# Análisis de las técnicas de machine learning aplicadas en la detección de fraudes bancarios

Ferrin Velásquez Rosa Julexy

October 16, 2023

**Resumen**

Este artículo realiza una revisión de literatura basada en diversos artículos de los dos últimos años, discute y evalúa la aplicación de técnicas de aprendizaje automático dentro del área bancario. Se explora varias métricas empleadas, las cuales ayudan a la evaluación para dar concretamente con el algoritmo más utilizado en la detección de fraudes bancario.

**Palabras clave:** Machine learning, inteligencia artificial, análisis de datos, fraudes bancarios

**Abstract**

This article conducts a literature review based on various articles from the last two years, discusses and evaluates the application of machine learning techniques within the banking area. Several metrics used are explored, which help the evaluation to specifically find the algorithm most used in the detection of banking fraud.

## 1 Introducción

Con el avance de la inteligencia artificial a lo largo de los años, se han desarrollado diversas metodologías de aprendizaje automático que tienen aplicaciones en diversas áreas de la vida cotidiana. En la actualidad, con la creciente cantidad de información en la web, es esencial contar con herramientas tecnológicas para obtener, procesar y comprender información relevante en ámbitos profesionales. El aprendizaje automático está experimentando un crecimiento significativo en la academia y en el mundo empresarial, transformando diferentes sectores, especialmente en educación, negocios y seguridad.

El aprendizaje automático se ha vuelto crucial para comprender y analizar la vasta cantidad de información en línea, ya que puede aprender patrones y tendencias automáticamente. Esto permite aplicar técnicas analíticas avanzadas, como el machine learning, para monitorear y configurar parámetros que facilitan la detección de acciones difíciles de prevenir anteriormente. En la actualidad,

muchas empresas, especialmente en el sector financiero, utilizan el aprendizaje automático para evaluar clientes de alto riesgo y detectar posibles fraudes.

El objetivo del artículo es analizar las técnicas de machine learning más comunes utilizadas en la detección de fraudes bancarios a través de una revisión de literatura y explorar las métricas utilizadas en este contexto.

# 2 Materiales y métodos

Se empleó una revisión de literatura con el fin de evidenciar las técnicas empleadas para la detección de fraudes bancarios, se revisaron artículos desde diferentes fuentes bibliográficas publicado en los años 2018 al 2020 con la finalidad de recabar información lo más actualizada posible.

Para garantizar la calidad y veracidad de la información consultada se aplican estrategias de búsqueda que garanticen un adecuado proceso de selección, se utilizaron bases de datos como Scopus, Scielo, Web of Science o IEEE Xplore; la selección se limita en función del título, palabras clave y el resumen que presenta cada artículo.

El objetivo es analizar la popularidad, características y eficiencia de las principales técnicas de minería de datos y machine learning desde el punto de vista que los investigadores exponen en función de la detección de fraudes bancarios.

# 3 Resultados y discusiones

## 3.1 Machine Learning en el sector bancario

El Machine Learning es una metodología para el análisis de datos que facilita el desarrollo de modelos analíticos. [2] indica que "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". En otras palabras, 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.

En el contexto de las entidades bancarias, el aprendizaje automático se utiliza para combatir el fraude y mejorar la experiencia del cliente con bienes y servicios. El fraude puede causar pérdidas financieras y dañar la reputación de la empresa bancaria. Por ello, el aprendizaje automático se utiliza para desarrollar sistemas de verificación y control contra este tipo de ataques, como sistemas de verificación de direcciones y tarjetas. Además, las herramientas de inteligencia artificial permiten una revisión eficiente de grandes volúmenes de datos del sector empresarial, particularmente de instituciones financieras.

[3] mencionan que la regresión lineal simple o múltiple, redes neuronales artificiales, análisis de discriminante lineal, máquinas de soporte vectorial, árboles de decisión o Naive Bayes; se determinan como las principales técnicas utilizadas para la detección de fraudes en entidades bancarias. Diferentes trabajos se han enfocado en determinar la eficiencia de estas en función de métricas que

evalúan su rendimiento, simplicidad y comportamiento, por ellos partiendo de la revisión bibliográfica se mencionan las más utilizadas.

Existen diversos algoritmos de aprendizaje automático, incluyendo:

- **Redes Neuronales.** Para [4] mencionan que estas redes están basadas en la biología humana, esto significa que imitan el comportamiento de las neuronas en cuanto al aprendizaje se refiere. Durante la evaluación, la red neuronal puede detectar transacciones que muestran patrones inusuales o divergen de lo que ha aprendido, lo que podría indicar un fraude.

- **Random Forest.** Se le denomina como clasificador capaz de discernir grandes cantidades de datos, trabajan con valores aleatorios semejando su funcionamiento a los árboles de decisión [1]. 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.

