

## Revisión de literatura sobre las técnicas de Machine Learning en la detección de fraudes bancarios

Literature review on Machine Learning techniques in bank fraud detection

Revisão de literatura sobre técnicas de Machine Learning na detecção de fraudes bancárias

**Julio Alvarado Zabala**

jr\_alvarado3108@hotmail.com  
Universidad Agraria del Ecuador  
<https://orcid.org/0000-0002-2792-7581>

**Ivette Martillo Alchundia**

ismartillo1607@hotmail.com  
Universidad Agraria del Ecuador  
<https://orcid.org/0000-0002-2195-3914>

**Geomar Guzman Seraquive**

jomaliz-1991@hotmail.com  
Universidad Agraria del Ecuador  
<https://orcid.org/0000-0002-8387-8921>

### RESUMEN

Se considera al aprendizaje automático o de máquinas (Machine Learning en inglés), como una subárea en el campo de la computación e informática, además de estar estrechamente ligada a la inteligencia artificial; el objetivo de esta técnica es lograr que los ordenadores aprendan, siendo un agente que mejore la experiencia; ha sido muy útil sobre todo para el análisis de investigaciones y procesos que generan grandes cantidades de datos; por ello para el presente artículo se realiza una revisión documental sobre el estado del arte de los principales métodos de aprendizaje automáticos, basados en publicaciones y artículos de hace no más de dos años, con la finalidad de conocer conceptos, identificar y comprender el funcionamiento de las diversas técnicas de Machine Learning empleadas para la detección de fraudes financieros.

**Palabras clave:** Machine Learning, inteligencia artificial, análisis de datos, aprendizaje automático.

### ABSTRACT

Machine learning or machine learning is considered as a subarea in the field of computing and informatics, in addition to being closely linked to artificial intelligence; The objective of this technique is to make computers learn, being an agent that improves the experience; it has been very useful especially for the analysis of investigations and processes that generate large amounts of data; For this article, a documentary review is carried out on the state of the art of the main automatic learning methods, based on publications and articles from no more than two years ago, in order to know concepts, identify and understand the operation of the various Machine Learning techniques used to detect financial fraud.

**Key words:** Machine Learning, artificial intelligence, data analysis, machine learning.

### RESUMO

O aprendizado de máquina ou aprendizado de máquina é considerado uma subárea no campo da computação e tecnologia da informação, além de estar intimamente ligado à inteligência artificial; O objetivo desta técnica é fazer os computadores aprenderem, sendo um agente que melhora a experiência; tem sido muito útil especialmente para a análise de investigações e processos que geram grandes quantidades de dados; Para este artigo, é realizada uma revisão documental sobre o estado da arte dos principais métodos de aprendizagem automática, com base em publicações e artigos de não mais de dois anos, a fim de conhecer conceitos, identificar e compreender o funcionamento dos vários Técnicas de Machine Learning usadas para detectar fraudes financeiras.

**Palavras-Chave:** Machine Learning, inteligência artificial, análise de dados, machine learning.

## 1. INTRODUCCIÓN

Con el pasar de los años, la inteligencia artificial ha evolucionado al punto de presentar diferentes metodologías de aprendizaje automático aplicadas a un sin número de áreas en la vida cotidiana; actualmente, con la gran cantidad de documentos que se producen y publican en la web, es fundamental contar con herramientas tecnológicas que permita a las personas obtener, procesar y discernir información que le resulte de utilidad en su formación profesional, justamente por ello “Las técnicas de aprendizaje automático están experimentando un auge sin precedentes en diversos ámbitos, tanto en el mundo académico como en el empresarial, constituyendo una palanca de transformación relevante” (Calvo, Guzmán, & Ramos, 2018). Es así que, con el desarrollo tecnológico que se evidencia, en el área de educación empresarial, y con mucha presencia en los últimos años, en temas de seguridad, el aprendizaje automático o de máquina, ha tomado principal relevancia con el objetivo de alcanzar un mayor y mejor entendimiento de toda la información que reposa en la nube.

Al ser esta una tecnología basada en patrones, es capaz de aprender relaciones y tendencias de manera automática, permitiendo integrar técnicas de gran capacidad analítica como el Machine Learning, además es posible, entre otras cosas, monitorear y configurar parámetros que colaboren en la detección de acciones que antes eran más difíciles de prevenir. Por ello, en la actualidad, diferentes empresas, sobre todo del área financiera, optan por esta alternativa para evaluar escenarios donde se valúan clientes con perfiles riesgosos e inclusive determinar operaciones que signifiquen fraudes.

