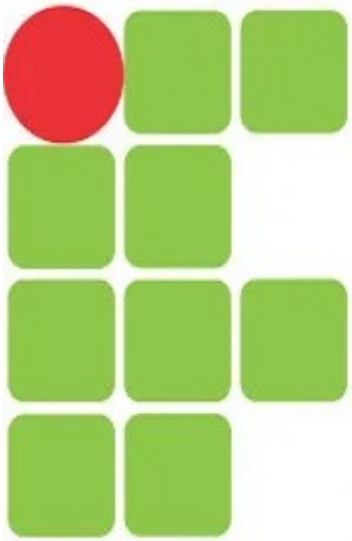


Instituto Federal da Paraíba

Conceito e técnicas de aprendizado de máquina e modelos preditivos

Detecção de Fraudes em Transações Bancárias com Aprendizado de Máquina

João Paulo Bianchi Pereira

Setembro 2025

1. Introdução

Com o crescimento acelerado das transações financeiras digitais, especialmente via PIX, aumentou também a incidência de fraudes e anomalias que desafiam a segurança dos sistemas bancários. A detecção precoce dessas irregularidades é essencial para proteger usuários e instituições, exigindo soluções inteligentes e automatizadas.

Este projeto tem como objetivo aplicar técnicas de aprendizado de máquina supervisionado para classificar transações bancárias como legítimas ou anômalas, utilizando algoritmos como Random Forest e AdaBoostM1 com J48, implementados na plataforma Weka. Ambos os modelos foram testados e comparados quanto ao desempenho, sendo o AdaBoostM1 selecionado como solução final por apresentar maior eficácia na detecção de fraudes.

A análise foi conduzida sobre um conjunto de dados contendo 10.000 registros de transações rotuladas quanto à presença de anomalias. Seguindo a metodologia CRISP-DM, o trabalho foi estruturado em etapas que incluem o entendimento do negócio, exploração e preparação dos dados, modelagem, avaliação e interpretação dos resultados. Ao final, foi realizada uma análise das métricas de desempenho, como acurácia, precisão, recall e F1-score, com o objetivo de validar a eficácia dos modelos testados e justificar a escolha do algoritmo final.

2. Entendimento do negócio

O presente trabalho tem como objetivo aplicar técnicas de aprendizado de máquina supervisionado para classificar transações bancárias como legítimas ou anômalas, com base em atributos como valor da transação, horário, chave PIX utilizada, instituições envolvidas, entre outros. A tarefa é de classificação binária, onde o modelo prevê se uma transação apresenta ou não características suspeitas.

A variável alvo do projeto é o atributo “Anomalia”, que indica se a transação é considerada suspeita (sim) ou não (não). A correta identificação de transações anômalas é essencial para a segurança das instituições financeiras, pois permite a detecção precoce de possíveis fraudes e a adoção de medidas preventivas, como bloqueios automáticos ou investigações internas.

Decisões importantes dependem dessa previsão. Transações classificadas como anômalas podem ser retidas para análise, enquanto transações legítimas devem ser processadas normalmente, garantindo agilidade e confiança no sistema. Uma previsão

incorreta pode gerar impactos significativos: falsos positivos (transações legítimas classificadas como suspeitas) podem causar transtornos aos clientes e sobrecarga operacional; já falsos negativos (fraudes não detectadas) representam riscos financeiros diretos e danos à reputação da instituição. A base de dados utilizada contém 10.000 registros de transações via PIX, previamente rotuladas quanto à presença ou ausência de anomalias. Para lidar com o desbalanceamento entre classes, foi aplicada a técnica SMOTE, ampliando a representatividade da classe “sim” e permitindo que os modelos aprendam padrões mais relevantes para a detecção de fraudes.

