risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 20/11/2019
Aceitação/Acceptance: 27/02/2020

Uso de técnicas de minería de datos y aprendizaje automático para la detección de fraudes en estados financieros: un mapeo sistemático de literatura

Alex Ramírez-Alpízar, Marcelo Jenkins, Alexandra Martínez, Christian Quesada-López

alex.ramirez@ucr.ac.cr, marcelo.jenkins@ucr.ac.cr, alexandra.martinez@ucr.ac.cr, cristian.quesadalopez@ucr.ac.cr

Universidad de Costa Rica, San Pedro, Costa Rica.

Pages: 97–109

Resumen: La detección de fraudes en estados financieros es una tarea constante y laboriosa en el área de la auditoría. Tradicionalmente, esta tarea ha sido realizada por expertos, limitando su alcance por restricciones en la capacidad de procesamiento manual. En los últimos años se ha incrementado el uso de técnicas de minería de datos y de aprendizaje automático para revisar de forma exhaustiva y automatizada los estados financieros de las organizaciones. El objetivo de esta investigación fue analizar técnicas de minería de datos y de aprendizaje automático utilizadas en la detección de fraudes financieros, con el fin de caracterizar los algoritmos reportados y las métricas usadas para evaluar su efectividad. Para ello se realizó un mapeo sistemático de literatura que identificó 67 artículos. Los resultados indican que desde el 2015 hubo un repunte en la cantidad de investigaciones que utilizan estas técnicas para la detección de fraude en estados financieros, donde las máquinas de soporte vectorial son la técnica más utilizada, con 19 estudios, seguida por las redes neuronales artificiales, con 15 reportes, y los árboles de decisión, con 11 reportes. La efectividad fue evaluada a partir del grado de exactitud con que las técnicas implementadas detectaban casos reales de fraude, obteniendo resultados de entre 70% y 99.9%.

Palabras-clave: Detección de fraude; aprendizaje automático; minería de datos; estados financieros, auditoría.

Use of data mining and machine learning techniques for fraud detection in financial statements: a systematic mapping study

Abstract: Fraud detection in financial statements is a constant and laborious task in the audit area. Traditionally, this task has been performed by experts, limiting its scope due to restrictions in manual processing capacity. In recent years, there has been an increase in the use of data mining and machine learning techniques to review in a comprehensive and automated way the organizations' financial statements. The objective of this study was to analyze data mining and machine learning techniques used in financial fraud detection, in order to characterize the

reported algorithms and the metrics used to evaluate their effectiveness. For this, a systematic mapping study of 67 studies was carried out. Our results show that since 2015 there was an upturn in the amount of studies that use these techniques for fraud detection in financial statements, where vector support machines are the most used technique, with 19 studies, followed by artificial neural networks, with 15 studies, and decision trees, with 11 studies. Effectiveness was assessed by the degree of precision with which the implemented techniques detected real fraud cases, obtaining values between 70% and 99.9%.

Keywords: Fraud detection; machine learning; data mining; financial statements; audit.

1. Introducción

La detección de fraudes en estados financieros es una tarea recurrente y una necesidad, tanto para organizaciones públicas como para empresas privadas. Las técnicas convencionales de auditoría financiera se utilizan como un medio para determinar la salud financiera y las perspectivas a futuro de la organización (Ngai y cols., 2011).

La revisión de estados financieros es vital para prevenir las consecuencias generalmente devastadoras de los fraudes. Esto implica distinguir datos fraudulentos de datos auténticos, revelando así actividades o comportamientos anómalos, con la finalidad de permitir a los tomadores de decisiones desarrollar, tan pronto como sea posible, estrategias que disminuyan el impacto del fraude (Ngai y cols., 2011).

No obstante, la capacidad de procesamiento de expertos humanos es limitada, y la cantidad de información generada cada vez es mayor, por lo que se hace necesario recurrir a la tecnología para procesar grandes volúmenes de datos, de manera que se puedan detectar patrones que posiblemente resultarían imperceptibles para un ser humano (Shalev-Shwartz,2014).

La presente investigación tiene por objetivo analizar las técnicas de minería de datos y aprendizaje automático, con respecto a sus algoritmos y su efectividad, en el contexto de detección de fraudes en estados financieros. Se realizó un mapeo sistemático de literatura para identificar la evidencia existente sobre la aplicación de estas técnicas y su efectividad obtenida. Para llevar a cabo el estudio se establecieron las siguientes preguntas de investigación:

RQ1. ¿Qué técnicas de minería de datos y de aprendizaje automático se han utilizado en la detección de fraudes en estados financieros?

RQ2. ¿Cómo ha sido evaluada la efectividad de las técnicas de minería de datos y de aprendizaje automático utilizadas en la detección de fraudes en estados financieros?

