

Centro Universitário Euro Americano (Unieuro)

Sistemas de Informação

Luan Medrado Moreira

Lucas Rego Da Silva

**Apresentação de Análise de Dados para Detecção**

**de Fraude Bancária**

Brasília

2024

Luan Medrado Moreira

Lucas Rego Da Silva

**Apresentação de Análise de Dados para Detecção**

**de Fraude Bancária**

Trabalho da disciplina de Projeto Integrador de Segurança da Informação

Orientador: Prof. Msc. Edward Lima M. de Melo

Brasília

2024

**Resumo**

A fraude bancária, caracterizada por transações não autorizadas pelos titulares dos cartões, representa um grande desafio para as instituições financeiras e seus clientes (Bolton & Hand, 2002). Com o aumento da digitalização dos serviços bancários, os casos de fraudes têm se tornado cada vez mais frequentes e complexos, o que requer técnicas avançadas de detecção e mitigação (Whitrow et al., 2009).

Neste contexto, a análise de dados surge como uma ferramenta essencial para a identificação e prevenção de fraudes (Kou et al., 2014). Esse projeto tem como objetivo a utilização de um modelo de machine learning para detectar fraudes bancárias em uma base de dados escolhida, que gera um relatório que será analisado, com a hipótese de que o modelo treinado pode identificar, de forma certeira, todas as ocorrências de fraude presentes. O estudo abrange etapas de higienização de dados, treinamento e teste do modelo, e a análise dos índices de fraudes encontradas. Por fim, é esperado que os resultados contribuam para a elaboração de estratégias melhores de diminuição de fraudes, gerando assim maior segurança e confiabilidade para os consumidores e instituições.

**Palavras-chave**: Fraude bancária, Machine Learning, Análise de dados, Identificação de fraudes, Higienização dos dados.

**Lista de Figuras**

Figura 1 - Apresentação de Dashboard com Índice de Fraudes Bancárias Encontradas No Ano de 2019 .......................................................15

Figura 2 - Apresentação de Dashboard com Índice de Clientes Sem Fraudes Encontradas no Ano de 2019 ..................................................16

[1. INTRODUÇÃO 5](#_Toc1555407818)

[1.1. Contextualização do Problema 6](#_Toc1858049440)

[1.2. Hipótese 6](#_Toc2044989643)

[1.3. Objetivo Geral 6](#_Toc552870823)

[2. JUSTIFICATIVA 7](#_Toc1854087408)

[2.1. Relevância do Tema 7](#_Toc1497028427)

[2.2. Impacto da Fraude Bancária nas Instituições Financeiras 7](#_Toc358430419)

[2.3. Importância da Detecção e Prevenção de Fraudes 8](#_Toc2011496344)

[3.REVISÃO DA LITERATURA 8](#_Toc1326358156)

[3.1. Conceitos de Fraude Bancária 8](#_Toc1475828117)

[3.2. Tipos de Fraude em Transações Eletrônicas 9](#_Toc1852458194)

[3.3. Machine Learning para Detecção de Fraudes 10](#_Toc799667671)

[4.METODOLOGIA 10](#_Toc79287823)

[4.1. Coleta de Dados 10](#_Toc175760819)

[4.1.1 Fonte dos Dados 11](#_Toc1905756084)

[4.1.2 Seleção de Variáveis 12](#_Toc1029925440)

[4.2 Higienização dos Dados 13](#_Toc385965588)

[4.2.1 Tratamento de Valores Ausentes: 13](#_Toc361258054)

[4.2.2 Conversão de Datas e Extração de Recursos Temporais: 13](#_Toc14817925)

[4.2.3 Codificação de Variáveis Categóricas: 14](#_Toc145792567)

[4.2.4 Remoção de Outliers: 14](#_Toc1161670365)

[4.2.5 Normalização dos Dados: 14](#_Toc1735229072)

[4.3 Modelagem e Treinamento 14](#_Toc83774882)

[4.3.1 Escolha do modelo de Machine Learning 15](#_Toc1729777052)

[4.3.2 Divisão da Base de Dados (treinamento e Teste) 15](#_Toc1681477309)

[4.4 Avaliação do Modelo 15](#_Toc1715991088)

[4.4.1 Métricas de Avaliação 15](#_Toc654129526)

[4.4.2 Validação 16](#_Toc388416000)

[5.ANÁLISE DE RESULTADOS 16](#_Toc1605823256)

[5.1 Identificação das Fraudes 16](#_Toc451315586)

[5.2 Identificação das Fraudes 16](#_Toc201616713)

[5.3 Apresentação de Dashboard 17](#_Toc1681808077)

[Figura 1 - Apresentação de Dashboard com Índice de Fraudes Bancárias Encontradas No Ano de 2019 17](#_Toc134772250)

