-APLICAÇÃO DE MACHINE LEARNING NA IDENTIFICAÇÃO DE FRAUDES FINANCEIRAS: UM ESTUDO DE CASO EM BASE DE DADOS DESBALANCEADA

Autor: João Daniel Temporin

Orientador: Prof. Maura Velho

RESUMO

A crescente complexidade das transações financeiras e o avanço das tecnologias digitais têm ampliado as oportunidades para práticas fraudulentas, tornando a detecção de fraudes um desafio estratégico para instituições financeiras. Este trabalho tem como objetivo aplicar técnicas de Machine Learning para identificar padrões suspeitos em uma base de dados financeira com alto desbalanceamento entre casos legítimos e fraudulentos. O estudo adota como metodologia a coleta e tratamento de dados, aplicação de técnicas de balanceamento como SMOTE e Random Under Sampling, e a implementação de modelos de classificação supervisionada, incluindo Regressão Logística, Random Forest e XGBoost. A avaliação dos modelos foi realizada por meio de métricas como precisão, revocação, F1-Score e AUC-ROC, priorizando a minimização de falsos negativos. Os resultados obtidos demonstraram que o modelo [inserir modelo], combinado com o balanceamento [inserir balanceamento], apresentou o melhor desempenho, atingindo [inserir percentual] de F1-Score e [inserir percentual] de AUC-ROC, evidenciando sua eficácia na detecção de fraudes. Conclui-se que a aplicação de algoritmos de aprendizado de máquina, quando aliada a estratégias adequadas de tratamento de dados desbalanceados, pode aprimorar significativamente a identificação de transações fraudulentas, contribuindo para a redução de perdas financeiras e o fortalecimento da segurança nas operações.

**Palavras-chave**: Machine Learning; Fraudes Financeiras; Detecção de Anomalias.

ABSTRACT

The increasing complexity of financial transactions and the advancement of digital technologies have expanded opportunities for fraudulent practices, making fraud detection a strategic challenge for financial institutions. This study aims to apply Machine Learning techniques to identify suspicious patterns in a financial dataset with a high imbalance between legitimate and fraudulent cases. The methodology involves data collection and preprocessing, the application of balancing techniques such as SMOTE and Random Under Sampling, and the implementation of supervised classification models, including Logistic Regression, Random Forest, and XGBoost. Model evaluation was conducted using metrics such as precision, recall, F1-Score, and AUC-ROC, with an emphasis on minimizing false negatives. The results show that the [inserir modelo] model, combined with [inserir balanceamento] balancing, achieved the best performance, reaching [inserir percentual] F1-Score and [inserir percentual] AUC-ROC, demonstrating its effectiveness in fraud detection. It is concluded that the application of machine learning algorithms, when combined with appropriate strategies for handling imbalanced data, can significantly enhance the identification of fraudulent transactions, contributing to financial loss reduction and increased security in operations.

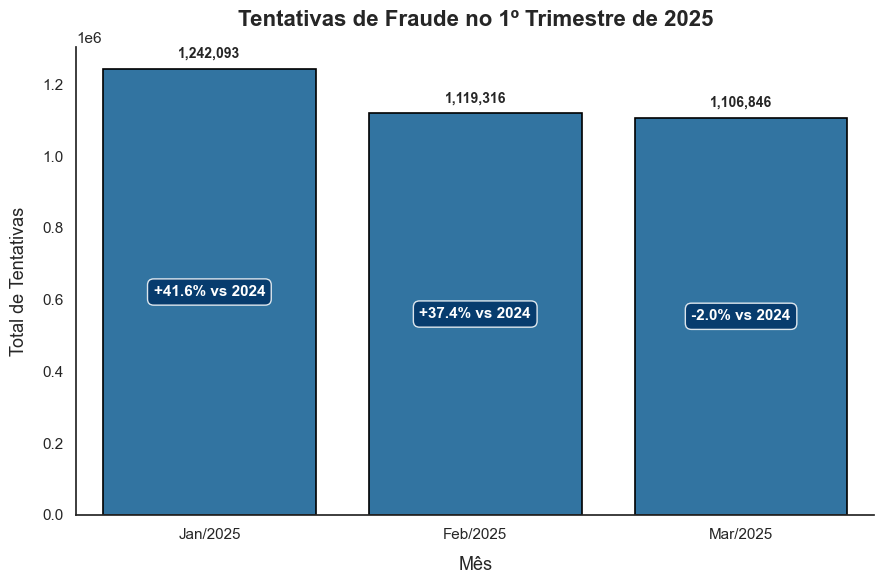
**Key-words:** Machine Learning; Financial Fraud; Anomaly Detection.