Este resto del artículo está estructurado de la siguiente manera: en la sección 2 se presenta el marco teórico, la sección 3 describe trabajos relacionados, la sección 4 explica la metodología utilizada, la sección 5 muestra los resultados obtenidos, la sección 6 discuten dichos resultados y, la sección 7 presenta las conclusiones.

2. Marco teórico

Los fraudes financieros se han clasificado comúnmente en tres grandes categorías: fraude bancario, fraude corporativo, y fraude de seguros (West y cols., 2015). Cada una de estas categorías se subdivide, a su vez, en distintos tipos. Los tipos de fraude bancario son: fraude con tarjetas de crédito, fraude hipotecario, y lavado de dinero. Los tipos de fraude corporativo incluyen fraude en estados financieros, y fraude en valores y materias primas. Finalmente, entre los tipos de fraude de seguros están: el fraude en seguros de automóviles, y el fraude en seguros de salud (West y cols., 2015).

El concepto "fraude en estados financieros" agrupa una serie de comportamientos en los cuales los participantes de un mercado financiero hacen declaraciones falsas sobre la verdadera naturaleza o la salud financiera de una compañía, un fondo o un producto de inversión (Reurink, 2016). Esta modalidad de fraude es típicamente cometida por una de estas razones: para encubrir una mala aplicación de fondos, para inducir a los inversores en un error, o para engañar a los reguladores sobre la rentabilidad de la organización (Reurink, 2016).

De acuerdo con la *Association of Certified Fraud Examiners* (2018), el fraude en estados financieros, si bien es el menos común, es también el más costoso para las organizaciones: en 2018, de un total de 2690 casos de fraude financiero en 125 países, representó el 10% de los casos, y una pérdida promedio por caso de 80,0000 dólares, mientras que la apropiación indebida de activos representó el 89% de los casos y una pérdida promedio de 114,000 dólares.

El concepto "aprendizaje automático" se refiere a la detección automática de patrones significativos en los datos, y se ha vuelto una herramienta común en casi cualquier tarea que requiera la extracción de información a partir de grandes volúmenes de datos (Shalev-Shwartz, 2014). Los algoritmos de aprendizaje automático han resultado exitosos en una amplia gama de tareas y dominios, incluyendo la visión por computadora, el reconocimiento de voz, la clasificación documental, la conducción automática y el soporte en la toma de decisiones (Blum y cols., 2015). Las aplicaciones de aprendizaje automático permiten un análisis completo de toda la información disponible (en lugar de solo muestras), así como la detección de patrones que pueden resultar imperceptibles para el humano (Shalev-Shwartz, 2014).

Existen diversas técnicas de minería y aprendizaje, entre las cuales están: regresión (regresión lineal simple, regresión lineal múltiple, regresión polinomial), clasificación (K vecinos más cercanos KNN, máquinas de soporte vectorial SVM, *Kernel* SVM, *Naïve Bayes*, árboles de decisión DT-, árboles aleatorios -RF-), agrupamiento (*K-means*, agrupamiento jerárquico), reducción de la dimensionalidad (análisis de componentes principales PCA, análisis de discriminante lineal LDA, *Kernel* PCA), redes neuronales (redes neuronales artificiales ANN, redes neuronales convolucionales), aprendizaje profundo (*deep learning*) y aprendizaje por refuerzo (Shalev-Shwartz, 2014; Blum y cols., 2015.), entre otras.GG

Además de conocer las técnicas usadas para la detección de fraudes en estados financieros, la presente investigación se avocó a determinar las métricas con las que se evalúa la efectividad de dichas técnicas, desde la perspectiva de su eficiencia y eficacia. La eficiencia de un algoritmo suele medirse en términos de su rendimiento o comportamiento, lo cual se centra principalmente en su simplicidad y el uso óptimo de los recursos. Esto último suele evaluarse con base en dos parámetros: el espacio, es decir, la memoria que utiliza, y el tiempo, que corresponde a lo que tarda el algoritmo en ejecutarse. Esos parámetros permiten comparar algoritmos entre sí, para determinar el más adecuado entre varios que solucionan un mismo problema (Guerequeta y Vallecillo, 2000). La eficacia determina qué tan cercana es la respuesta que da un algoritmo a la respuesta correcta u óptima (Shalev-Shwartz, 2014).