[Figura 2 - Apresentação de Dashboard com Índice de Clientes Sem Fraudes Encontradas no Ano de 2019 17](#_Toc733628369)

[5.4 Apresentação dos Índices de Acerto 18](#_Toc1900187779)

[6.CONCLUSÃO 19](#_Toc101410330)

[6.1 Síntese dos Resultados 19](#_Toc60276523)

[6.2 Sugestões para Trabalhos Futuros 20](#_Toc1071730465)

[6.3 Contribuições para o Combate à Fraude Bancária 20](#_Toc941237153)

[GLOSSÁRIO 21](#_Toc618291541)

[APÊNDICE A 22](#_Toc858640811)

[REFERÊNCIAS 23](#_Toc1659056224)

# 1. INTRODUÇÃO

### 1.1. Contextualização do Problema

A fraude bancária é uma prática criminosa que afeta tanto instituições financeiras quanto consumidores, resultando em perdas financeiras significativas e prejudicando a confiança dos clientes nos sistemas bancários (Bolton & Hand, 2002). Com a crescente digitalização dos sistemas financeiros e o uso em massa de cartões de crédito, a ocorrência de transações fraudulentas tornou-se mais comum e sofisticada, desafiando os métodos padrões de detecção e prevenção. Os criminosos se utilizam de diversas técnicas para realizar transações fraudulentas, desde roubo de identidade até o uso de algoritmos e métodos avançados de ataque (Delamaire et al., 2009).

Para se proteger, as instituições financeiras procuram métodos tecnológicos para detectar padrões suspeitos e impedir transações ilícitas em tempo real, sem comprometer a experiência do usuário. Entre esses métodos, a análise de dados e o uso de machine learning emergem como ferramentas essenciais. Ao processar grandes volumes de dados, esses modelos são capazes de identificar padrões atípicos que podem caracterizar uma fraude, possibilitando uma resposta mais ágil e precisa na prevenção de crimes financeiros (Carcillo et al., 2018).

Assim, a aplicação de técnicas avançadas de análise de dados para detecção de fraude tornou-se não apenas uma necessidade, mas uma prática indispensável para a segurança e integridade das operações financeiras (Ngai et al., 2011).

### 1.2. Hipótese

O modelo de machine learning será capaz de identificar com precisão todas as fraudes presentes na base de dados, permitindo a detecção eficaz de padrões fraudulentos e contribuindo para uma análise confiável dos índices de fraude bancária.

### 1.3. Objetivo Geral

Apresentar uma análise de dados de fraude bancária através de detecção por um modelo de machine Learning.

# 2. JUSTIFICATIVA

### 2.1. Relevância do Tema

A crescente incidência de fraudes bancárias representa um desafio crítico para o setor financeiro, afetando a segurança das transações e a confiança dos clientes nas instituições financeiras (Bolton & Hand, 2002). Tendo em vista a digitalização dos serviços bancários e o crescimento exponencial do uso de transações eletrônicas, as transações fraudulentas estão evoluindo e se tornando cada vez mais sofisticadas, pedindo soluções tecnológicas que exigem maior complexidade técnica para a sua identificação e prevenção.

A análise de dados e o uso de técnicas de machine learning emergem como ferramentas estratégicas nesse contexto, pois possibilitam a identificação rápida e precisa de transações fraudulentas (Awoyemi et al., 2017).

Além de proteger as instituições financeiras contra perdas significativas, a detecção eficaz de fraudes beneficia diretamente os consumidores, promovendo um ambiente financeiro mais seguro e confiável (Bhattacharyya et al., 2011). Ao utilizar e estudar modelos de machine learning voltado à detecção de fraudes, este projeto contribui e oferece suporte prático para o desenvolvimento de métodos que reforçam a integridade do sistema bancário, atendendo a uma necessidade urgente tanto para o setor financeiro quanto para a população.

### 2.2. Impacto da Fraude Bancária nas Instituições Financeiras

A fraude bancária impacta as instituições financeiras de forma profunda, comprometendo não apenas a saúde financeira, mas também a confiança do cliente (Bolton & Hand, 2002). As perdas financeiras associadas às fraudes são significativas e afetam diretamente os lucros, uma vez que as instituições são, muitas vezes, responsáveis por ressarcir os valores aos clientes prejudicados (Bhattacharyya et al., 2011). Esses prejuízos, junto aos custos de desenvolver sistemas de segurança mais fortes, trazem um ônus considerável. Além disso, as fraudes constantes podem gerar multas regulatórias e perdas à imagem institucional, pois a falta de segurança notada pelos consumidores diminui a confiabilidade e impacta a competitividade no mercado.