Ante lo expuesto, se pretende responder a la interrogante ¿cuáles son los principales métodos de aprendizaje automáticos empleados para la detección de fraudes financieros?, por lo cual este artículo realiza un análisis documental con la intención de conocer, profundizar y generar conocimiento relacionado a las principales técnicas de Machine Learning que se utilizan para la detección temprana de fraudes financieros.

## 2 FUNDAMENTO TEÓRICO

Antes de proceder a la revisión teórica, es preciso considerar las investigaciones relativas al uso del Machine Learning en la detección de fraudes bancarios, así por ejemplo se presenta a Awoyemi, Adetunmbi, & Oluwadar (2017) quienes evaluaron el rendimiento de los algoritmos de clasificación conocidos como KNN y Naive Bayes en fraudes con tarjetas crediticias identificando por medio de muestreos aquella información asimétrica, identificando que éstos poseen una precisión del 97.69% y 97.92% respectivamente, lo que denota su utilidad para la banca. En la misma línea se encuentran Dhankhad, Mohammed, & Far (2018) quienes sugieren que los algoritmos de aprendizaje automático deben emplear información del entorno real a fin de prevenir transacciones fraudulentas en transacciones con tarjeta de crédito, su modelo propone la identificación de aquellas variables más significativas que permitan detectar acciones inadecuadas.

Por su parte Yee, Sagadera, & Malim (2018) mediante la metodología de aprendizaje automático, predijeron aquellas transacciones bancarias virtuales inusuales y de las cuales se sospecha de fraude, clasificándolas de aquellas que no lo eran, así por medio de la minería de información se pudieron reconocer ciertos patrones en los datos, así los algoritmos como Naive Bayes K2, TAN (Tree Augmented Naïve) presentaron una exactitud mayor al 95%.

En otro estudio, Campus (2018) investigaron Random Forest, SVM y el proceso logístico de regresión en fraudes con tarjetas crediticias y de débito en transacciones virtuales y físicas obteniéndose una precisión del 97.7% y 95.5% según corresponde. Cabe señalar que se trabajó con 284.786 registros transaccionales con tarjetas de individuos titulares de Europa. Mientras que Sailusha y otros (2020) emplearon Random Forest y Adaboost identificando que el primero

presenta un mejor desempeño en la detección de fraudes en entidades bancarias por medio de transacciones virtuales.

Estos hallazgos presentados por los investigadores sugieren la importancia y la gran necesidad de los entes bancarios de emplear medidas de prevención de fraudes pudiendo identificar estas acciones con antelación, esto se debe en gran medida que los clientes o usuarios, en la actualidad gestionan sus operaciones por vía electrónica, lo cual incrementa el riesgo de manipulación de ciertos procesos por hackers. Se reconoce en general que el fraude efectuado a los bancos son uno de los grandes inconvenientes para los mismos, en cuanto deriva en un problema económico, detrimento de su imagen y una notoria desconfianza de las personas por usar sus servicios.

## 2.1 Inteligencia artificial

La inteligencia artificial como tal es la simulación de tareas en base al conocimiento humano, pero realizado por máquinas, estos van desde el aprendizaje donde se incluye datos y modelos, razonamiento, en base a las características ingresadas que a su vez pueden elaborar una aproximación de un resultado en específico.

Tiene como objetivo convertirse en un futuro en una técnica empleada en todos los sectores de la sociedad, esto se lograría gracias a la implementación de sistemas inteligentes, o a su vez algoritmos y el aprendizaje automático (Bataller, 2019).

Es así que esta herramienta está inmersa desde las máquinas que son capaces de mantener un juego en línea, automóviles que no requieren un ente humano para funcionar, informes médicos automatizados y muchos más. Todo esto va de la mano con el Machine Learning y el aprendizaje profundo.