3. Trabajo relacionado

En esta sección se presentan estudios secundarios que realizan investigaciones sobre las técnicas de minería de datos y aprendizaje automático para la detección de fraudes financieros. Albashrawi (2016) llevó a cabo una revisión de literatura entre 2004 y 2015 sobre técnicas de minería de datos para la detección de fraudes financieros. Encontró que la regresión logística, DT, SVM, ANN y las redes bayesianas han sido ampliamente utilizados, aunque no siempre están asociados a los mejores resultados. Analizó 65 artículos relevantes y abarcó diversas formas de fraude financiero, por ejemplo, con tarjetas de crédito, con seguros de automóviles y de salud; en lo concerniente a fraudes en estados financieros, obtuvo 21 artículos. En términos de detección de fraudes en general -no solo de estados financieros-, encontró que el algoritmo más utilizado fue la regresión logística, con 13%, seguido por ANN y DT, con 11% cada uno, y SVM, con 9%.

Duhart y Hernández (2016) hicieron una revisión de literatura de los principales indicadores y algoritmos de minería de datos utilizados para la detección de fraudes. Entre los algoritmos referidos están SVM, ANN, las redes neuronales probabilísticas y K-vecinos más cercanos. Los autores compararon la exactitud de las clasificaciones obtenidas por los algoritmos. Las redes bayesianas ocuparon el primer lugar, con 90.3%, seguidas por ANN, con 80%, y DT, con 73.6%.

Ngai y cols. (2011) realizaron una revisión de literatura sobre la aplicación de técnicas de minería de datos para la detección de fraudes financieros, de 1997 a 2008. Analizaron 49 artículos y crearon una clasificación de tipos de fraude. El fraude en estados financieros fue clasificado dentro de la categoría “Otros fraudes financieros relacionados”, junto con los fraudes de mercadeo masivo.

Como aporte, la presente investigación se centra específicamente en el análisis de las técnicas para la detección de fraudes en estados financieros, y se analizan un total de 67 artículos del 2007 a 2019. Adicionalmente, se indaga sobre las métricas con las que se mide la efectividad de los algoritmos y sus resultados.

4. Metodología

En esta sección se describen brevemente los pasos del proceso de mapeo realizado, de acuerdo con los lineamientos de Petersen y cols. (2015) y las recomendaciones de

Kitchenham (2007). El objetivo del estudio, formulado con el modelo GQM (Basili y cols., 1994), fue analizar técnicas de minería de datos y aprendizaje automático, con el propósito de caracterizarlas con respecto a sus algoritmos, su eficiencia y efectividad, desde el punto de vista de los investigadores, en el contexto de detección de fraudes en estados financieros.

4.1. Estrategia de búsqueda y proceso de selección de estudios

Se realizó una búsqueda exploratoria para identificar estudios relevantes, los cuales fueron usados como artículos de control, es decir, estudios base para guiar el proceso de búsqueda. Estos estudios fueron: Affifah y cols. (2017), Li y Wong (2015), Seemakurthi y cols. (2015), y Yao y cols. (2018). Esta búsqueda se basó en el objetivo y las preguntas de investigación del estudio. La cadena de búsqueda se construyó a partir de la extracción de términos clave del título y del resumen del conjunto de artículos de control, y el criterio de los investigadores. Se usó el modelo PICO (Población, Intervención, Comparación, Salidas) (Pai y cols., 2004) para la construcción de la cadena de búsqueda, dando como resultado la siguiente cadena:

(“data mining” OR “machine learning” OR “data analysis”) AND
(“financial” AND “fraud” AND “detection”)*

La cadena fue producto de un proceso de refinamiento que incluyó varias pruebas piloto para reducir el ruido. Las búsquedas automatizadas se realizaron en las bases de datos *SCOPUS*, *IEEE Xplore*, y *Web of Science*. El protocolo base del mapeo fue desarrollado durante el primer semestre del 2019. La búsqueda automatizada se realizó en mayo de 2019 y los estudios se analizaron entre mayo y agosto de 2019.

El número de estudios recuperado para cada base de datos fue: 240 en *Scopus*, 147 en *IEEE Xplore* y 33 en *Web of Science*. Los artículos fueron tabulados en MS Excel para los procesos de selección, evaluación y extracción de datos. Se eliminaron los duplicados, se aplicaron los criterios de inclusión y exclusión (I/E) y finalmente se hizo la extracción y el análisis de los resultados. Tras la la eliminación de los artículos duplicados, se obtuvo un total de 316 entradas diferentes.

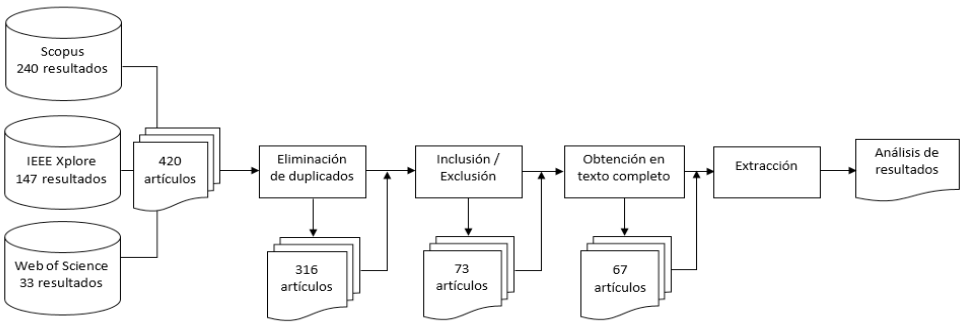

Figura 1 – Proceso de selección de los artículos.