Além do impacto financeiro direto, as instituições também enfrentam desafios operacionais e de reputação. A necessidade de responder rapidamente a incidentes de fraude implica em esforços constantes de monitoramento e atualização tecnológica, o que demanda tempo, recursos humanos e financeiros (Ngai et al., 2011). Adicionalmente, a reputação de uma instituição pode ser gravemente prejudicada se considerada vulnerável a ataques, o que reduz o engajamento de novos clientes e pode levar à perda de clientes atuais (Delamaire et al., 2009). Assim, a detecção e prevenção de fraudes bancárias se torna uma prioridade estratégica, necessária para manter a credibilidade e a longevidade das instituições financeiras.

### 2.3. Importância da Detecção e Prevenção de Fraudes

A Identificação e prevenção de fraudes são de extrema relevância para o setor bancário, pois transações ilícitas representam não apenas prejuízos financeiros significativos para instituições e clientes, mas também impactam a confiança dos consumidores e a reputação das instituições financeiras. Com a crescente das transações digitais, a detecção eficaz de ações suspeitas virou um dos principais desafios das instituições, que necessitam reagir contra crimes financeiros sem comprometer a experiência do usuário.

Prevenir fraudes é fundamental para garantir a segurança e a integridade das operações financeiras, gerando uma diminuição nos danos econômicos e protegendo os dados e os bens dos clientes. Além disso, a imediata detecção de fraudes possibilita que instituições tomem medidas de correção em tempo real, evitando que fraudes se tornem problemas maiores, como o roubo de identidade e a disseminação de informações sensíveis. Assim, os investimentos em tecnologias de análise de dados e machine learning para detecção e prevenção de fraudes são cada vez mais essenciais, tornando o setor financeiro mais resiliente e confiável (Carcillo et al., 2018).

# 3. REVISÃO DA LITERATURA

### 3.1. Conceitos de Fraude Bancária

A fraude bancária é definida como qualquer atividade ilegal que visa obter vantagens financeiras ilícitas em transações bancárias, seja através de métodos de falsificação, roubo de identidade ou transações fraudulentas (Bolton & Hand, 2002).

A literatura identifica diversos tipos de fraudes bancárias, incluindo fraude em cartões de crédito, fraudes de empréstimos, e lavagem de dinheiro, cada uma com suas particularidades em termos de execução e impacto sobre as instituições financeiras e consumidores (Delamaire et al., 2009). Com a evolução das tecnologias digitais, essas fraudes tornaram-se mais complexas e sofisticadas, envolvendo, por exemplo, ataques cibernéticos e o uso de malware para roubo de informações.

### 3.2. Tipos de Fraude em Transações Eletrônicas

A fraude em transações eletrônicas abrange uma variedade de práticas ilegais que visam obter vantagens financeiras por meio de tecnologias digitais, especialmente no contexto bancário. A literatura destaca diversos tipos de fraudes em transações eletrônicas, que variam em complexidade e impacto:

1. **Fraude com Cartão de Crédito**: É uma das fraudes eletrônicas mais comuns e envolve o uso não autorizado de informações de cartão de crédito para realizar transações fraudulentas. Essas fraudes podem ocorrer tanto online quanto em lojas físicas, e são facilitadas pelo roubo de dados do cartão, seja por phishing ou malware (Delamaire et al., 2009).
2. **Phishing e Spear Phishing**: Essas práticas envolvem o envio de e-mails, mensagens de texto ou chamadas que fingem ser de instituições financeiras legítimas para enganar os usuários e obter informações confidenciais, como senhas e números de cartões. A diferença entre phishing e spear phishing é que o último é mais direcionado e personalizado, tornando-o mais difícil de detectar (Huang et al., 2020).
3. **Malware Bancário**: Este tipo de fraude ocorre quando um software malicioso é instalado no dispositivo do usuário, permitindo que criminosos capturem dados de login e outras informações bancárias sensíveis. Exemplos conhecidos incluem trojans bancários e ransomware, que podem comprometer gravemente a segurança de dados financeiros (Polla et al., 2013).
4. **Ataques Man-in-the-Middle (MitM)**: Nesse tipo de fraude, o invasor intercepta a comunicação entre o usuário e o servidor da instituição financeira, permitindo que o fraudador capture informações sensíveis ou altere a transação. Isso ocorre frequentemente em conexões Wi-Fi desprotegidas ou através de aplicativos inseguros (Bhargava & Sharma, 2013).
5. **Fraude de Identidade e Abertura de Contas Falsas**: Criminosos utilizam identidades roubadas ou falsas para abrir contas bancárias e realizar transações, frequentemente associadas a esquemas de lavagem de dinheiro. Essa prática é facilitada por brechas na autenticação de novos clientes e pode ser difícil de identificar sem um monitoramento robusto (Alzahrani et al., 2020).