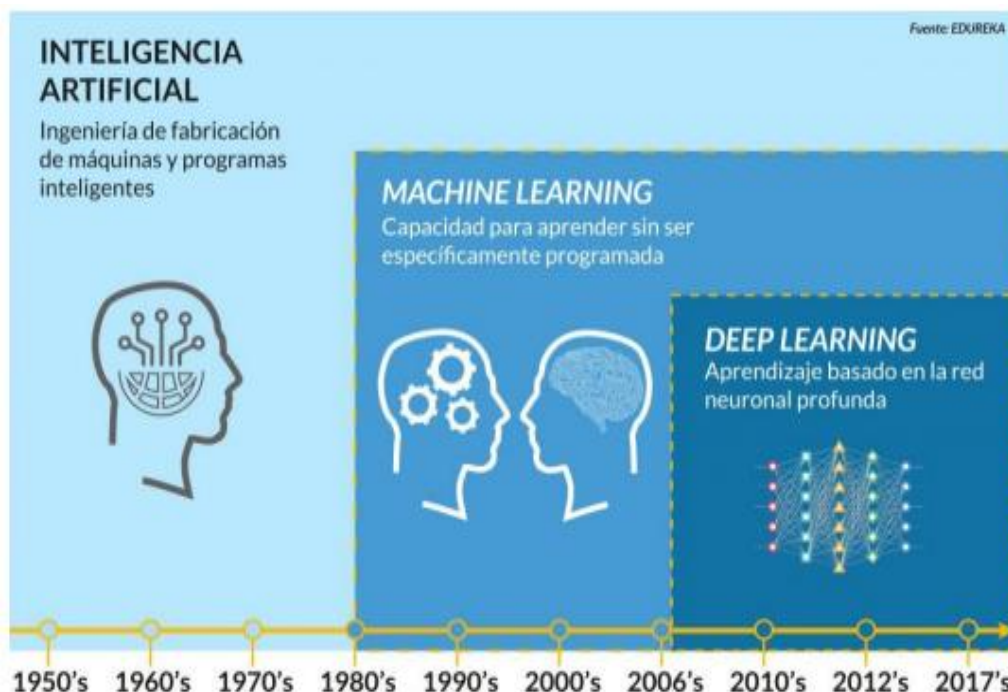


Fig. 1. Evolución de la inteligencia artificial Fuente: (Kamlofsky, Miana, & Gonzalez, 2019).

Dentro de la inteligencia artificial se encuentra el big data que se refiere a la recopilación y análisis periódicos de grandes cantidades de datos, estos pueden ser personales, empresariales, los mismos son objeto de un tratamiento automático en base a algoritmos para generar relaciones, parámetros, modelos (Hueso, 2019). Cabe recalcar que en la red se maneja millones de datos

procedentes de redes sociales y la web como tal, también entra en juego los scanner digitales, sensores biométricos y cualquier dispositivo que tenga la capacidad de adquirir información.

Con la ayuda de esta herramienta es posible generar parámetros para los programas de aprendizaje automático, aproximación a tendencias futuras, evaluar el comportamiento de un cliente, realizar estudios de mercado, mejorando así la toma de decisiones gracias a la predicción del comportamiento.

También se menciona al Deep Learning el cual trabaja con un conjunto de algoritmos que no son lineales aplicados para el modelamiento de los datos y patrones, emplea niveles que facilitan la extracción de la información ya sean datos o variables. Deep Learning para su funcionamiento emplea redes neuronales trabajando en niveles desde el más simple hasta el complejo en este último se dice que se genera el tipo de aprendizaje profundo (Kamlofsky, Miana, & Gonzalez, 2019).

Es así que cada red neuronal es capaz de generar aprendizaje con el fin de la generación de la respuesta. Así se busca adquirir una precisión mayor en el aprendizaje que el utilizado en Machine Learning y no hace falta otorgar características especiales de datos. La máquina es capaz de reconocer patrones que para el ojo humano son imperceptibles. Esto se logra con lo mencionado anteriormente. Como ejemplo de Deep Learning se puede mencionar al programa informático Alpha Go propiedad de Google, éste logró vencer al campeón de este juego que tiene muchas más combinaciones que el ajedrez lo cual ya es difícil para una máquina. Esta herramienta es utilizada en infinidad de situaciones tales como:

- Identificación de logos de empresas en la red.
- Seguimiento de canales online cuando realizan el lanzamiento de una marca
- Capacidad de predecir las preferencias de los clientes en la red
- Posibilidad de detectar personas con intenciones fraudulentas en el sector financiero, entre otras.