# Introdução

O avanço das tecnologias digitais e a popularização de serviços financeiros online transformaram profundamente a forma como transações monetárias são realizadas, trazendo benefícios em agilidade, conveniência e alcance global. No entanto, esse cenário também ampliou o espaço para a ocorrência de fraudes financeiras, que geram prejuízos bilionários todos os anos e representam um desafio estratégico para instituições financeiras e empresas de diversos setores. Segundo a *Association of Certified Fraud Examiners* (ACFE, 2024), organizações no mundo perdem, em média, 5% de sua receita anual devido a atividades fraudulentas, valor estimado em cerca de 4,7 trilhões de dólares.

No Brasil, o problema é igualmente preocupante. Um estudo realizado pela *Serasa Experian* (2025) estimou em mais de 3,4 milhões de tentativas de fraude no primeiro trimestre de 2025. O volume representa uma média de 1 tentativa a cada 2,2 segundos em todo o território nacional, e as áreas mais afetadas são Bancos/Cartões e Serviços, representando 54,0% e 31,9% do total das transações fraudulentas, respectivamente. Essa realidade reforça a necessidade de soluções mais sofisticadas para detecção e prevenção de fraudes.

**Figura 1** – Tentativas de fraude no 1º trimestre de 2025 por mês, com variação percentual em relação ao mesmo período de 2024.



**Fonte**: Serasa Experian, 2025.

Métodos tradicionais de detecção baseados em regras fixas apresentam limitações frente ao grande volume de dados e à diversidade dos padrões fraudulentos. Nesse contexto, as técnicas de **Machine Learning** têm se mostrado promissoras, pois permitem analisar grandes conjuntos de dados, aprender padrões e se adaptar a novos cenários (Ngai et al., 2011). Modelos como *Random Forest*, *Regressão Logística* e *Extreme Gradient Boosting* (XGBoost) têm obtido bons resultados em estudos recentes, especialmente quando combinados com estratégias de pré-processamento adequadas (Dal Pozzolo et al., 2015; Carcillo et al., 2019).

Entretanto, um desafio recorrente nesse tipo de aplicação é o **desbalanceamento das bases de dados**, situação em que o número de registros legítimos é muito superior ao número de registros fraudulentos. Esse desequilíbrio tende a levar os modelos a priorizar a classe majoritária, reduzindo a capacidade de identificar casos positivos raros (Japkowicz & Stephen, 2002). Para contornar esse problema, técnicas como o *Synthetic Minority Oversampling Technique* (SMOTE) e o *Random Under Sampling* têm sido amplamente utilizadas para equilibrar a proporção entre as classes e melhorar a performance dos algoritmos (Chawla et al., 2002).

Diante desse cenário, este trabalho se orienta pela seguinte questão norteadora: **Como a aplicação de algoritmos de Machine Learning, aliada a técnicas de tratamento de dados desbalanceados, pode contribuir para a identificação eficaz de fraudes financeiras?**

O objetivo geral é investigar e implementar modelos de aprendizado de máquina capazes de identificar transações fraudulentas de forma eficiente, mesmo em contextos de desbalanceamento de dados. Entre os objetivos específicos, destacam-se: (i) realizar a coleta, limpeza e pré-processamento da base de dados; (ii) aplicar e comparar diferentes técnicas de balanceamento; (iii) implementar múltiplos algoritmos de classificação supervisionada; e (iv) avaliar os resultados utilizando métricas como precisão (*precision*), revocação (*recall*), F1-Score e AUC-ROC, priorizando a redução de falsos negativos.