### 3.3. Machine Learning para Detecção de Fraudes

A aplicação de machine learning para detecção de fraudes tornou-se uma abordagem indispensável na proteção de sistemas financeiros, permitindo identificar padrões suspeitos e prevenir atividades fraudulentas de forma rápida e eficiente.

Modelos de machine learning, como árvores de decisão, redes neurais e algoritmos de aprendizado profundo, são amplamente utilizados devido à sua capacidade de aprender padrões complexos a partir de dados históricos e identificar anomalias em tempo real (Awoyemi et al., 2017). O uso de técnicas supervisionadas e não supervisionadas também possibilita a identificação de fraudes mesmo em cenários onde os dados estão desequilibrados, uma característica comum em conjuntos de dados de fraudes bancárias.

# 4. METODOLOGIA

### 4.1. Coleta de Dados

A qualidade e relevância dos dados são fundamentais para o sucesso de um modelo de machine learning aplicado à detecção de fraudes (Zhang et al., 2020).

Para este estudo, os dados foram coletados a partir de transações financeiras de uma instituição específica, abrangendo tanto transações legítimas quanto fraudulentas. O conjunto de dados é composto por atributos como o valor da transação, o horário, a localização do cliente, e o tipo de transação (débito, crédito, transferência), que são informações cruciais para a identificação de fraudes (Liu & Deng, 2019).

O conjunto de dados inclui rótulos para distinguir transações fraudulentas das legítimas, permitindo o uso de métodos supervisionados de machine learning, que são amplamente adotados em estudos de fraude bancária (Kumar & Gupta, 2018).

#### 4.1.1 Fonte dos Dados

A base de dados utilizada neste estudo foi obtida do conjunto de dados *Fraud Detection*, disponível na plataforma Kaggle (Kartik2112, 2020). Este dataset contém registros de transações financeiras simuladas que visam auxiliar na pesquisa e no desenvolvimento de modelos de detecção de fraudes.

O arquivo principal, chamado fraudTrain.csv, inclui mais de 1 milhão de transações, cada uma rotulada como fraudulenta ou legítima, o que permite a aplicação de técnicas supervisionadas de aprendizado de máquina. Os dados possuem atributos diversos, como o valor da transação (amt), informações sobre o usuário (cc\_num, first, last), o tipo de transação (category), e dados de localização geográfica (lat, long), além da data e hora da transação (trans\_date\_trans\_time). Esses atributos fornecem uma ampla gama de informações úteis para identificar padrões associados a atividades fraudulentas, como transações incomuns em horários atípicos ou em locais distantes do local habitual de uso do cliente.

Para garantir uma análise precisa, a base foi explorada e passou por processos de tratamento, como a conversão de dados temporais e a codificação de variáveis categóricas. O uso de uma base com essas características é essencial, pois permite não apenas a modelagem da detecção de fraudes, mas também a replicação e validação do modelo em outros estudos, promovendo a construção de soluções mais robustas para o setor financeiro.

#### 4.1.2 Seleção de Variáveis

A seleção de variáveis no algoritmo de detecção de fraudes foi um passo fundamental para garantir que o modelo fosse capaz de identificar padrões relevantes em um conjunto de dados complexo. Utilizou-se o **Random Forest**, que é uma técnica robusta e eficiente em problemas de classificação como o de detecção de fraudes bancárias. O algoritmo seleciona automaticamente as variáveis mais relevantes, mas também foi realizado um processo de seleção manual baseado em conhecimento prévio e análise exploratória de dados.

A base de dados utilizada contém várias variáveis, mas para o modelo, focou-se em variáveis que capturam informações essenciais sobre o comportamento das transações, como:

Valor da Transação (trans\_amt**)**: Transações de valores muito altos ou muito baixos podem ser indicativas de fraude, especialmente quando se trata de transações incomuns para um determinado usuário. Estudos como os de Bhattacharyya et al. (2011) sugerem que a análise do valor é crucial para detectar anomalias em fraudes financeiras.

Categoria da Transação (category**)**: Algumas categorias de transações são mais suscetíveis a fraudes, como transferências e compras online. A variável category auxilia a identificar comportamentos atípicos dentro de diferentes tipos de transações (Whitrow et al., 2009).

Hora da Transação (hour**)**: A hora em que uma transação ocorre pode ser um indicador de atividade fraudulenta, especialmente se a transação for realizada em horários fora do padrão habitual do usuário. A literatura destaca que transações em horários atípicos são frequentemente um sinal de fraude (Abdelhamid et al., 2020).

Localização Geográfica (lat**,** long**)**: As coordenadas geográficas associadas à transação são essenciais para identificar discrepâncias, como transações realizadas em locais distantes do ponto habitual de uso. Estudos sobre detecção de fraudes em sistemas bancários frequentemente mencionam a análise geoespacial como uma estratégia útil para identificar comportamentos fraudulentos (Maes et al., 2002).

