilizados, tienen la finalidad de encontrar patrones anómalos o características peculiares en los datos mediante técnicas como el clustering, con la particularidad de agrupar y reagrupar los objetos de un conjunto de

datos de acuerdo con su similitud; proceso de agrupación acorde con la dinámica de cada algoritmo utilizado, con el uso de diferentes reglas para definir la semejanza de los elementos del conjunto de datos (Bangotra *et al.*, 2018; Prajapati y Jain, 2018; Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013).

Por su parte, Apapan (2018) explica que el aprendizaje no supervisado es aquel que toma la información de nuevas transacciones para detectar comportamientos anómalos. Este modelo, estructura la distribución de datos para aprender más sobre ellos, es un modelo subjetivo debido a que no tiene respuestas precisas. Sirve para agrupar los datos en algoritmos de agrupamiento y algoritmos de asociación (Gonzalo, 2018).

Algunos métodos de detección no supervisada que se exploraran en este estudio son K-means o K-Medias, agrupamiento jerárquico, DBSCAN, propagación de afinidad, los mapas auto-organizados, el bosque de aislamiento y el factor de valor atípico local. Véanse a continuación:

- a. **K-means o K-Medias:** agrupa los datos al tratar de separar muestras en n grupos de igual varianza, minimizando un criterio conocido como la inercia o la suma de cuadrados dentro del grupo. Este algoritmo, requiere que se especifique el número de clústeres y se utiliza cuando se adquieren datos no etiquetados, sin categorías o grupos definidos con el fin de elegir centroides que minimicen la inercia o el criterio de suma de cuadrados dentro del clúster. Son bastante útiles para aplicaciones que requieren identificar valores atípicos en operaciones financieras (Mittal y Tyagi, 2019; González, 2020; Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013).
- b. **Agrupamiento Jerárquico:** es un algoritmo que crean agrupaciones anidadas concentrando o fraccionando sucesivamente. La jerarquía de grupos se constituye como un árbol o dendrograma. La raíz del árbol, es el grupo único que reúne todas las muestras, siendo las hojas los grupos con una sola muestra. En la agrupación jerárquica, los datos no se dividen en un clúster en particular en un solo paso, lo que sucede es que se dan una serie de divisiones que pueden producirse desde un único clúster el cual contiene todos los objetos hasta n clusters grupos (González, 2020; Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013).

Adicionalmente, la agrupación jerárquica se subdivide en métodos aglomerativos, los cuales realizan una agrupación jerárquica utilizando un enfoque ascendente: cada observación comienza en su propio grupo y los grupos se fusionan sucesivamente. Los criterios de vinculación determinan la métrica utilizada para la estrategia de fusión: 1) Ward: minimiza la suma de las diferencias al cuadrado dentro de todos los grupos utilizando un enfoque que minimiza la varianza y, en este sentido, es similar a la función objetivo k-means pero se aborda con un enfoque jerárquico aglomerativo; 2) La vinculación máxima o completa: minimiza la distancia máxima entre observaciones de pares de grupos; 3) El enlace promedio: minimiza el promedio de las distancias entre todas las observaciones de pares de grupos; y, c) El enlace único: minimiza la distancia entre las observaciones más cercanas de pares de grupos (González, 2020; Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013).

- c. **DBSCAN:** algoritmo determinista que toma los grupos como áreas de alta densidad separadas por áreas de baja densidad. El enfoque en este método, es crear grupos con un tamaño y densidad mínimos. Debido a esta visión bastante genérica, los

grupos encontrados por DBSCAN pueden tener cualquier forma a diferencia de k-means que supone que los grupos tienen forma convexa (Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013; Vats *et al.*, 2018).

- d. **Propagación de afinidad:** algoritmo que crea grupos enviando mensajes entre pares de muestras hasta converger. El algoritmo aglomerativo, logra la función de integrar la partición de datos con un nuevo agrupamiento jerárquico aglomerativo. Esta actualización, ocurre hasta lograr la convergencia, en cuyo punto, se eligen los ejemplos finales y, por lo tanto, se proporciona la agrupación final (Vats *et al.*, 2018; Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013).

3. Aprendizaje por refuerzo

La tercera técnica de ML es el Aprendizaje por refuerzo que contextualiza todos los algoritmos inteligentes, los cuales aprenden observando la realidad a su alrededor. Sus entradas la obtienen de la retroalimentación obtenida de su contexto gracias a sus acciones, en este caso, los sistemas se entrenan y aprenden con pruebas de ensayo-error (Kumar *et al.*, 2019).