3. Entendimento dos dados

Inicialmente, foi realizada uma análise exploratória para compreender a estrutura e a qualidade dos dados. Os atributos foram classificados entre numéricos (como o valor da transação) e categóricos ou nominais (como o tipo de chave, bancos envolvidos e o campo “Anomalia”). Também foram identificados campos do tipo string, como CPF/CNPJ e descrição, que exigem tratamento específico para uso em algoritmos de aprendizado de máquina.

Durante a exploração, foram verificados:

- Valores ausentes: Não foram encontrados valores ausentes nos dados, o que elimina a necessidade de imputação ou exclusão de registros.
- Outliers: Os valores das transações variam entre R$0,00 e R$5.000,00. Após análise estatística, não foram identificados outliers significativos dentro desse intervalo.
- Distribuições: Foram utilizados histogramas e boxplots para visualizar a distribuição dos valores numéricos, como o valor das transações, e a frequência das categorias nominais, como os tipos de chave PIX utilizadas.

Para essa etapa, foi utilizado o software Jamovi, que permitiu realizar análises estatísticas descritivas e gerar os gráficos necessários, conforme representados nas tabelas e gráficos a seguir:

Tabela 1: Estatística descritiva dos valores das transferências

Estatística Descritiva	
	Valor
N	10000
Média	2505
Desvio padrão	1456
Mínimo	0.00
Máximo	5000

Gráfico 1: Histograma de densidade dos valores das transferências

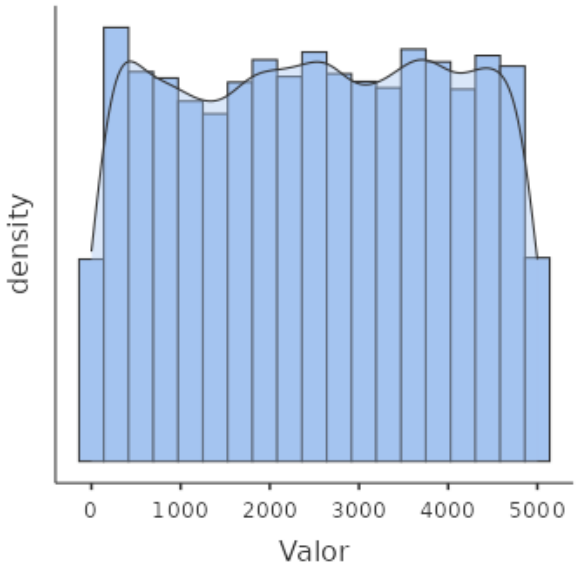


Gráfico 2: Gráfico boxplot de distribuição dos valores de transferência

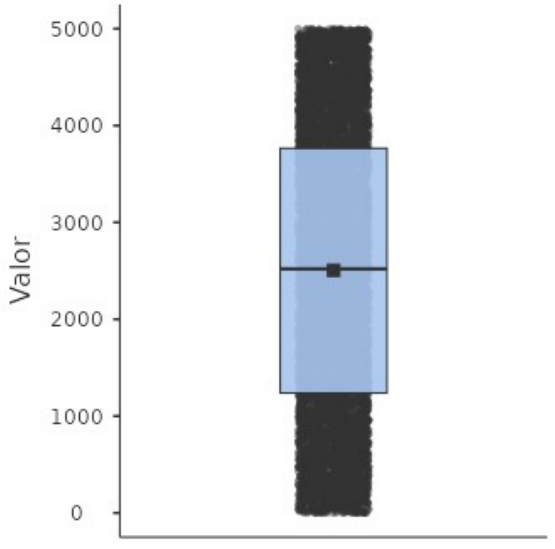


Tabela 2: Quantidade de transações por tipo de chave

Estatística Descritiva

	TipoChave	Valor
N	CNPJ	1919
	CPF	2032
	Chave Aleatória	2092
	E-mail	2009
	Telefone	1948