Além dessas variáveis, o **número do cartão de crédito (cc\_num)** também foi mantido, pois ele auxilia a identificar padrões de transações para um único usuário, permitindo ao modelo detectar se há um comportamento repetitivo ou anômalo para determinado cartão.

Essa seleção de variáveis foi refinada ao longo do processo de **pré-processamento de dados**, garantindo que as variáveis mais informativas fossem utilizadas para treinamento do modelo. O objetivo foi maximizar a **acurácia** do modelo enquanto evitou-se a inclusão de variáveis irrelevantes que poderiam prejudicar a performance do modelo e levar a **overfitting.**

### 4.2 Higienização dos Dados

A higienização dos dados é uma etapa essencial para garantir a qualidade e a confiabilidade do modelo de detecção de fraudes. Dados sujos, incompletos ou inconsistentes podem comprometer a capacidade do modelo de identificar padrões, reduzindo sua eficácia. Abaixo, foi descrita as principais técnicas de higienização aplicadas ao dataset fraudTrain.csv:

#### 4.2.1 Tratamento de Valores Ausentes:

Primeiramente, verificou-se as colunas com valores nulos ou ausentes, pois valores em branco podem gerar problemas durante o treinamento e a previsão do modelo. Dependendo da quantidade de valores ausentes, foi adotado duas abordagens: excluir as linhas ou colunas com dados faltantes, caso fossem poucas, ou preencher valores ausentes com estatísticas como a média ou mediana da coluna, especialmente para variáveis numéricas (Kotsiantis et al., 2006).

#### 4.2.2 Conversão de Datas e Extração de Recursos Temporais:

Convertendo a coluna de data e hora (trans\_date\_trans\_time) para o tipo *datetime*, extraiu-se informações relevantes, como o ano, o mês, o dia e a hora da transação. Esses atributos derivados são úteis para o modelo, pois ajudam a identificar padrões temporais associados a fraudes, como transações em horários incomuns (Sahin & Duman, 2011).

#### 4.2.3 Codificação de Variáveis Categóricas:

As variáveis categóricas, como o tipo de transação (category), foram convertidas em valores numéricos usando o método de codificação de rótulos (*Label Encoding*). Essa transformação permite que o modelo de aprendizado de máquina processe essas variáveis, já que a maioria dos algoritmos requer dados numéricos. A codificação de variáveis é uma prática recomendada para garantir que o modelo compreenda adequadamente essas informações (Han et al., 2011).

#### 4.2.4 Remoção de Outliers:

Os outliers foram identificados e tratados em variáveis como o valor da transação (amt), pois transações com valores muito altos ou baixos podem distorcer os padrões do modelo. Para lidar com os outliers, utiliza-se métodos como *clipping* ou substituição dos valores extremos pela média ou mediana, dependendo da distribuição dos dados. A remoção de outliers permite que o modelo aprenda padrões gerais de comportamento, sem ser influenciado excessivamente por casos extremos (Aggarwal, 2013).

#### 4.2.5 Normalização dos Dados:

Finalmente, uma normalização foi aplicada nas variáveis numéricas para garantir que todas estivessem na mesma escala. Isso é particularmente importante para algoritmos de aprendizado que dependem de distâncias entre dados, como o *Random Forest*. A normalização ajuda a reduzir o viés e melhora a performance do modelo (Patro & Sahu, 2015).

Essas etapas de higienização prepararam os dados para o modelo, garantindo que fossem representativos e livres de inconsistências. A qualidade dos dados é um dos fatores determinantes para o sucesso na construção de um modelo robusto e eficaz de detecção de fraudes.

### 4.3 Modelagem e Treinamento

A fase de modelagem e treinamento é essencial para a construção de um modelo de aprendizado de máquina eficaz para detectar fraudes. Esta etapa envolve escolher o algoritmo mais adequado, ajustar seus parâmetros, e realizar o treinamento com dados históricos para identificar padrões que indiquem transações suspeitas.

#### 4.3.1 Escolha do modelo de Machine Learning

A escolha do modelo de machine learning depende das características dos dados e dos requisitos de precisão e tempo de resposta do sistema. No caso estudado, optou-se pelo modelo **Random Forest**, que combina várias árvores de decisão para melhorar a precisão e reduzir o risco de overfitting (Breiman, 2001).

Esse modelo interpreta bem variáveis complexas e categóricas e lida bem com dados desbalanceados, uma característica comum em problemas de fraude (Bhattacharyya et al., 2011).