Metodología

La investigación es descriptiva-explicativa, puesto que como lo plantea Sampieri (2018) busca entender el contexto, las propiedades, características de un fenómeno; de igual forma es cualitativo porque permite realizar el análisis temático sobre la información que reposa en los artículos científicos y libros del estudio. Así mismo, se considera que es de tipo documental porque la fuente de información principal está alojada en documentos físicos y digitales permitiendo, de esta manera, indagar sobre las técnicas supervisadas y no supervisadas usadas para el análisis de datos con sus algoritmos y los resultados obtenidos. En este contexto, al identificar las técnicas de ML, usadas para la detección de los fraudes en tarjetas de crédito se indaga sobre la aplicación de la inteligencia artificial, para la solución de una problemática social que afecta a la gran parte de las personas y organizaciones; más aún, cuando las transacciones se hacen en su mayoría a través de medios electrónicos.

Resultados

Fraude con tarjeta de crédito

Una tarjeta de crédito son pequeñas tarjetas de plástico (de forma rectangular) generadas por una institución financiera a un usuario, el cual la obtiene para el beneficio de compra de bienes y servicios o avances en efectivo; tales compras, entendidas como transacciones, actualmente se pueden realizar de manera presencial o virtual (Mittal y Tyagi 2019).

El fraude con tarjeta de crédito se clasifica en dos categorías:

1. Fraudes causados por obtener ilegalmente la posesión de una tarjeta física. Esto no solo se puede hacer robando la tarjeta al propietario real, antes o después de la entrega; también, por otros métodos en los que se crea una nueva tarjeta, conocida como clonada, que puede actuar como una falsificación para la tarjeta real.
2. Fraude por obtención ilegal de información de tarjetas de crédito, situación que es bastante común cuando se entrega la tarjeta en un sitio de compra (surfing, phishing) (Mittal y Tyagi 2019).

Otros autores como Awoyemi *et al.* (2017), describen que las clasificaciones de este tipo de fraude son más amplias como fraude con tarjeta interna y fraude externo, o fraudes tradicionales relacionados con tarjetas (solicitud, robo, toma de una cuenta y falsificación), fraudes relacionados con comerciantes (colusión y triangulación de comerciantes) y fraudes por Internet (clonación de sitios, generadores de tarjetas de crédito y sitios falsos de comerciantes). entre otros; situación, que para el año 2014 generaron significativas pérdidas financieras por este delito, pues se analiza que por cada USD 100 se está perdiendo USD 5.6 centavos de dólar por esta modalidad.

Cabe anotar, que los estafadores estudian nuevas formas de imitar el comportamiento del uso de la tarjeta legítima, siendo altamente dinámicas para realizar este hecho fraudulento (Awoyemi *et al.*, 2017); para ello, según Mittal y Tyagi (2019), estudios a través de una detección temprana, diseñan un sistema de detección de fraude computacional (FDS), el cual analiza la información que recibe de la tarjeta y determina si es el usuario real o es un estafador el que está realizando un movimiento. Señalan los autores, además, un FDS es aquel que aprende del comportamiento de uso de la tarjeta de usuario donde se identifican transacciones normales y las de fraude. Es así, como se utiliza el Aprendizaje Automático -supervisado y no supervisado- para ser aplicado al conjunto de datos.

Para combinar técnicas avanzadas de Aprendizaje Automático, que identifiquen y respondan a los ataques, los modelos estáticos son efectivos, pues logran identificar patrones históricos de fraude. Los de autoaprendizaje, incluyen los nuevos datos de las transacciones con el fin de reconocer y adaptarse a la evolución de los fraudes que reflejan las últimas tendencias, a fin de enfocar los esfuerzos y garantizar la autenticidad de las órdenes de los clientes a través de la red (CyberSource, 2019).

En este sentido, algunas empresas han incursionado, como estrategia de prevención, en la aplicación de las técnicas de Aprendizaje Automático (Machine Learning -ML-) para detectar, de manera predictiva, el fraude y ayudar al trabajo del Auditor. Estas herramientas, pueden proporcionar al profesional mayor información para su análisis y, al mismo tiempo, contribuir a mejorar el uso del tiempo; asimismo, lleva a cabo procesos que agilicen la detección de fraudes, incluso, anticiparse a los mismos con el uso de la Inteligencia Artificial -IA-, como un gran aliado para el trabajo del auditor (Auditól, 2019).

Estas técnicas de reconocimientos de patrones predictivos, identificarían la tendencia hacia el fraude financiero, entregarían el significado de los datos sobre actividades sospechosas que no son fáciles de detectar por el ser humano, lo que implicaría el uso

acertado de algoritmos que establezcan las alertas tempranas, permitiendo ahorrar tiempo en la revisión, reducir la cantidad falsos positivos y lograr detener la acción de fraude oportunamente (Cisco Systems, 2018).