El proceso de I/E se hizo con base en el título y el resumen de los artículos (cuando hubo duda, se hizo lectura completa del artículo). Se incluyeron solo (I1) artículos en inglés, (I2) que presentaran la aplicación de técnicas de minería de datos y de aprendizaje automático en el contexto de la detección de fraudes en estados financieros. Se excluyeron publicaciones que (E1) no trataran sobre fraude en estados financieros, (E2) artículos que no son estudios primarios, y (E3) artículos sobre medicina, criptomonedas, intrusiones o malware. Se identificaron un total de 67 artículos, tal como se muestra en la Figura 1. Existen 6 artículos que no pudieron ser obtenidos en texto completo y que reportamos a continuación: Young Moon y Don Kim (2017), Song y Ge (2012), Jan y Hsiao (2018), Rizani y Respati (2018), Meenatkshi y Sivaranjani (2016) y Xiong y cols. (2012). Estos estudios no fueron analizados.

4.2. Evaluación de calidad

La evaluación de la calidad refleja el nivel de detalle ofrecido por cada artículo para los aspectos estudiados. Para la evaluación de la calidad de los estudios primarios identificados se definieron las siguientes preguntas: ¿El artículo explica claramente una o varias técnicas de aprendizaje automático o minería de datos?, ¿se explica el proceso de desarrollo de una herramienta de software?, ¿se utilizan métricas para evaluar la herramienta? y ¿a qué tipo de estudio corresponde (¿experimento, cuasi-experimento o caso de estudio, encuesta? La puntuación se realizó con una escala de 0 a 1, donde 0= No cumple en lo absoluto, 0.5= Cumple parcialmente, 1 = Cumple totalmente. Los valores de calidad obtenidos variaron entre 0 y 4, con una mediana de 3,5 y un promedio de 2,9, lo que indica que la mayoría de los estudios analizados brindan el detalle requerido para responder a las preguntas de investigación. El detalle de la evaluación de calidad se encuentra disponible en http://shorturl.at/dvLPT.

4.3. Amenazas a la validez

A continuación se presentan las amenazas a la validez del estudio, así como las estrategias para minimizarlas.

Cobertura sujeta a los términos de búsqueda y a los repositorios de búsqueda. La cadena de búsqueda fue definida a partir de un conjunto de artículos de control, y piloteada en varias pruebas, para reducir el ruido. Las bases de datos seleccionadas son reconocidas por tener gran cobertura en el área de la ingeniería de software (SE). Ante dudas sobre la inclusión de un artículo se realizó la lectura completa. Se excluyó literatura gris y artículos que no están en inglés. Los estudios secundarios identificados durante el proceso validan la selección de artículos primarios.

Extracción y clasificación. La extracción se basa en un esquema de clasificación específico. El proceso de clasificación y extracción fue realizado por el primer autor. La interpretación de los resultados por parte de los investigadores es una amenaza a la validez. Los artículos fueron clasificados de acuerdo con lo reportado por los autores originales y en caso de no ser reportados explícitamente los investigadores de este estudio intentaron dar una clasificación. Se realizó un proceso sistemático para la clasificación de los artículos. Se diseñó un formulario de extracción para la recolección de datos que guía

el proceso y podría ser revisado. La aplicación de los criterios de calidad fue realizada solo por un investigador, lo que representa una amenaza a la validez.

Generalización de los resultados. La generalización de resultados se limita a los estudios incluidos en el mapeo. Durante todo el proceso, se aplicaron protocolos para ejecutar estudios secundarios. Se reportó el proceso para facilitar el análisis y replicación.

4.4. Proceso de extracción y análisis

El proceso de extracción y análisis permitió obtener y procesar la información de interés para cada uno de los estudios relevantes. Para cada artículo se extrajo los datos para su identificación y la información para responder cada una de las preguntas de investigación: las técnicas de minería de datos y aprendizaje automático a las que hizo referencia, en qué contexto, el algoritmo utilizado, las métricas y sus resultados. Se clasificaron los algoritmos encontrados en 10 categorías, según el tipo de técnica en la que se basó cada uno, y se desarrollaron distribuciones de frecuencia con el fin de determinar las tendencias de las técnicas más utilizadas. La clasificación se basó en las categorías presentadas por Shalev-Shwartz (2014). La extracción se realizó por el investigador principal en los formularios previamente definidos para este proceso.