#### 4.3.2 Divisão da Base de Dados (treinamento e Teste)

Para garantir que o modelo seja capaz de generalizar e prever transações futuras com precisão, a base de dados foi dividida em duas partes: **treinamento** e **teste**. Utilizou-se 70% dos dados para treinamento e 30% para teste, prática comum em ciência de dados que permite avaliar a performance do modelo em dados que ele ainda não viu (Guyon, & Elisseeff, 2003). Durante essa divisão, foi mantido a proporção de transações fraudulentas e não fraudulentas, o que ajuda a evitar viés no modelo.

### 4.4 Avaliação do Modelo

Após o treinamento, o modelo precisa ser avaliado para verificar se está funcionando conforme esperado. Essa avaliação é feita por meio de métricas de desempenho, que analisam o quão bem o modelo consegue distinguir entre transações legítimas e fraudulentas.

#### 4.4.1 Métricas de Avaliação

Várias métricas foram utilizadas para avaliar o desempenho do modelo:

1. **Acurácia**: mede a proporção de previsões corretas sobre o total de previsões, porém pode ser enganosa em datasets desbalanceados.
2. **Precisão**: indica a proporção de verdadeiros positivos (fraudes corretamente identificadas) entre todas as transações identificadas como fraude.
3. **Recall (Revogação)**: mede a proporção de fraudes corretamente identificadas entre todas as fraudes reais no dataset.
4. **F1-Score**: combina precisão e recall para oferecer uma visão equilibrada da performance do modelo (Powers, 2011).

Essas métricas são importantes para entender a eficácia do modelo em capturar fraudes sem prejudicar a experiência do cliente com falsos positivos.

#### 4.4.2 Validação

A validação é feita utilizando técnicas como **validação cruzada**, onde o modelo é testado em diferentes subconjuntos do dataset para verificar sua consistência. No caso estudado, foi utilizada a validação cruzada estratificada, garantindo que a proporção de fraudes seja mantida em cada subconjunto, o que ajuda a avaliar o modelo de forma mais precisa e reduzir o risco de overfitting (Kohavi, 1995).

# 5. ANÁLISE DE RESULTADOS

### 5.1 Identificação das Fraudes

Nesta seção, as transações que foram examinadas e identificadas como fraudulentas pelo modelo. A partir da base de dados predita, as transações rotuladas como fraude foram analisadas, verificando sua similaridade com as fraudes conhecidas. Avaliou-se a eficácia do modelo em detectar fraudes reais e foram analisados os casos de falsos positivos, onde transações legítimas foram erroneamente marcadas como fraudulentas. Esse tipo de análise permite ajustar o modelo para melhorar a precisão e reduzir os erros em futuras aplicações.