Pertinente señalar, el uso de estas técnicas de Aprendizaje Automático exige que exista con anterioridad una muestra clasificada de datos para que estas técnicas puedan aprender o modelar de manera similar; por ejemplo, para la detección de fraude con tarjeta de crédito, el clasificador de Aprendizaje Automático intentará etiquetar las transacciones que probablemente sean fraudulentas en función de un conjunto de casos de fraude conocidos. Es por ello, que la categorización es vital en la predicción y ésta debe ser organizada en clases y atributos que definan su pertenencia considerándose, así, todas las diferencias relevantes, derivadas de combinaciones de atributos o variables (Mackenzie, 2015).

Por su parte, en cuanto a las entidades financieras, estas requieren reconocer transacciones inusuales para la detección de valores atípicos -anormales o inusuales- que pueden generarse por un usuario o cliente, o que en ocasiones son generadas por personas delictivas que toman los datos de la tarjeta de crédito y realizan transacciones fraudulentas que afectan a la entidad financiera o al cliente. Sin embargo, en el caso de la detección de valores atípicos, se dificulta el reconocer estas problemáticas ya que no se cuenta con un conjunto de datos limpio que represente la población de observaciones regulares que se pueden utilizar para entrenar cualquier herramienta (Pedregosa *et al.*, 2011; Buitinck *et al.*, 2013).

Cisco Systems¹ (2018), reveló que el 96% de las redes corporativas del mundo – según una muestra de 30 de las más significativas–, generaron tráfico hacia sitios web con malware donde sus servidores fueron “secuestrados”. En tanto que, el informe de CyberSource² (2019) indica los 10 tipos de ataques con mayor frecuencia de fraude, entre ellos: robo de identidad 42%; phishing –pharming– waling 45%; robo de cuenta 37%; prueba de tarjeta 36%; fraude amigable 36%; fraude de asociados 33%; uso abusivo de cupón-descuento-reembolso, botnes, reenvío 23%; fraude en programas de fidelización 23%. De acuerdo con las cifras, el tercer lugar lo ocupa el robo de cuenta, lo que muestra la tendencia creciente de los consumidores en almacenar datos de sus tarjetas de pagos en las tiendas online.

A continuación en la tabla 1, se presentan los Algoritmos de Aprendizaje Automático que se han empleado para la detección de fraudes financieros:

¹ Cisco Systems es una empresa global con sede en San José, California, Estados Unidos. Está dedicada, principalmente a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

² **CyberSource, compañía de Visa, es el sistema de detección de fraude en tiempo real en el mundo**, el cual permite a los comercios en línea localizar el fraude más rápidamente, con mayor precisión y menos intervención manual.

Tabla 1

Algoritmos de Aprendizaje Automático que se han usado para la detección de fraudes financieros.

Autores / año	Algoritmos usados en la detección de fraude con tarjetas de crédito	Resultados encontrados por los autores
S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick (2002)	Redes bayesianas y neuronales.	La red bayesiana funciona mejor que la red neuronal en la detección de fraudes con tarjetas de crédito.
Y. Kou, C-T. Lu, S. Sinvongwattana, Y-P. Huang (2004)	Árboles de decisión y máquinas de soporte vectorial (SVM).	Los clasificadores propuestos de los enfoques de árbol de decisión superan a los enfoques SVM en la solución del problema bajo investigación.
A. Shen, R. Tong, Y. Deng (2007)	Árbol de decisión, redes neuronales y regresión logística.	El clasificador propuesto de redes neuronales y enfoques de regresión logística, superan el árbol de decisión en la solución del problema bajo investigación.
S. Bhattacharyya, S. Jha, K. Tharakunnel, J. C. Westland (2011)	Regresión logística junto con dos enfoques avanzados de minería de datos, máquinas de soporte vectorial y bosques aleatorios.	La regresión logística muestra un rendimiento apreciable, a menudo, superando el de los modelos SVM con diferentes núcleos.
Y. Sahin, E. Duman (2011)	Redes Neuronales Artificiales (ANN) y Regresión Logística (LR), se desarrollan y aplican al problema de detección de fraude de tarjetas de crédito	Los resultados muestran que los clasificadores ANN propuestos, superan a los clasificadores LR en la resolución del problema bajo investigación.
K. K. Sherly (2012)	Árbol de decisión, red neuronal y clasificadores ingenuos de bayes.	Se informa que los clasificadores de redes neuronales son adecuados solo para bases de datos más grandes y requieren mucho tiempo para entrenar el modelo. Los clasificadores bayesianos, son más precisos y mucho más rápidos de entrenar y adecuados para diferentes tamaños de datos, pero son más lentos cuando se aplican a nuevas instancias.
J. Pun, Y. Lawryshyn (2012)	Árbol de decisión, los Bayesianos ingenuos y los algoritmos vecinos más cercanos.	Usando el algoritmo Bayesiano ingenuo como el algoritmo de meta-nivel para combinar las predicciones del clasificador base, el resultado muestra una mejora del rendimiento del 28%.
T. R. Patil, S. S. Shrekar (2013)	Naïve Bayes y el árbol de decisión	Los resultados muestran que la eficiencia y precisión de J48 es mejor que la de Naïve Bayes.