Gráfico 3: Histograma de densidade das transações por tipo de chave

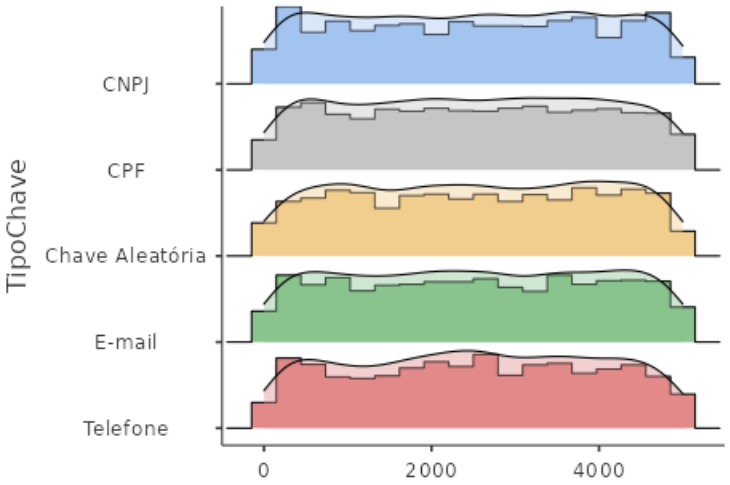
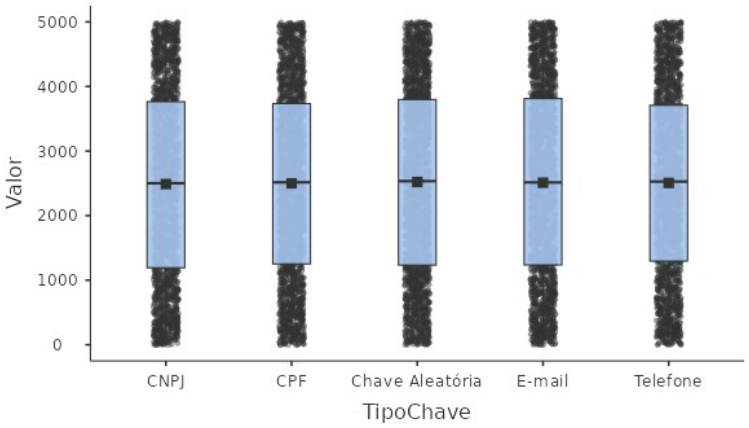


Gráfico 4: Gráfico boxplot demonstrando a distribuição dos dados por tipo de chave



A análise exploratória revelou uma distribuição relativamente uniforme tanto nos valores das transferências quanto na quantidade de transações por tipo de chave PIX. Observou-se que os dados referentes aos valores das transações e aos tipos de chave não apresentam outliers significativos.

Em relação às anomalias, identificou-se que, entre as 10.000 transações analisadas, apenas 100 foram classificadas como anômalas, representando 1% do total. Os gráficos apresentados a seguir, ilustram a densidade e a distribuição das transações anômalas em relação aos valores financeiros envolvidos. Embora os valores dessas transações estejam dispersos ao longo do intervalo analisado, observa-se uma tendência de concentração em faixas mais altas, sugerindo que transações de maior valor podem estar mais associadas a comportamentos suspeitos.