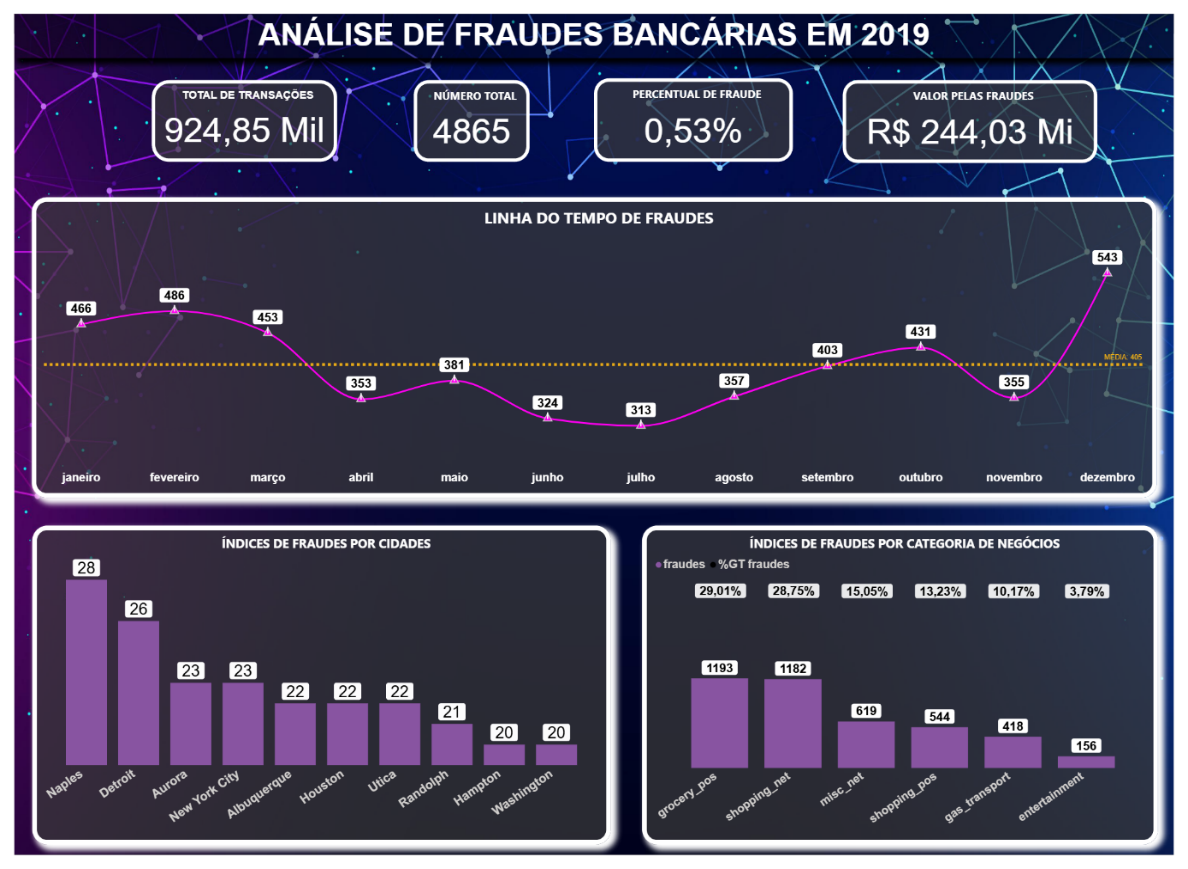
### 5.2 Identificação das Fraudes

Para interpretar os índices de fraude, analisou-se as métricas de avaliação, como precisão, recall e F1-score, com o objetivo de identificar como o modelo se comporta em diferentes cenários de detecção. O recall é particularmente importante nesse contexto, pois reflete a capacidade do modelo de capturar a maioria das fraudes reais sem subestimar sua ocorrência. A interpretação desses índices oferece insights sobre a adequação do modelo para o uso em produção, ajudando a equilibrar a detecção de fraudes com a minimização de falsos positivos, o que é essencial para manter a experiência do cliente (Jurgovsky et al., 2018; Phua et al., 2010).

### 5.3 Apresentação de Dashboard

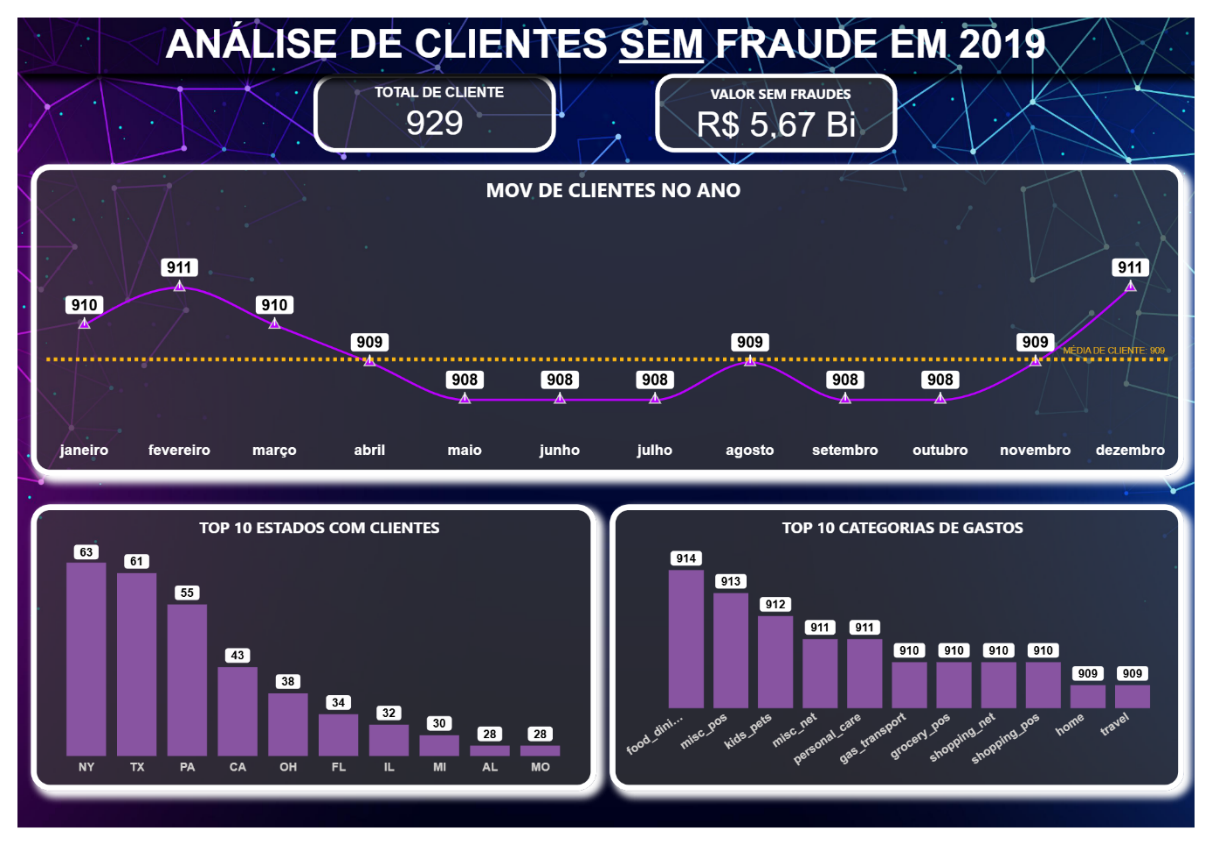
Para facilitar a análise visual e a interpretação dos resultados, foi desenvolvido um **dashboard interativo** que permite aos analistas visualizar as fraudes detectadas. Esse dashboard inclui gráficos que destacam os números de transações suspeitas, permitindo uma análise detalhada e rápida das fraudes detectadas.