5. Análisis de resultados

En esta sección se presentan los resultados del mapeo. El listado completo de estudios primarios analizados se encuentra disponible en *http://shorturl.at/dvLPT*. Cada artículo se identifica con el identificador *Sx*, donde *x* corresponde al número del artículo. Los primeros artículos analizados son de 2007 y desde entonces se identificaron artículos de interés para cada año, hasta 2019. Como puede observarse en la figura 2, en 2015 y 2016 hubo un repunte en la cantidad de artículos relevantes, ambos con 11 reportes; mientras que de 2012 y 2013 se obtuvo un solo artículo de interés por cada año.

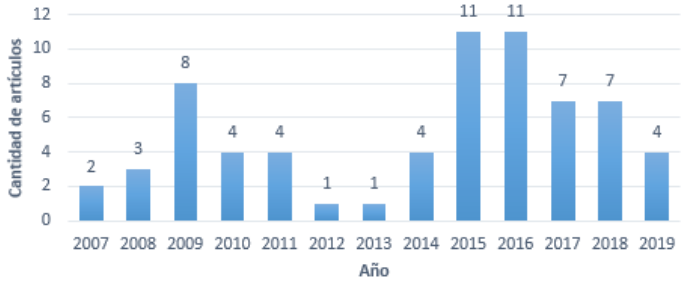

Figura 2 – Cantidad de artículos por año.

5.1. Técnicas de minería de datos y aprendizaje automático aplicadas en la detección de fraudes financieros (RQ1)

Se identificaron 8 técnicas generales de minería de datos y aprendizaje automático, además de híbridos entre 2 técnicas y propuestas de *frameworks*, de manera que se

utilizó una clasificación en 10 categorías. Se reportaron 57 algoritmos, los cuales se clasificaron dentro de cada una de las categorías. En la tabla 1 se muestran los artículos que reportan cada una de las técnicas.

Técnica	Referencia	Cantidad
Clasificación	S10, S16, S31, S44, S47, S61, S64, S66, S99, S104, S108, S112, S126, S130, S131, S133, S153, S161, S162, S163, S175, S176, S184, S188, S193, S215, S217, S220, S221, S224, S230, S235, S239, S265, S282, S297, S311, S315	38
Redes Neuronales	S10, S14, S99, S104, S126, S130, S133, S161, S163, S175, S181, S183, S217, S220, S235, S240, S265, S292, S296, S302, S311	21
Regresión	S10, S31, S112, S130, S163, S175, S176, S220, S221, S235	10
Agrupamiento	S126, S215, S217, S221, S264, S292, S297, S301	8
Probabilísticos	S3, S102, S172, S300, S304	5
Propios	S18, S247, S257, S263, S271	5
Frameworks	S11, S12, S13, S30, S111	5
Heurísticos	S126, S155, S168, S187	4
Reducción de dimensionalidad	S130, S215, S297	3
Híbridos	S15, S79, S235	3

Tabla 1 – Técnicas para detección de fraude financiero.

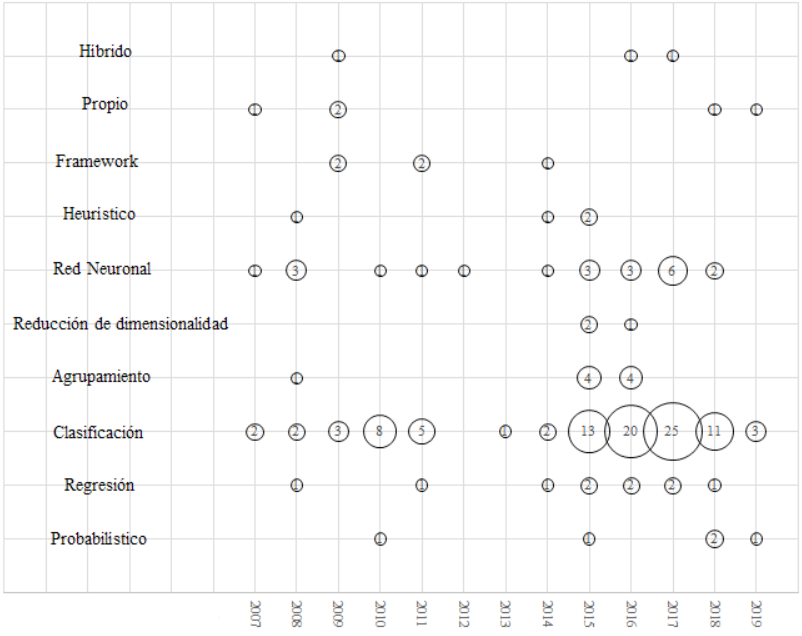

Figura 3 – Técnicas reportadas para la detección de fraudes en estados financieros.