A justificativa teórica baseia-se na relevância de pesquisas voltadas à aplicação de métodos inteligentes e adaptativos para detecção de anomalias, tema amplamente explorado na literatura científica (Ngai et al., 2011; Dal Pozzolo et al., 2015; Carcillo et al., 2019). A justificativa prática está relacionada à necessidade crescente das instituições de mitigar riscos financeiros, aumentar a segurança das operações e preservar a confiança dos clientes. Ao unir a aplicação de conceitos de Machine Learning e estratégias de tratamento de dados desbalanceados, este estudo pretende contribuir para o desenvolvimento de soluções mais eficazes e aplicáveis a cenários reais.

# REFERENCIAL TEÓRICO E EMPÍRICO

**2.1 Referencial Teórico**

A literatura sobre detecção de fraudes financeiras destaca o **desbalanceamento de dados** como obstáculo relevante à performance preditiva, uma vez que modelos tendem a se favorecer pela classe majoritária (Japkowicz & Stephen, 2002). Técnicas como **SMOTE** e **Random Under Sampling** surgem como soluções eficazes para mitigar esse viés (Chawla et al., 2002).

Além disso, Ngai et al. (2011) categorizam métodos de *Machine Learning* aplicáveis à detecção de fraudes, apontando sua **capacidade adaptativa e generalização** como vantagens frente a modelos baseados em regras. Estudos como os de Dal Pozzolo et al. (2015) demonstram resultados superiores com o uso desses algoritmos, especialmente quando incluem uma etapa de balanceamento eficaz. Por fim, Carcillo et al. (2019) reforçam a importância de métricas como *recall* e F1-Score, por serem mais sensíveis à detecção de fraudes em contextos desbalanceados.

**2.2 Referencial Empírico**

Carcillo et al. (2019) aplicaram modelos híbridos em transações de cartão de crédito, mostrando uma sensibilidade aprimorada na identificação de fraudes. Dal Pozzolo et al. (2015) também evidenciam que reamostragem aliada à calibração de probabilidades melhora significativamente o desempenho dos modelos em bases desbalanceadas.

No cenário nacional, Souza & Bordin Jr. (2023) publicaram na *Revista Brasileira de Computação Aplicada* um tutorial prático sobre detecção de transações fraudulentas via cartão de crédito com *Machine Learning*, descrevendo técnicas clássicas, híbridas e estratégias de balanceamento de dados.

Brum & Reis (2025), em revisão sistemática publicada na *Revista CRC-SC*, identificaram que entre 2019 e 2024, as técnicas de **controle interno, *Machine Learning* e tecnologias/software** foram as mais pesquisadas no combate a fraudes financeiras.

Além disso, pesquisa da UNESP desenvolveu um sistema de detecção de fraudes que incorporou **engenharia de características e análise temporal**, evidenciando que essas etapas são fundamentais para aprimorar o desempenho dos modelos, sobretudo em ambientes reais com alto volume transacional.

**2.3 Síntese Crítica**

A base teórica e empírica revisitada demonstra que:  
(i) o **desbalanceamento é um problema central**, exigindo soluções específicas de balanceamento e ajustes metodológicos;  
(ii) **Modelos de *Machine Learning***, quando combinados com engenharia de dados avançada, revelam-se mais eficazes que abordagens tradicionais;  
(iii) a literatura nacional compartilha dessas conclusões e confirma a eficácia prática de tais métodos em nossos contextos institucionais.

Com isso, este estudo se posiciona em consonância com as principais tendências: aplicará e comparará modelos supervisionados, combinando técnicas de balanceamento e engenharia de dados, para identificar fraudes financeiras em base desbalanceadacontribuindo tanto academicamente quanto na prática para a mitigação de riscos no setor financeiro.