Gráfico 5: Densidade dos dados anômalos

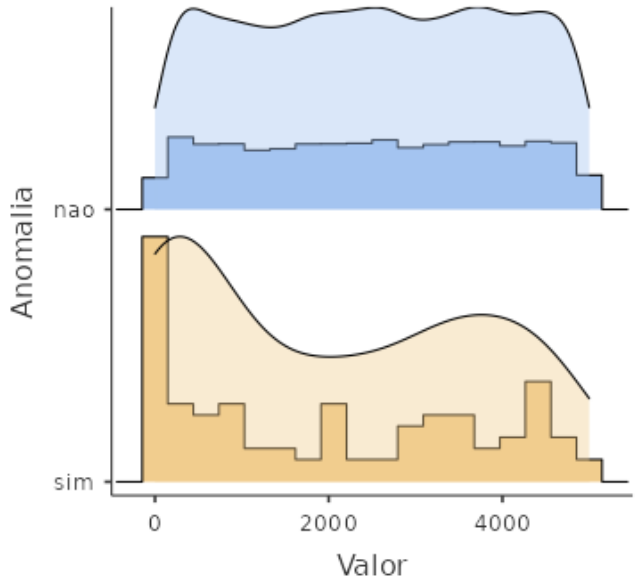
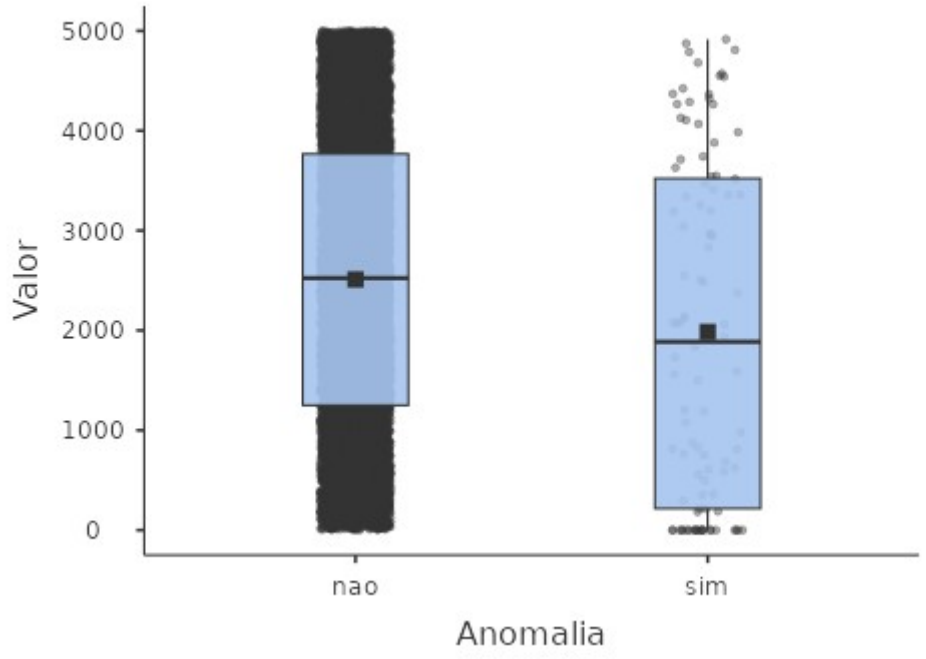


Gráfico 6: Distribuição dos valores de transferências anômalas



Diante do forte desbalanceamento entre classes, a etapa seguinte envolveu o uso da técnica SMOTE, com o objetivo de gerar exemplos sintéticos da classe minoritária e permitir que os modelos de aprendizado de máquina captassem padrões mais representativos para a detecção de fraudes.

4. Preparação dos dados

Após a etapa de entendimento e análise exploratória, foi realizada a preparação dos dados com o objetivo de torná-los adequados para a aplicação dos algoritmos de aprendizado de máquina.

Como não foram identificados valores ausentes na base, não foi necessário realizar remoção de registros. Os dados estavam completos, o que facilitou o processo de limpeza.

Em relação à transformação dos dados, foram realizadas as seguintes etapas:

- Codificação de variáveis categóricas: O atributo “tipo de chave PIX (TipoChave)”, foi convertido para formato numérico por meio de codificação nominal, permitindo que os algoritmos interpretassem essas informações corretamente.
- Normalização dos atributos numéricos: o atributo “Valor” foi normalizado para garantir que sua escala não influenciasse indevidamente o desempenho do algoritmo utilizando o método Min-Max Scaling.
- Padronização de categorias: nomes de instituições e tipos de chave foram revisados para evitar duplicações causadas por variações de escrita ou formatação.
- Remoção de atributos irrelevantes: Foi realizado um ranqueamento ranqueamento por ganho de informação (InfoGain) disponível no Weka. Essa técnica permitiu identificar quais variáveis contribuem de forma mais significativa para a classificação da variável alvo. A partir dessa análise, foram excluídos os atributos que apresentaram ganho de informação inferior a 0,01, por serem considerados irrelevantes para o modelo. Campos como moedas, IDs das transações, números de agências e contas foram excluídos da modelagem.