El Deep Learning tiene gran acogida en diferentes áreas pero dos de éstas son parte de las técnicas de aprendizaje en inteligencia artificial.

a) Reconocimiento de voz e imágenes: Tanto en el sector empresarial como académico se ha optado por trabajar con esta herramienta, incluso se mencionan aplicaciones como Skype, Siri que emplean Deep Learning para el reconocimiento de patrones de voz de individuos. En cuanto a las imágenes esta herramienta hace posible que se generen subtítulos y detalles de la escena de forma automática del lugar, facilitando encontrarlos en miles de fotos enviadas por usuarios (Arellano, 2019).

b) Sistemas de recomendación: Realizan las recomendaciones en base a las preferencias de los clientes (Paràmo, 2019). Una vez que ingrese a la aplicación por ejemplo Netflix le muestra una lista de las posibilidades que le interesarían. Previamente revisando su historial de búsquedas.

## 2.2 Machine Learning

El Machine Learning es una metodología para el análisis de datos que facilita el desarrollo de modelos analíticos, “se refiere a la capacidad que tienen los ordenadores de aprender a partir de los datos, mediante el uso de algoritmos que permiten a la máquina cambiar su comportamiento” (Zepeda, 2019) es una rama de la inteligencia artificial fundamentada en la idea que un sistema

puede aprender de datos para así identificar patrones y tomar decisiones con una mínima intervención del agente humano.

Esta disciplina se encuentra estrechamente ligada a la inteligencia artificial, la misma se plantea con la finalidad de abordar sistemas capaces de aprender automáticamente en un contexto de identificación de patrones y conductas en una amplia base de datos; esto mediante la utilización de algoritmos que se encargan de la revisión de dichos datos. El surgimiento del interés en el aprendizaje automático y el constante desarrollo de las tecnologías de la información y computación ha permitido que esta técnica evolucione a un contexto iterativo, ya que a medida que los modelos son expuestos a nuevos datos, éstos pueden aprender y adaptarse de forma independiente a través de cálculos previos, emitiendo resultados confiables.

Si bien esta metodología no es del todo nueva, ha tomado nuevos propósitos y rutas basada en algoritmos de aprendizaje de máquina aplicados en diferentes contextos del mundo real como por ejemplo cálculos matemáticos complejos de Big data o simplemente ofertas y recomendaciones en línea.

### 2.3 Machine Learning en el sector bancario

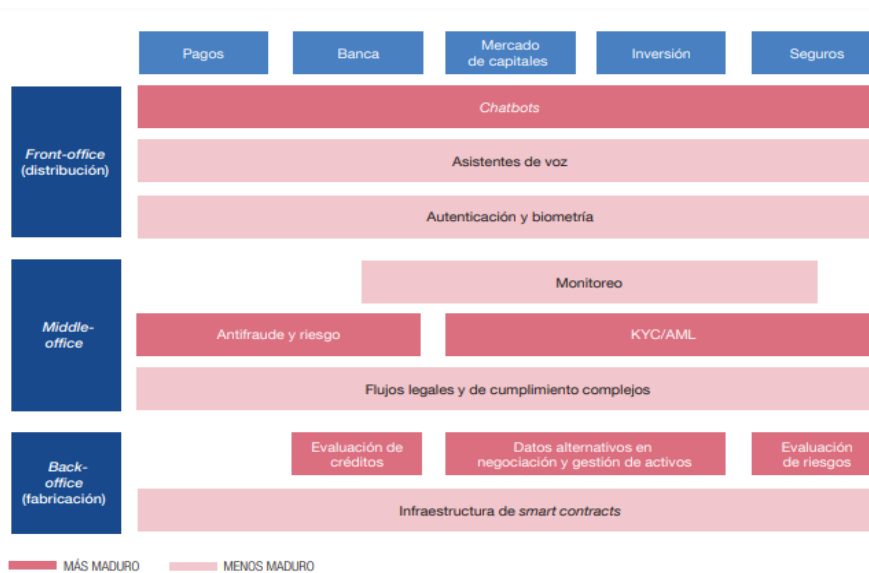


Fig. 2. Funcionamiento del Machine Learning en el sector financiero Fuente: (Giraldo & Caimàn, 2019).