## **3 PROCEDIMENTOS METODOLÓGICOS**

A metodologia adotada neste trabalho busca assegurar a consistência científica necessária para responder à questão norteadora da pesquisa: como a aplicação de algoritmos de Machine Learning, aliada a técnicas de tratamento de dados desbalanceados, pode contribuir para a identificação eficaz de fraudes financeiras. Para tanto, o estudo foi estruturado em quatro etapas principais: (i) coleta e pré-processamento dos dados; (ii) tratamento do desbalanceamento da base; (iii) implementação dos modelos supervisionados; e (iv) avaliação dos resultados obtidos.

### ****3.1 Coleta e Pré-processamento dos Dados****

A base de dados utilizada foi disponibilizada pelo Machine Learning Group da Universidade Livre de Bruxelas (ULB) por meio da plataforma Kaggle, sob o título Credit Card Fraud Detection Dataset. Trata-se de um conjunto amplamente referenciado em pesquisas científicas na área de detecção de fraudes (DAL POZZOLO et al., 2015; CARCILLO et al., 2019).

O dataset é composto por **284.807 transações financeiras realizadas por titulares europeus de cartão de crédito ao longo de dois dias**, das quais **492 correspondem a fraudes** e **284.315 a transações legítimas**. Essa proporção evidencia o elevado grau de desbalanceamento (0,172% de fraudes). As variáveis presentes no conjunto são todas numéricas e incluem:

* **Time**: intervalo em segundos entre cada transação e a primeira transação registrada;
* **V1 a V28**: 28 variáveis resultantes de transformação por Principal Component Analysis (PCA), uma técnica de anonimização de atributos originais sensíveis;
* **Amount**: valor monetário da transação;
* **Class**: variável-alvo binária, onde **0** representa uma transação legítima e **1** representa uma fraude.

### ****3.2 Tratamento do Desbalanceamento da Base****

Um dos principais desafios encontrados em bases de dados voltadas à detecção de fraudes refere-se ao forte desbalanceamento entre as classes. Em geral, as transações legítimas superam em milhares de vezes as transações fraudulentas, o que compromete a capacidade dos modelos em reconhecer a classe minoritária (JAPKOWICZ; STEPHEN, 2002).

Para mitigar esse problema, foram aplicadas duas técnicas complementares de reamostragem: o Synthetic Minority Oversampling Technique (SMOTE) e o Random Under Sampling. Enquanto o primeiro atua gerando exemplos sintéticos da classe minoritária a partir das instâncias existentes (CHAWLA et al., 2002), o segundo reduz aleatoriamente instâncias da classe majoritária. A utilização combinada de ambas as técnicas permitiu equilibrar a base, aumentando a sensibilidade dos algoritmos sem comprometer excessivamente a representatividade da classe majoritária.

### ****3.3 Modelagem e Implementação dos Algoritmos****

Na etapa de modelagem, foram implementados três algoritmos de classificação supervisionada, selecionados por sua relevância na literatura e adequação ao problema em estudo: Regressão Logística, Random Forest e XGBoost.

A Regressão Logística foi utilizada como modelo de referência, dada sua ampla aplicação em problemas de classificação binária e sua facilidade de interpretação. O Random Forest foi empregado por sua robustez frente a bases complexas e pela capacidade de lidar com variáveis de diferentes naturezas (NGAI et al., 2011). Já o XGBoost foi escolhido por representar uma das abordagens mais eficientes em competições de ciência de dados, sendo reconhecido por sua precisão e estabilidade em cenários de alta dimensionalidade (DAL POZZOLO et al., 2015; CARCILLO et al., 2019).

Os algoritmos foram treinados em subconjuntos de dados obtidos a partir da divisão da base em treino e teste, além da aplicação da técnica de validação cruzada k-fold. Essa estratégia teve como objetivo reduzir riscos de sobreajuste (overfitting) e garantir maior confiabilidade nos resultados.