Fuente: adaptado de Awoyemi *et al.* (2017).

Se observa, según la tabla que, a raíz del uso masivo de las tarjetas de crédito, desde los investigadores, han usado diversas técnicas supervisadas y no supervisadas, para afrontar este tipo de fraude; en este sentido, estudios argumentan que con frecuencia las entidades financieras aplican técnicas para la detección de fraudes puesto que el uso de tarjetas de crédito se ha vuelto común (Buonaguidi, 2017). De acuerdo con el reporte de Nilson Report³, referente a los fraudes por tarjetas en el año 2015, la cifra llegó a los US \$21.000 millones y se espera que para el 2020 la cifra llegue a los US \$31.000 millones. Entre los tipos de fraude con tarjeta, se destacan dos categorías “fraude de tarjeta no presente” y “fraude con tarjeta presente”.

Conclusiones

Las técnicas de Aprendizaje Automático cada día van tomando mayor importancia en el manejo de transacciones con tarjeta de crédito, especialmente, por su efectividad para detectar o anticiparse a los fraudes, ayudando a las compañías en disminuir pérdidas económicas y, a su vez, a los usuarios de las tarjetas de crédito quienes se sienten seguros por las medidas tomadas en la detección temprana de un acto fraudulento.

De acuerdo con el análisis de la información obtenida sobre la aplicación de las diferentes técnicas de Aprendizaje Automático (Machine Learnig, ML) en la detección de fraude con tarjeta de crédito, se puede determinar que los algoritmos no supervisados arrojan mejores resultados y mayor efectividad en tiempo real al momento de establecer si una transacción es fraudulenta, puesto que tienen la capacidad de separar datos sin etiquetas, agruparlos por similitud y autoaprender en la medida en que se presentan las ciberamenazas por fraude financiero en los sistemas informáticos de las organizaciones.

Por último, son diversas las investigaciones que se vienen adelantando desde el año 2002. Se observa, una ostensible preocupación por detener el fraude en las tarjetas de crédito, más aún, cuando su uso es masivo, observándose que los autores de estas investigaciones son de India, China y Estados Unidos. Se deja abierto para futuras investigaciones, el explorar con algoritmos de aprendizaje reforzado y el aprendizaje profundo.

Referencias bibliográficas

- Apapan Pumsirirat, L. Y. (2018). *Detección de fraude de tarjetas de crédito mediante aprendizaje profundo basado en codificador automático y máquina Boltzmann restringida*. (IJACSA) Revista Internacional de Informática Avanzada y Aplicaciones, 9, 1, 18-. doi:10.14569 / IJACSA.2018.090103
- Auditól. (10 de 05 de 2019). *Inteligencia artificial, un gran aliado para el trabajo del auditor*. Obtenido de <https://www.incp.org.co/inteligencia-artificial-gran-aliado-trabajo-del-auditor/>

³ The Nilson Report es la fuente de noticias y análisis sobre la industria de las tarjetas internacionales y de pagos con dispositivos móviles más relevante y respetada. Esta empresa entrega un boletín informativo con estadísticas propias sobre marcas, emisores, compradores y proveedores.

- Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis,. International Conference on Computing Networking and Informatics (ICCNi), 1-9.
- Bangotra, D., Singh, Y., & Selwal, A. (2018). Machine Learning in Wireless Sensor Networks: Challenges and Opportunities. 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 534-539. doi:10.1109/PDGC.2018.8745845
- Buitinck, L., Louppe, G., Blondel, M., Pedregosa, F., Mueller, A., Grisel, O., . . . Holt, B. (2013). design for machine learning software: experiences from the scikit-learn. 108--122. Obtenido de <https://scikit-learn.org/stable/about.html#citing-scikit-learn>
- Cisco Systems. (2018). Reporte anual de ciberseguridad 2018. Cisco systems. San Jose , California: Cisco Systems..
- Crespo, J. A. M. (2009). Detección del fraude en una auditoría de estados financieros. Perspectivas, (24), 227-242. Disponible en: <https://www.redalyc.org/pdf/4259/425942160012.pdf>
- CyberSource. (2019). Lo que se necesita para ser líder en prevención de fraude Reporte global de fraude en eCommerce 2019. Foster city - USA: Cyber Source
- Dighe, D., Patil, S., y Kokate, S. (2018). Detection of Credit Card Fraud Transactions Using Machine Learning Algorithms and Neural Networks: A Comparative Study,” P. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-6.
- González, L. (2020). <https://ligdigonzalez.com/>. (Ligdi González) Recuperado el 02 de 02 de 2020, de <https://ligdigonzalez.com/curso-gratis-introduccion-a-machine-learning/>
- Gonzalo, Á. (26 de mayo de 2018). Machine Learning, Data Science Y Analítica Avanzada. Obtenido De Machine Learning, Data Science Y Analítica Avanzada: <http://machinelearningparatodos.com/tipos-de-aprendizaje-automatico/>
- Hassan, J. C., M. G., Sanchez, N. S., Aros, L. H., Guzman, M. F., Cossio, L. G., . . . N. L. (2018). *Visiones de la Contabilidad en el siglo XXI*, Manifestaciones de las prácticas de aseguramiento financiero, a partir de estudios de caso emblemáticos en Colombia (Vol. 1). (R. P. Estepa, Ed.) Bogotá, Bogotá D.E., Colombia: Ediciones Nueva Jurídica.
- Kumar, D. P., Amgoth, T., & Annavarapu, C. S. (2019). Machine learning algorithms for wireless sensor networks: A survey. . Information Fusion, 1-25.
- Legal Information Institute (2018). *Fraude con Tarjeta de crédito*. Disponible en https://www.law.cornell.edu/wex/es/fraude_con_tarjeta_de_cr%C3%A9dito
- Mackenzie, A. (1 de agosto de 2015). *La Producción de Predicciones: ¿Qué quiere el aprendizaje automático?* Revista Europea de Estudios Culturales, 18,

- 429-445. Obtenido de <https://bbibliograficas.ucc.edu.co:2160/10.1177%2F1367549415577384>
- MarthWorks. (s.f.). *Aprendizaje Supervisado*. Obtenido de Técnica de Machine Learning para crear modelos predictivos a partir de datos de entrada y respuesta conocidos: <https://es.mathworks.com/discovery/supervised-learning.html..html>
- Mittal, S., y Tyagi, S. (29 de 07 de 2019). *Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection*. 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 320-324. Doi:10.1109/CONFLUENCE.2019.8776925
- Mohamad, M. A. (2018). *La combinación de auto codificadores y apoyo de vectores para la detección de fraude en transacciones con tarjeta de credito*. segunda conferencia en tendencias inteligentes en sistemas, seguridad y sostenibilidad (worldS4) (págs. 178 - 184). Londres: IEEE.
- Ñaupas, C. (2016). *Minería de datos aplicada a la detección de fraude electrónico en entidades bancarias*. Disponible en: <http://cybertesis.unmsm.edu.pe/handle/cybertesis/5080>
- Prajapati, J., y Jain, S. C. (2018). Machine Learning Techniques and Challenges in Wireless Sensor Networks. Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 233-238.
- Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., . . . Prettenhofer, P. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 2825--2830. Obtenido de <https://scikit-learn.org/dev/about.html#citing-scikit-learn>
- Pedregosa, F., Varoquaux, G., Gramfort, A., Perrot, M., Otros, Michel, V., . . . Duchesnay, É. (12 de 10 de 2011). https://scikit-learn.org/stable/modules/outlier_detection.html. Recuperado el 22 de 09 de 2019, de https://scikit-learn.org/stable/modules/outlier_detection.html
- Porto, A. v. (2015). Modelos computacionales y metodologías utilizadas en la detección de fraude de las tarjetas de crédito (tesis de grado) Universidad Nacional La Plata. Obtenido de <http://sedici.unlp.edu.ar/handle/10915/71300>
- Sampieri, R. H. (2018). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. McGraw Hill México.
- Vats, V., Zhang, S., Ahmed, S., y Enz, E. (2018). A Comparative Analysis of Unsupervised Machine Techniques for Liver Disease Prediction. IEEE International Symposium on Signal Processing and Information Technology, 486-489.
- Varmedja, D., Karanovic, M., Sladojevic, S., y Arsen, M. (2019). *Credit Card Fraud Detection - Machine Learning methods*. 18th International Symposium INFOTEH-JAHORINA (INFOTEH), 1-5.