Las herramientas con las que cuenta la inteligencia artificial hacen posible que, en el sector empresarial de forma específica en entidades financieras, se elabore una revisión de gran volumen de datos y de forma rápida (Frola, y otros, 2019). Esto conlleva a una precisión en la identificación de las tarjetas de crédito, evitando que ingresen datos fraudulentos, conceder préstamos por medio de revisión automática sin tener previa entrevista con el cliente, entre otros.

### 3 PROCEDIMIENTOS METODOLOGICOS

Se empleó una revisión de literatura que comprende un análisis bibliográfico, el mismo que de acuerdo con Hurtado (2020) se trata de un proceso documental que permite la recuperación de información publicada respecto a un tema en particular, por lo mismo posee un carácter retrospectivo en cuanto permite el acopio de datos de un periodo específico en el tiempo. Este proceso implica la selección de la documentación, su evaluación y posterior síntesis conforme los objetivos del estudio que se lleva a cabo.



Es así, que, con el fin de evidenciar las técnicas empleadas para la detección de fraudes bancarios, se revisaron 22 artículos, desde la biblioteca de Google académico, Dialnet, Scielo, Crossref, para ello se emplearon términos específicos o palabras clave que facilitaron la búsqueda, estos son: Machine Learning y fraude bancario, detección de fraude bancario, herramientas para prevenir el fraude bancario. Las publicaciones seleccionadas correspondieron al periodo entre los años 2018 al 2019 momento que es considerado como trascendental para la banca pues con la intención de mejorar su relación con los clientes se potencian los diversos servicios financieros por canales digitales valiéndose del auge de las tecnologías de la información y comunicación.

En términos metodológicos, la revisión planteada se diferencia de otras publicaciones en cuanto no valora la efectividad de los algoritmos de Machine Learning si no que se enfoca en identificar, de acuerdo a los investigadores seleccionados, cuáles son aquellos que generalmente se emplean para la detección de fraudes financieros. Los resultados del análisis de los artículos recabados se presentan a continuación:

#### 4. RESULTADOS Y DISCUSIÓN

En los 22 documentos analizados se evidenció una concordancia en cuanto al uso de las técnicas para detectar el fraude bancario. Así, se evidenciaron 5 técnicas principales para la detección de fraudes detalladas en la siguiente tabla:

**Tabla 1.** Técnicas de Machine Learning para detectar el fraude

Técnicas	Porcentaje de técnicas principales en la revisión de literatura
Redes neuronales	7 ( 32%)
Random forest	5 (23%)
Naive Bayes	4 (18%)
Maquinas vectoriales de soporte	4 (18%)
Modelos lineales generalizados (Modelo logit, probit, log-log)	2 (9%)
<b>Total</b>	<b>22 ( 100%)</b>

Según los resultados obtenidos se evidencia que la técnica aplicada de forma mayoritaria con un 32% es la Red Neuronal, seguida, por Random Forest con un 23%, de igual manera con un 18% respectivamente se encuentra Naive Bayes y las máquinas vectoriales de soporte, por último con 9% los modelos lineales generalizados (Ver tabla 1).

Ahora bien al respecto cabe indicar que en el caso de las redes neuronales, identificadas como las de mayor uso en la detección de fraudes, de acuerdo con Bellido (2019) éstas se fundamentan en la biología humana, esto significa que imitan el comportamiento de las neuronas en cuanto al aprendizaje se refiere, naturalmente esto únicamente en sus funcionalidades primarias. Son una técnica de la inteligencia artificial que se encarga de realizar regresiones complejas sobre grandes volúmenes de datos.

Las características principales son: aprendizaje desde la experiencia, sistematizan a partir de ejemplos previos para la generación de otros nuevos y abstracción de los datos de entrada. Esto concuerda precisamente con la propuesta de Dhankhad, Mohammed, & Far (2018) investigadores que expusieron la importancia del uso de algoritmos de aprendizaje automático que hagan uso de

datos reales con la intención de poder predecir y prevenir fraudes en transacciones electrónicas por medio del reconocimiento de variables destacadas en aquellas acciones irregulares que se detecten.