### ****3.4 Avaliação de Desempenho****

A análise do desempenho dos modelos foi realizada por meio de métricas apropriadas a bases desbalanceadas, entre as quais se destacam: precisão (precision), revocação (recall), F1-Score e a área sob a curva ROC (AUC-ROC).

A ênfase foi dada especialmente ao recall e ao F1-Score, uma vez que, no contexto de fraudes financeiras, a ocorrência de **falsos negativos** (fraudes não identificadas) representa prejuízos mais significativos do que os falsos positivos (transações legítimas classificadas incorretamente como fraude). Esse enfoque está em consonância com a literatura, que aponta a necessidade de privilegiar métricas sensíveis à classe minoritária para problemas de segurança financeira (CARCILLO et al., 2019).

### ****3.5 Síntese Metodológica****

Em síntese, a metodologia seguiu um delineamento estruturado em quatro etapas: preparação e pré-processamento dos dados; aplicação de técnicas de balanceamento; implementação de modelos supervisionados; e avaliação por métricas adequadas. Tal abordagem permitiu não apenas comparar o desempenho de diferentes algoritmos, mas também verificar como a aplicação de técnicas de reamostragem impacta diretamente na qualidade da detecção de fraudes. Dessa forma, os procedimentos adotados asseguram robustez ao estudo e oferecem evidências empíricas sobre a contribuição das técnicas de Machine Learning no combate a fraudes financeiras em bases desbalanceadas

**REFERÊNCIAS**

BRUM, Mayara; REIS, Gustavo. **Detecção e prevenção de fraudes financeiras: uma revisão sistemática da literatura (2019–2024)**. Revista CRC-SC, v. 6, n. 2, p. 1–20, 2025. Disponível em: <https://revista.crcsc.org.br/index.php/CRCSC/article/view/3538>. Acesso em: 20 ago. 2025.

CARCILLO, Fabrizio et al. **Combining unsupervised and supervised learning in credit card fraud detection**. Information Sciences, v. 557, p. 317-331, 2019.

CHAWLA, Nitesh V. et al. **SMOTE: Synthetic Minority Over-sampling Technique**. Journal of Artificial Intelligence Research, v. 16, p. 321-357, 2002. DOI: <https://doi.org/10.1613/jair.953>.

DAL POZZOLO, Andrea et al. **Calibrating Probability with Undersampling for Unbalanced Classification**. IEEE Symposium Series on Computational Intelligence, 2015.

JAPKOWICZ, Nathalie; STEPHEN, Shaju. **The class imbalance problem: A systematic study**. Intelligent Data Analysis, v. 6, n. 5, p. 429-449, 2002. DOI: <https://doi.org/10.3233/IDA-2002-6504>.

NGAI, Eric W. T. et al. **The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature**. Decision Support Systems, v. 50, n. 3, p. 559-569, 2011. DOI: <https://doi.org/10.1016/j.dss.2010.08.006>.

SERASA EXPERIAN. **Indicador de Tentativas de Fraude**. Serasa Experian, 2025. Disponível em: <https://www.serasaexperian.com.br/>. Acesso em: 12 ago. 2025.

SOUZA, Diogo Ribeiro; BORDIN JUNIOR, Ricardo. **Detecção de fraude de cartão de crédito por meio de algoritmos de aprendizado de máquina: um tutorial**. Revista Brasileira de Computação Aplicada (RBCA), v. 15, n. 1, p. 92–110, 2023. DOI: <https://doi.org/10.5335/rbca.v15i1.14051>.

UNIVERSIDADE ESTADUAL PAULISTA (UNESP). **Detecção de fraudes financeiras com técnicas de machine learning**. Repositório Institucional UNESP, 2022. Disponível em: <https://repositorio.unesp.br/entities/publication/efd6dd5f-1bca-409c-911c-ee79f6b00ad4>. Acesso em: 20 ago. 2025.

# APÊNDICE A – TÍTULO DO APÊNDICE

**APÊNDICE B – TÍTULO DO APÊNDICE**

# ANEXO A – tÍTULO DO ANEXO

# ANEXO B – tÍTULO DO ANEXO