Algunos artículos hacen referencia a más de un algoritmo, ya sean dentro de la misma categoría o de distintas categorías. En la figura 3 se muestran las categorías y los reportes por año. La técnica más reportada es la clasificación, utilizada en 95 ocasiones. Este número representa el producto de cada algoritmo reportado y la cantidad de ocasiones que utilizado en los artículos analizados.

El año 2017 es el que en más ocasiones se presenta la utilización de algoritmos dentro de la categoría *Clasificación*, con un total de 25. Del total de algoritmos distribuidos entre todas las categorías, el más frecuente fue SVM con 19 reportes, seguido por ANN con 14 reportes y DT con 11 reportes, el primero y el tercero pertenecientes a la técnica *Clasificación* y ANN perteneciente a la técnica *Redes Neuronales*, tal como se observa en la figura 4. SVM fue particularmente utilizado en 2016, con 5 referencias; además, muestra su primer reporte en 2008 y 3 reportes en 2011 y 2018, lo que evidencia que ha sido una técnica ampliamente usada; mientras que ANN y DT muestran una tendencia creciente, especialmente de 2015 a 2017 , año en que tuvieron 4 reportes cada una. Se destaca además que 34 algoritmos se reportan solo una vez, además 5 herramientas corresponden a propuestas de *frameworks* y hay 5 desarrollos que no siguen una técnica en particular (desarrollos propios).

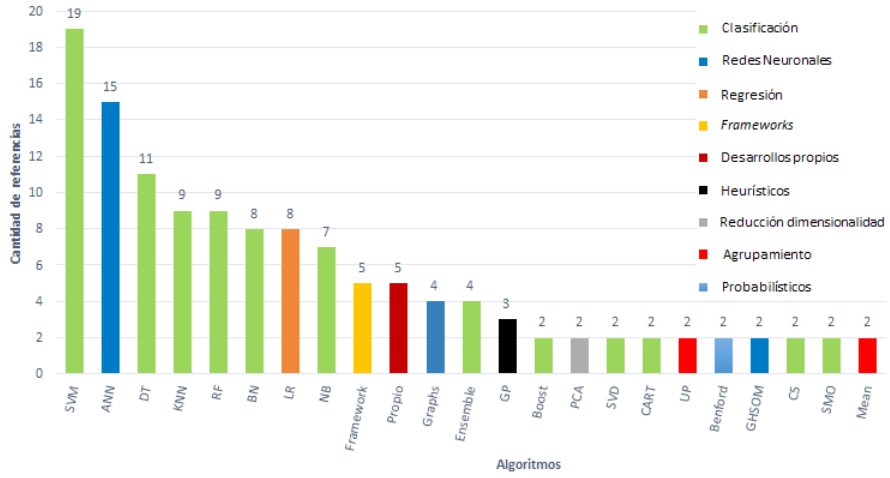

Figura 4 – Algoritmos reportados para la detección de fraudes en estados financieros.

5.2. Evaluación de la efectividad de las técnicas de minería de datos y de aprendizaje automático utilizadas en la detección de fraudes en estados financieros (RQ2)

Con respecto a las métricas utilizadas para evaluar la eficacia de las técnicas implementadas, la métrica llamada *accuracy*, (exactitud), es la más utilizada. Esta se define como el número total de predicciones correctas sobre el total de registros analizados (Seemakurthi y cols., 2015).

En la tabla 2 se muestra el listado de las métricas utilizadas para medir la eficacia de los algoritmos. Se listaron aquellas reportadas en al menos dos artículos. Puede observarse

que la exactitud es ampliamente utilizada, seguida por la especificidad y la tasa de falsos positivos. A pesar de que las tasas de falsos positivos y negativos y de verdaderos positivos y negativos son necesarias para calcular la exactitud, en algunos artículos solo se calcularon aisladamente, sin llegar a calcular la exactitud.

Es importante notar que en algunos casos se utilizan métricas con un mismo nombre, pero con fórmulas distintas: Pradeep y cols. (2015) definen la sensitividad como *TP / (TP + FN)*, mientras Minhas y Hussain (2016) la definen simplemente como *TP*, y Moepya y cols. (2016) la formulan como *TP / (TN + FN)*.

En cuanto a la medición de la eficiencia se encontraron referencias a 6 métricas relacionadas con el desempeño computacional de las herramientas: *speed*, con 2 reportes (S183 y S184), *velocity* (S10), *scalability* (S257), *computational time* (S108), *computational cost* (S10) y *execution time* (S264), con un reporte cada una.