Devido ao forte desbalanceamento entre as classes — com apenas 1% das transações classificadas como anômalas — foi aplicada a técnica SMOTE (Synthetic Minority Over-

sampling Technique). Essa abordagem gerou exemplos sintéticos da classe minoritária (“sim”), aumentando sua representatividade no conjunto de dados e permitindo que os modelos aprendessem padrões mais relevantes para a detecção de anomalias.

Por fim, a avaliação do modelo foi realizada por meio de validação cruzada estratificada (10-fold), garantindo maior confiabilidade nos resultados e evitando viés decorrente de divisões fixas entre treino e teste.

5. Modelagem

Com os dados devidamente preparados, foi iniciada a etapa de modelagem. O objetivo principal foi construir um modelo de aprendizado supervisionado capaz de classificar transações bancárias como legítimas ou anômalas. Para isso, foram testados diferentes algoritmos e configurações, incluindo Random Forest e AdaBoostM1 com J48 como classificador base.

Durante o processo de experimentação, foram avaliadas variações do algoritmo J48 (implementação da árvore de decisão baseada no C4.5), com e sem poda, além de ajustes nos parâmetros de divisão mínima de instâncias por folha. O Random Forest inicialmente apresentou resultados promissores em termos de acurácia, recall e F1-score, especialmente após o balanceamento da base com a técnica SMOTE.

No entanto, após ajustar parâmetros no AdaBoostM1 — como aumento do número de iterações, ativação de reamostragem e normalização dos dados — observou-se um desempenho superior na detecção da classe minoritária. O modelo final, baseado em AdaBoostM1 com J48, alcançou acurácia de 99,43%, recall de 94,1% para a classe “sim” e F1-score de 0,968, superando os resultados obtidos com o Random Forest.

Para garantir maior confiabilidade na avaliação dos modelos, foi utilizada a técnica de validação cruzada estratificada (10-fold), que permite testar o desempenho dos algoritmos em diferentes subconjuntos dos dados, reduzindo o risco de viés e aumentando a capacidade de generalização.

O desempenho dos modelos foi avaliado com base em métricas como acurácia, precisão, recall, F1-score, área sob a curva ROC (AUC), área sob a curva de precisão-recall (PRC) e coeficiente de correlação de Matthews (MCC), permitindo uma análise abrangente da capacidade preditiva e da sensibilidade à classe minoritária.

6. Avaliação

Após a construção dos modelos com os algoritmos Random Forest e AdaBoostM1 com J48, foi realizada a etapa de avaliação para verificar a eficácia de cada abordagem na classificação de transações bancárias como legítimas ou anômalas. A avaliação foi conduzida por meio de validação cruzada estratificada (10-fold), garantindo maior confiabilidade nos resultados e preservando a proporção entre classes em cada subdivisão dos dados.

Random Forest

O modelo Random Forest apresentou desempenho excepcional, com acurácia de 99,32% e estatística Kappa de 0,9579, indicando alta concordância entre as previsões e os rótulos reais. A análise por classe revelou recall de 92,6% para a classe “sim” (transações anômalas), com precisão de 100% e F1-score de 0,962. A área sob a curva ROC (AUC) foi de 0,990, e o coeficiente de correlação de Matthews (MCC) atingiu 0,959, reforçando a robustez do modelo.

A matriz de confusão mostra que o Random Forest classificou corretamente 9900 transações legítimas e 926 transações anômalas, com apenas 74 falsos negativos e nenhum falso positivo. Esse resultado demonstra que o modelo é capaz de detectar fraudes com alta confiabilidade, sem comprometer a experiência dos usuários legítimos.