Además, Yee, Sagadera, & Malim (2018) expusieron algo similar, pues al igual que el cerebro humano, sugirieron métodos de aprendizaje automático que permitan la predicción de transacciones poco comunes y su clasificación de aquellas normales, de manera que con la minería de datos se puedan identificar aquellas patrones en las acciones poco habituales o anómalas en la banca virtual considerando que la precisión de esta metodología puede alcanzar hasta un 95%.

Por otra parte, en relación a Random Forest, Suntaxi, Ordoñez, & Pesantes (2018) lo denominan como un clasificador capaz de discernir grandes cantidades de datos, trabaja con valores aleatorios semejando su funcionamiento a los árboles de decisión. En la detección de fraudes utiliza la selección al azar de usuarios creando así nuevas entradas que a su vez permiten aprender el comportamiento pasado. En torno a ello Campus (2018) consideró que Random Forest posee una exactitud en la detección de fraudes del 97.7%, es decir mayor a las redes neuronales.

En cuanto a Naive bayes, éste se enfoca en la probabilidad de ocurrencia, es muy preciso cuando se trata de manejar grandes cantidades de información. Según los casos que se ingresan como nuevas entradas realiza la interpretación de cada variable (González & Ortiz, 2018). Al respecto para Awoyemi, Adetunmbi, & Oluwadar (2017) el rendimiento de este algoritmo asciende al 97.92% demostrando su gran utilidad en la banca, concordando con los hallazgos de Yee, Sagadera, & Malim (2018) quienes le otorgan una precisión superior al 95%.

Además, están las máquinas vectoriales de soporte, las cuales emplea un conjunto de datos que han sido introducidos previamente por el ente humano, estos son resultados de las observaciones de un entendido en el tema, a su vez sirven para el entrenamiento del sistema de aprendizaje (Bonsón & Ortega, 2019). Es importante mencionar que no siempre un individuo debe estar revisando los resultados obtenidos.

Las máquinas vectoriales de soporte se emplean para clasificar información y en el planteamiento de regresiones en tanto posee un error similar al de bayes, sin embargo posee una gran desventaja relativa a su complejidad algorítmica (Morteza, 2018).

Finalmente, en relación a los modelos lineales generalizados (logit, probit, log-log), estos trabajan con medios aleatorios y variables independientes, a su vez emplean el método de clasificación para el reconocimiento de patrones en usuarios que registren datos fraudulentos. Muestran datos que contienen mayor relevancia por ejemplo si se introducen 30 términos de entradas a la realización, la evaluación mediante este modelo solo arroja las respuestas más significativas (Calvo, Guzmán, & Ramos, 2018).

Por ejemplo, cuando se emplean modelos probit y logit, los hallazgos de ambos tienen una alta probabilidad de ser similares. Logit trabaja con razones de probabilidades y probit presenta un mejor rendimiento ante variables dependientes de dos valores (binarias). En cuanto a Log-Log, se trata de un modelo asimétrico y su funcionalidad es mayor frente a regresiones de Cox (probabilidad de que un evento suceda) que emplean riesgo proporcional (Guillén, 2019).

De tal manera que la detección de fraudes bancarios por medio de las técnicas de Machine Learning presenta variedad en el uso de algoritmos, siendo unos más efectivos que otros. Sin embargo queda claro que su uso siempre dependerá del tipo de datos que se analicen o empleen en la predicción de eventos inusuales, por lo que en algunos casos se podrán detectar las variables que los caracterizan, mientras que en otros se predecirá en base a la detección de acciones poco comunes. Sea cual fuere el algoritmo empleado, la finalidad siempre es la prevención y el detectar acciones consideradas como fraude en la banca en tanto afectan al balance no solo de la entidad financiera que lo sufre sino en la economía local.

## 5. CONCLUSIÓN

La revisión documental realizada permitió profundizar en los principales conceptos, definiciones y características del aprendizaje automático o de máquina (Machine Learning) y sus aplicaciones en cuanto a la seguridad y prevención de fraudes financieros; se pudo identificar las principales técnicas de Machine Learning expuestas por los autores de los artículos consultados de los años (2018 y 2019) donde se observa una tendencia alineada a la metodología de redes neuronales en la que se especifican las ventajas debido a su capacidad de estimar modelos no lineales, que sirven sobre todo para la cuantificación del riesgo de crédito.