- **Naive Bayes.** Se utiliza para calcular la probabilidad de que una transacción sea fraudulenta dado un conjunto de características. Luego, se compara esta probabilidad con un umbral para determinar si la transacción es sospechosa.

- **Máquinas Vectoriales de Soporte (SVM).** Se utiliza para encontrar un hiperplano que separe las transacciones normales de las fraudulentas en un espacio multidimensional de características. Las transacciones que caen en el lado equivocado del hiperplano se consideran sospechosas.

- **Modelos lineales generalizados logit, probit, log log.** Trabaja con medios aleatorios y variables independientes, a su vez emplea el método de clasificación para el reconocimiento de patrones en usuarios que registren datos fraudulentos [5].

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

| Técnicas | Porcentaje de técnicas principales en la revisión de literatura |
|---|---|
| **Redes neuronales** | (36%) |
| **Random forest** | (20%) |
| **Naive Bayes** | (16%) |
| **Maquinas vectoriales de soporte** | (16%) |
| **Modelos lineales generalizados (Modelo logit, probit, log, log)** | (12%) |
| **Total** | (100%) |

Figura 1: Técnicas de Machine Learning para detectar el fraude

Como se puede ver en la Figura 1, según los resultados obtenidos se evidencia que la técnica aplicada de forma mayoritaria con un 36 % es la red neuronal, seguida, por Random Forest con un 20 %, de igual manera con un 16 % respectivamente se encuentra Naive Bayes y las maquinas vectoriales de soporte, por último, con 12 % los modelos lineales generalizados.
Una vez definida la popularidad de las técnicas de machine learning entre los autores, se analizan las métricas que los mismos utilizan para (Frola, y otros, 2019) evaluar la eficiencia de estas, para las métricas juegan un rol fundamental en problemas de clasificación donde se busca analizar algoritmos Machine y Deep Learning, facilitando así la elección del mejor algoritmo en función de un objetivo concreto.

| Métrica | Descripción | Porcentaje |
|---|---|---|
| **Accurary** | Clasificaciones predichas de manera correcta en función del total de incidencias | (58%) |
| **Recall** | Porcentaje de casos positivos debidamente clasificados | (20%) |
| **False positive rate** | Precisión de una prueba de diagnóstico o aprendizaje | (10%) |
| **Specificity** | Porcentaje de casos positivos debidamente clasificados | (6%) |
| **Índice kappa** | K=Po-Pe/1-Pe -> donde Po es la proporción de accuarary observado por lo tanto Po = accurary | (6%) |
| **Total** | | (100%) |

Figura 2: Métricas utilizadas para la evaluación de técnicas machine learning

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.

# 4 Conclusiones

La revisión de literatura se centró en el aprendizaje automático o de máquina (machine learning) y sus aplicaciones en la seguridad y prevención de fraudes financieros. Se destacaron técnicas de machine learning, como las redes neuronales, Random Forest y Naive Bayes, con un énfasis en la capacidad de las redes neuronales para estimar modelos no lineales y cuantificar el riesgo de crédito. Se concluye que existen diversas técnicas efectivas para reducir el riesgo de fraude financiero, con una preferencia hacia las redes neuronales debido a su versatilidad en diversas aplicaciones.

La exactitud o accurary es la métrica de mayor utilización, los principales valores de exactitud expuestos están entre el 70 y 99 % en las diferentes implementaciones y técnicas de clasificación sobre todo en redes neuronales, convolu-

cionales y máquinas vectoriales de soporte. Estas se enfocan en el tiempo que le toma al algoritmo arrojar resultados, por su parte alguna de ella se enfoca en el costo computacional.

# Referencias


[1] Monleón Getino A. Rodellar J Borja Robalino, R. Estandarización de métricas de rendimiento para clasificadores machine y deep learning. *Revista Ibérica de Sistemas e Tecnologias de Informaçã*, 30:84–196, 2020.

[2] L Hueso. Riesgos e impato del big data, la inteligencia artificla, y la róbotica. enfoque modelos y principios de la respuesta del derecho. *Revista general del derecho administrativo*, pages 2–37, 2019.

[3] J. M. Martínez A. Quesada López C Ramírez, A. Uso de técnicas de minería de datos y aprendizaje automático para la detección de fraudes en estados financieros: un mapeo sistemático de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação*, pages 97 – 109, 2020.

[4] Benannou Sadgali, Sael. Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, pages 45–54, 2019.

[5] Baliyan N. Singla, S. *Space Shuttle Landing Control Using Supervised Machine Learning*. Book Chapter published 2019 in Advances in Intelligent Systems and Computing, 1st edition, 2019.