AdaBoostM1 com J48

Após ajustes nos hiperparâmetros — incluindo 50 iterações, weight percentage de 100% e reamostragem ativada — o modelo AdaBoostM1 com J48 apresentou desempenho superior. A acurácia alcançada foi de 99,43%, com recall de 94,1% para a classe “sim” e F1-score de 0,968. A estatística Kappa foi de 0,965, e o MCC também atingiu 0,965, indicando equilíbrio e precisão na classificação.

A matriz de confusão mostra que o modelo classificou corretamente 9897 transações legítimas e 941 transações anômalas, com apenas 59 falsos negativos e 3 falsos positivos. Além disso, o modelo obteve AUC de 0,989 e PRC Area de 0,976, reforçando sua capacidade de distinguir padrões mesmo em cenários desbalanceados.

Comparação entre os modelos

Embora o Random Forest tenha apresentado excelente desempenho, o AdaBoostM1 com J48 superou em métricas-chave relacionadas à detecção da classe minoritária, especialmente no recall e na redução de falsos negativos. Essa diferença é crítica em

sistemas de detecção de fraudes, onde a sensibilidade à classe “sim” é essencial. Por esse motivo, o modelo AdaBoostM1 com J48 foi selecionado como solução final do projeto.

Tabela 3: Comparativo de resultados entre Random Forest e AdaBoost + J48

Métrica	Random Forest	AdaBoostM1 + J48 (final)
Acurácia	99,32%	**99,43%**
Kappa	0,9579	**0,965**
Recall (classe “sim”)	92,6%	**94,1%**
Precisão (classe “sim”)	100%	99,7%
F1-score (classe “sim”)	0,962	**0,968**
Falsos negativos (classe “sim”)	74	**59**
Falsos positivos (classe “não”)	0	3
MCC (coeficiente de Matthews)	0,959	**0,965**
Área sob a curva ROC (AUC)	0,990	0,989
Tempo de execução	~1,2s	**1,55s**

Figura 1: Resultados finais obtidos com AdaboostM1

```
Correctly Classified Instances       10838               99.4312 %
Incorrectly Classified Instances        62                0.5688 %
Kappa statistic                          0.965
Mean absolute error                      0.0057
Root mean squared error                  0.0753
Relative absolute error                  3.4152 %
Root relative squared error             26.0957 %
Total Number of Instances            10900

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1,000    0,059    0,994      1,000    0,997      0,965    0,976     0,995     nao
                 0,941    0,000    0,997      0,941    0,968      0,965    0,989     0,976     sim
Weighted Avg.    0,994    0,054    0,994      0,994    0,994      0,965    0,977     0,993

=== Confusion Matrix ===

    a    b   <-- classified as
 9897    3 |    a = nao
   59  941 |    b = sim
```

Figura 2: Resultados obtidos com Random Forest e fold 10

```
Correctly Classified Instances       10826               99.3211 %
Incorrectly Classified Instances        74                0.6789 %
Kappa statistic                          0.9579
Mean absolute error                      0.0858
Root mean squared error                  0.1087
Relative absolute error                 51.4565 %
Root relative squared error             37.6721 %
Total Number of Instances            10900

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1,000    0,074    0,993      1,000    0,996      0,959    0,990     0,998     nao
                 0,926    0,000    1,000      0,926    0,962      0,959    0,990     0,981     sim
Weighted Avg.    0,993    0,067    0,993      0,993    0,993      0,959    0,990     0,997

=== Confusion Matrix ===

    a    b   <-- classified as
 9900    0 |    a = nao
   74  926 |    b = sim
```