Otras técnicas destacadas son Random Forest y Naive bayes, mismas que se enfocan en la probabilidad de que ocurra un hecho aislado, manejando grandes cantidades de información, trabajando con valores aleatorios que semejan el funcionamiento de un árbol de decisión.

Entonces, se concluye mediante el estudio realizado que existen diferentes técnicas capaces de establecer herramientas eficientes que reduzcan el riesgo de fraude financiero en este tipo de instituciones, además que, las redes neuronales son las que mayor aceptación y predilección entre los autores, que se explica en el sentido en que cuenta con gran versatilidad para diferentes aplicaciones pero no necesariamente son las más precisas.

Por su parte, la técnica Naive Bayes es simplista, y presenta una semántica sencilla que usa y genera conocimiento a través de análisis probabilísticos lo que la vuelve también una metodología popular entre los autores y además presenta mayor precisión que las demás.

Finalmente cabe indicar que el presente estudio presentó ciertas limitaciones a nivel teórico y metodológico, en cuanto no se identifican estudios a nivel de naciones, más bien las investigaciones son generales y no se realizan análisis de las situaciones locales. Por otra parte, las publicaciones encontradas datan de más de 10 años en un gran porcentaje, lo que las descalifica como información actualizada considerando la evolución de la tecnología y obviamente de los servicios bancarios. Considerando lo expuesto pueden surgir nuevas investigaciones enfocadas en el análisis del Machine Learning en cada país y los algoritmos de mayor uso en cada caso, además de indagaciones acerca de su efectividad.

## REFERENCIAS

- Arellano, W. (2019). El derecho a la transparencia algorítmica en Big Data e inteligencia artificial. *Revista General de Derecho Administrativo*.
- Awoyemi, J., Adetunmbi, A., & Oluwadare, S. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1-9). IEEE.
- Bataller, R. (2019). *La era de la inteligencia artificial. Nuevas herramientas para los creadores*. San Juan : Unversidad Nacional de San Juan .
- Bellido. (2019). Redes neuronales para predecir el comportamiento del conjunto de activos financieros más líquidos del mercado de valores peruano. *Revista Cientfica de la UCSA*,, 49-64. Retrieved from [https://ucsa.edu.py/yeah/wp-content/uploads/2019/04/4\\_A0.\\_Bellido-B.-Redes-neuronales-para-predecir-el-comportamiento\\_49-64.pdf](https://ucsa.edu.py/yeah/wp-content/uploads/2019/04/4_A0._Bellido-B.-Redes-neuronales-para-predecir-el-comportamiento_49-64.pdf)
- Bonsón, E., & Ortega, M. (2019). Big data, Inteligencia Artificial y Data Analytics ( BIDA). *Dialnet*, 11-13.
- Calvo, J., Guzmán, M., & Ramos, D. (2018). Machine Learning, una pieza clave en la transformación de los modelos de negocio. *Management Solutions*, 1 - 42. Retrieved from <https://www.managementsolutions.com/sites/default/files/publicaciones/esp/machine-learning.pdf>
- Campus, K. (2018). Credit card fraud detection using machine learning models and collating machine learning models. *International Journal of Pure and Applied Mathematics*, 118(20), 825-838.