Solamente uno de los estudios analizados reporta claramente una evaluación de la eficiencia: L. Yao y Wang (L. Yao y Wang, 2015) evaluaron la escalabilidad de un algoritmo de detección de valores atípicos (*outlier detection*). Probaron el algoritmo con 4 conjuntos de datos: 1.09 MB, 1.65 MB, 3.25 MB y 5.30 MB, con los cuales se determinó que la aplicación era escalable, al obtener resultados positivos, sin que el tamaño del conjunto afectara significativamente el desempeño.

Métrica	Referencia	Cantidad
Accuracy	S10, S3, S44, S47, S61, S66, S79, S99, S112, S126, S130, S131, S133, S153, S161, S162, S1175, S176, S187, S188, S193, S220, S221, S224, S235, S282, S297, S300	30
Specificity	S66, S108, S126, S130, S168, S176, S188, S193, S221, S282	10
False positive rate	S15, S61, S79, S133, S162, S220, S221, S282, S296, S302	10
Precision	S8, S66, S162, S187, S188, S221, S239, S271, S282	9
Sensitivity	S66, S108, S126, S168, S176, S188, S193, S221, S282	9
False negative rate (FN)	S15, S61, S79, S133, S162, S220, S296, S302	8
Recall	S18, S66, S162, S187, S239, S271	6
F-Measure	S66, S220, S221, S282, S301	5
F1-Score	S161, S162, S239, S271	4
Classes discovered	S181, S230, S247	3
Motyka distance	S215, S297	2
True negative rate (TN)	S155, S220	2
Dice distance	S215, S297	2
Area Under Curve	S126, S161	2
Error-rate	S188, S220	2

Métrica	Referencia	Cantidad
Squared Euclidean distance	S215, S297	2
Kappa	S176, S193	2
Lorentzian distance	S215, S297	2
True positive rate (TP)	S155, S220	2

Tabla 2 – Métricas utilizadas para evaluar la eficacia.

6. Conclusiones

Se realizó un mapeo sistemático de literatura con el que se identificaron las técnicas de minería de datos y aprendizaje automático utilizadas para la detección de fraudes en estados financieros. A partir 67 artículos que datan de 2007 a 2019, se extrajeron los algoritmos reportados y se clasificaron en 10 categorías, correspondientes a técnicas distintas.

Se extrajeron también las métricas utilizadas para medir la efectividad de los algoritmos, desde su eficacia y su eficiencia. Se encontró que en 2015 hubo un repunte en la cantidad de investigaciones y que la técnica clasificación es la más reportada, y dentro de ella, las máquinas de soporte vectorial (SVM) son el algoritmo más utilizado, reportado en 19 estudios, seguido por las redes neuronales artificiales (ANN), con 15 reportes y los árboles de decisión (DT), con 11 reportes.

La exactitud (*accuracy*) es la métrica de eficacia más utilizada. Se encontraron valores de exactitud que rondan entre el 70% y el 99.9% en implementaciones de técnicas de clasificación, específicamente con SVM, que fue el algoritmo más reportado, por lo que puede observarse un cambio con lo obtenido por Albashrawi (2016), quien determinó que, para 2015, SVM ocupaba el tercer lugar en tendencia de uso y Duhart y Hernández-Gress (2016), que localizaron las redes bayesianas, ANN y DT en las primeras posiciones.

De las 6 métricas de eficiencia identificadas en los artículos, 4 están enfocadas en el tiempo que toman las técnicas implementadas en arrojar un resultado (*speed*, *velocity*, *execution time* y *computational time*), una métrica midió el costo computacional (*computational cost*) y una contempló ambos aspectos (*scalability*).

Se requiere una apertura de la industria financiera para proveer conjuntos de datos de casos reales que permitan crear herramientas que, incluso, podrían eventualmente hacer detecciones de fraude en tiempo real. Los resultados obtenidos permiten contar con una referencia para la elección del enfoque más apropiado en la implementación de sistemas para la detección de fraudes en estados financieros, por ejemplo, en empresas y entidades de fiscalización gubernamentales. Como trabajo futuro se propone realizar mayor investigación sobre la eficiencia de los algoritmos, de manera que pueda hacerse mayor comparación de la velocidad o el costo computacional de implementarlos.

Referencias

Association of Certified Fraud Examiners, Inc. (2018). *Report To The Nations 2018. Global Study On Occupational Fraud And Abuse*. Descargado de https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

Afifah Rizki, A., Surjandari, I. y Aldiana Wayasti, R. (2017, 10). *Data mining application to detect financial fraud in indonesia's public companies*. En (p. 206-211). doi: 10.1109/ICSITech.2017.8257111

Albashrawi, M. (2016, 07). Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015. *Journal of Data Science*,14, 553-570.