Figura 3: Resultados obtidos com Random Forest e divisão 70/30

```
Correctly Classified Instances        7571               99.2267 %
Incorrectly Classified Instances        59                0.7733 %
Kappa statistic                          0.9516
Mean absolute error                      0.0895
Root mean squared error                  0.1118
Relative absolute error                 53.5457 %
Root relative squared error             38.7783 %
Total Number of Instances            7630

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1,000    0,085    0,992      1,000    0,996      0,953    0,980     0,996     nao
                 0,915    0,000    1,000      0,915    0,956      0,953    0,980     0,965     sim
Weighted Avg.    0,992    0,077    0,992      0,992    0,992      0,953    0,980     0,993

=== Confusion Matrix ===

    a    b   <-- classified as
 6932    0 |    a = nao
   59  639 |    b = sim
```

Figura 4: Árvore de decisão J48 com parâmetro MinNumObj = 5 e poda (unpruned) desativada

```
Correctly Classified Instances        7494               98.2176 %
Incorrectly Classified Instances       136                1.7824 %
Kappa statistic                          0.8924
Mean absolute error                      0.0412
Root mean squared error                  0.1329
Relative absolute error                 24.6294 %
Root relative squared error             46.0999 %
Total Number of Instances            7630

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 0,991    0,102    0,990      0,991    0,990      0,892    0,957     0,992     nao
                 0,898    0,009    0,906      0,898    0,902      0,892    0,957     0,898     sim
Weighted Avg.    0,982    0,093    0,982      0,982    0,982      0,892    0,957     0,983

=== Confusion Matrix ===

    a    b   <-- classified as
 6867   65 |    a = nao
   71  627 |    b = sim
```

Figura 5: Árvore de decisão J48 com parâmetro MinNumObj = 5 e poda (unpruned) ativa

```
Correctly Classified Instances        7269               95.2687 %
Incorrectly Classified Instances       361                4.7313 %
Kappa statistic                          0.6291
Mean absolute error                      0.0828
Root mean squared error                  0.2075
Relative absolute error                 49.516  %
Root relative squared error             71.9733 %
Total Number of Instances             7630

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1,000    0,517    0,951      1,000    0,975      0,677    0,874     0,981     nao
                 0,483    0,000    1,000      0,483    0,651      0,677    0,874     0,625     sim
Weighted Avg.    0,953    0,470    0,955      0,953    0,945      0,677    0,874     0,949

=== Confusion Matrix ===

    a    b   <-- classified as
 6932    0 |    a = nao
  361  337 |    b = sim
```

7. Conclusão

O presente trabalho demonstrou a eficácia da aplicação de técnicas de aprendizado de máquina supervisionado na detecção de transações bancárias anômalas, com foco em operações realizadas via PIX. A partir de uma base de dados composta por 10.000 registros rotulados, foram realizadas etapas de análise exploratória, preparação dos dados, balanceamento com a técnica SMOTE e modelagem utilizando diferentes algoritmos, incluindo Random Forest e AdaBoostM1 com J48.

O modelo Random Forest apresentou desempenho excepcional, com acurácia de 99,32%, recall de 92,6% para a classe anômala e F1-score de 0,962, além de zero falsos positivos. Esses resultados evidenciam sua capacidade de identificar fraudes com alta precisão, sem comprometer a experiência dos usuários legítimos.

No entanto, após ajustes refinados no modelo AdaBoostM1 — como aumento do número de iterações, normalização dos dados e ativação de reamostragem — observou-se um desempenho superior. O modelo final alcançou acurácia de 99,43%, recall de 94,1% para a classe “sim” e F1-score de 0,968, além de apresentar maior equilíbrio entre precisão e sensibilidade. A aplicação da técnica SMOTE foi fundamental para superar o desafio do desbalanceamento entre classes, permitindo que os algoritmos aprendessem padrões relevantes da classe minoritária.

Dessa forma, o modelo AdaBoostM1 com J48 foi selecionado como solução final do projeto, por apresentar os melhores resultados na detecção de fraudes e maior robustez para aplicação prática em sistemas de monitoramento de transações financeiras.

8. Referências

BUENO, L. PIX banking transaction. Kaggle, 2025. Disponível em: https://www.kaggle.com/datasets/juniorbueno/pix-banking-transaction. Acesso em: 10 set. 2025.