- Dhankhad, S., Mohammed, E., & Far, B. (2018). Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. In 2018 IEEE International Conference on Information Reuse and Integration (IRI) (122-125). IEEE.
- Díaz, C. (2018). *Sistema de control ocular para una silla de ruedas motorizada*. Bogotá: Universidad Pedagógica Nacional. Retrieved from <http://200.119.126.32/bitstream/handle/20.500.12209/9488/TE-22264.pdf?sequence=1&isAllowed=y>
- Fernández, A. (2019). Inteligencia artificial en los servicios financieros. *Boletín Económico*, 1-10.
- Frola, Chesñevar, Alvez, Etchart, Miranda, Ruiz, & Teze. (2019). *Framework SDF Machine Learning en transacciones financieras y detección temprana de fraudes*. In XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan)..
- Giraldo, & Caimàn. (2019). Bigdata, Análisis Y Tendencias En La Economía Digital. *Eventos integrados*, 1-522.
- González, E., & Ortiz, A. (2018). *Detección de Fraude en Tarjetas de Crédito mediante técnicas de minería de datos*. Universidad Santo Tomás .
- Guillén, R. (2019). *Sistemas para detectar fraude en medios de pago*. Madrid: Universidad Politécnica de Madrid.
- Hueso, L. (2019). Riesgos e impactos del Big Data, la inteligencia Artificial, y la robótica. enfoques, modelos y principios de la respuesta del derecho . *Revista general del derecho administrativo* , 50-17.
- Hurtado, J. (2020). Metodología de la investigación. Guía para la comprensión holística de la ciencia (Cuarta ed.). Caracas: Quirón Ediciones.
- Jain, R., & Bhatnagar, R. (2019). Applications of Machine Learning in Cyber Security - A Review and a Conceptual Framework for a University Setup. *Book Chapter published 2020 in Advances in Intelligent Systems and Computing*, 599-608. Obtenido de [doi.org/10.1007/978-3-030-14118-9\\_60](https://doi.org/10.1007/978-3-030-14118-9_60)
- Kamlofsky, J., Miana, V., & Gonzalez, E. (2019). Uso de técnicas de inteligencia Artificial para el análisis del impacto de ambientes contaminantes en el índice de daño genético. *Revista abierta de informática Aplicada (RAIA)*, 11-34.
- Kumar, A., Bhatnagar, R., & Srivastava, S. (2018). Analysis of Credit Risk Prediction Using ARSkNN. *Book Chapter published 2018 in The International Conference on Advanced Machine Learning Technologies and Applications (AMLT2018)*, 644-652. [doi:doi.org/10.1007/978-3-319-74690-6\\_63](https://doi.org/10.1007/978-3-319-74690-6_63)
- Meneses, M. (2018). Grandes datos, grandes desafíos para las ciencias sociales. *Revista Mexicana de Sociología*, 415-444. Obtenido de <http://www.scielo.org.mx/pdf/rms/v80n2/0188-2503-rms-80-02-415.pdf>
- Morteza. (2018). Machine Learning: A Convergence of Emerging Technologies in Computing. *Book Chapter published 2018 in The International Conference on Advanced Machine Learning Technologies and Applications (AMLT2018)*, 181-192. [doi:doi.org/10.1007/978-3-319-74690-6\\_18](https://doi.org/10.1007/978-3-319-74690-6_18)
- Paràm, L. (2019). Inteligencia Artificial: ¿ Más peligros que beneficios? *Revista Ideales*, 1-6.
- Paulino, L., & Huayna, A. (2019). Sistema experto probabilístico en redes bayesianas para la predicción del cáncer de cuello uterino. *Revista Peruana de Computación y Sistemas*, 15-26. Obtenido de <https://revistasinvestigacion.unmsm.edu.pe/index.php/rpcsis/article/view/16360/14138>
- Reddy, D., Lingras, P., & Venkatanareshbabu. (2018). Advances in Machine Learning and Data Science. *Book published 2018 in Advances in Intelligent Systems and Computing*. [doi:doi.org/10.1007/978-981-10-8569-7](https://doi.org/10.1007/978-981-10-8569-7)
- Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. (2020). Credit Card Fraud Detection Using Machine Learning. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (1264-1270). IEEE.
- Singla, S., & Baliyan, N. (2019). Space Shuttle Landing Control Using Supervised Machine Learning. *Book Chapter published 2019 in Advances in Intelligent Systems and Computing*, 349-356. [doi:doi.org/10.1007/978-981-13-1822-1\\_32](https://doi.org/10.1007/978-981-13-1822-1_32)
- Suntaxi, M., Ordoñez, P., & Pesantes, M. (2018). Applications of Deep Learning in Financial Intermediation: A Systematic Literature Review. *KnE Engineering*, 47-60. [doi:10.18502/keg.v3i9.3645](https://doi.org/10.18502/keg.v3i9.3645)
- Yee, O., Sagadevan, S., & Malim, N. (2018). Credit card fraud detection using machine learning as data mining technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 10(1-4), 23-27.
- Zepeda. (2019). Los Big Data: conceptos relacionados y algunas aplicaciones en pediatría. *Revista Chilena de Pediatría*, 376-383. Retrieved from [https://scielo.conicyt.cl/pdf/rcp/2019nahead/0370-4106-rcp-rchped\\_v90i4\\_1306.pdf](https://scielo.conicyt.cl/pdf/rcp/2019nahead/0370-4106-rcp-rchped_v90i4_1306.pdf)