Basili, V., Gianluigi, C. and Rombach, D. (1994). The goal question metric approach. *Encyclopedia of software engineering 1994*, pp. 528–532.

Blum, A., Hopcroft, J., y Kannan, R. (2015). Foundations of data science. Descargado de https://www.cs.cornell.edu/jeh/book.pdf

Duhart, B., y Hernández-Gress, N. (2016, 12). Review of the principal indicators and data science techniques used for the detection of financial fraud and money laundering. En (p. 1397-1398). doi: 10.1109/CSCI.2016.0267

Guerequeta, R., y Vallecillo, A. (2000). Técnicas de diseño de algoritmos. Descargado de: http://www.lcc.uma.es/~av/Libro/

Jan, C.-L., y Hsiao, D. (2018, 04). Detection of fraudulent financial statements using decision tree and artificial neural network. *ICIC Express Letters, Part B: Applications*, 9, 347-352.

Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical report, Ver. 2.3 EBSE Technical Report*.

Li, H., y Wong, M. L. (2015, 05). Financial fraud detection by using grammar-based multi-objective genetic programming with ensemble learning. doi: 10.1109/CEC.2015.7257014

Meenatkshi, R., y Sivaranjani. (2016, 01). Fraud detection in financial statement using data mining technique and performance analysis. 9, 407-413.

Minhas, S., y Hussain, A. (2016, 05). From spin to swindle: Identifying falsificationin financial text. *Cognitive Computation*, 8. doi: 10.1007/s12559-016-9413-9

Moepya, S., Akhoury, S., Nelwamondo, F., y Twala, B. (2016, 02). The role of imputation in detecting fraudulent financial reporting; 12, 333-356.

Ngai, E., Hu, Y., Wong, Y., Chen, Y., y Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and anacademic review of literature. *Decision Support Systems*, 50(3), 559 - 569. Descargado de: http://shorturl.at/nRS28. doi: https://doi.org/10.1016/j.dss.2010.08.006O.

Pai, M., McCulloch, M., Gorman, J.D., Pai, N.P., Enanoria, W.T., Kennedy, G.E., Tharyan, P., & Colford, J.M. (2004). Systematic reviews and meta-analyses: an illustrated, step-by-step guide. *The National medical journal of India,* 17 2, 86-95.

Petersen, K., Vakkalanka, S. and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, vol. 64, pp. 1–18, 2015.

Pradeep, G., Ravi, V., Nandan, K., L. Deekshatulu, B., Bose, I., y Aditya, A. (2015). Fraud detection in financial statements using evolutionary computation based rule miners. En (Vol. 8947, p. 239-250). doi: 10.1007/978-3-319-20294-5_21

Reurink, A. (2016, 05). Financial fraud: A literature review. *MPIfG Discussion Paper Series*,1 6. doi: 10.1111/joes.12294

Rizani, F., y Respati, N. (2018, 04). Factors influencing the presentation of fraudulent financial reporting in indonesia. *Journal of Advanced Research in Law and Economics*, 9, 254-264. doi: 10.14505/jarle.v9.1(31).31

Seemakurthi, P., Zhang, S., y Qi, Y. (2015, April). Detection of fraudulent financial reports with machine learning techniques. En *2015 Systems and information engineering design symposium* (p. 358-361). doi: 10.1109/SIEDS.2015.7117005

Shalev-Shwartz, B.-D. S., S. (2014). Understanding machine learning: From theory to algorithms. Descargado de: http://shorturl.at/cmwQ4

Song, X., y Ge, Y. (2012, 01). Detecting financial statement fraud: A comparative study using data mining methods. *International Review on Computers and Software*, 7, 1778-1783

West, J., Bhattacharya, M., y Islam, M. R. (2015, 10). Intelligent financial fraud detection practices: An investigation. doi: 10.1007/978-3-319-23802-9_16

Xiong, H., Lu, W., y Jiang, T. (2012, 12). Rare class analysis: Svms using local clustering and nearest neighbor. *Journal of Computational Information Systems*, 8, 9815-9822

Yao, J., Zhang, J., y Wang, L. (2018, 05). A financial statement fraud detectionmodel based on hybrid data mining methods. En (p. 57-61). doi: 10.1109/ICAIBD.2018.8396167

Yao, L., y Wang, Z. (2015, 09). Research on the algorithm of hadoop-based spatial-temporal outlier detection. En (p. 799-804). doi: 10.1109/IMCCC.2015.175

Young Moon, W., y Dong Kim, S. (2017, 10). Adaptive fraud detection framework for fintech based on machine learning. *Advanced Science Letters*, 23, 10167-10171. doi: 10.1166/asl.2017.10412