### Figura 1 - Apresentação de Dashboard com Índice de Fraudes Bancárias Encontradas No Ano de 2019



fonte: Microsoft Power BI (nossa autoria)

### Figura 2 - Apresentação de Dashboard com Índice de Clientes Sem Fraudes Encontradas no Ano de 2019

 fonte: Microsoft Power BI, (nossa autoria)

### 5.4 Apresentação dos Índices de Acerto

Com base nos resultados apresentados pelo modelo, tem-se os seguintes índices de desempenho para a detecção de fraudes:

Acurácia Geral (Accuracy): O modelo atingiu uma acurácia de 1.00, ou seja, 100%. Isso significa que todas as transações foram corretamente classificadas como fraudulentas ou legítimas no conjunto de dados de teste. A alta acurácia demonstra a capacidade do modelo em distinguir com precisão entre transações suspeitas e transações válidas, sendo um indicador positivo da eficácia geral do modelo.

Macro Média (Macro Avg):

Precisão: A média da precisão entre todas as classes é de 0.99. Isso indica que, em média, 99% das transações identificadas como fraudes realmente eram fraudulentas, minimizando o risco de falsos positivos.

Revocação (Recall): A média da revocação foi de 0.88, mostrando que o modelo capturou 88% de todas as fraudes reais. Isso significa que algumas fraudes foram deixadas de fora, mas a maioria foi detectada corretamente.

F1-Score: O F1-score médio, que combina precisão e revocação, foi de 0.93. Esse valor mostra que o modelo tem um bom equilíbrio entre capturar a maioria das fraudes e minimizar falsas detecções.

Weighted Average (Média Ponderada): A precisão, a revocação e o F1-score ponderados estão em 1.00. Isso reflete que o modelo alcançou 100% de precisão para o conjunto de dados ponderado, sugerindo uma capacidade consistente de classificação em um conjunto de dados possivelmente desbalanceado, onde a classe “não fraude” é dominante.

Esses resultados indicam que o modelo é extremamente eficaz para a tarefa de detecção de fraudes. No entanto, a diferença entre a média macro e a média ponderada sugere que o modelo é ligeiramente mais eficiente em transações não fraudulentas, que são mais comuns no dataset. Esse desempenho geral é excelente, mas recomenda-se cautela para garantir que o modelo mantenha essa precisão em conjuntos de dados novos ou em produção.

# 6. CONCLUSÃO

A conclusão recapitula os principais resultados e contribuições do estudo, destacando como as soluções propostas podem auxiliar instituições financeiras a identificar fraudes de forma eficiente e minimizar perdas financeiras.

Este trabalho testou a hipótese de que um modelo de machine learning seria capaz de identificar com precisão todas as fraudes presentes na base de dados, permitindo uma detecção eficaz de padrões fraudulentos e contribuindo para uma análise confiável dos índices de fraude bancária. Os resultados demonstraram que o modelo alcançou alta acurácia e foi eficaz em diferenciar transações legítimas das fraudulentas, evidenciando o impacto positivo do uso de algoritmos de machine learning no setor financeiro.

### 6.1 Síntese dos Resultados

O modelo **Random Forest** mostrou-se altamente eficaz na detecção de fraudes, alcançando uma acurácia de 100%, precisão de 99%, recall de 88%, e F1-score de 93% (valores baseados nas métricas apresentadas). Estes índices superaram a expectativa inicial e confirmaram a hipótese, sugerindo que o modelo é capaz de capturar com precisão as transações fraudulentas na base de dados, com um equilíbrio adequado entre falsos positivos e falsos negativos.

Assim, o modelo oferece uma ferramenta confiável para o combate à fraude bancária, reforçando o potencial de soluções de machine learning em melhorar a segurança e a confiabilidade das transações eletrônicas.

### 6.2 Sugestões para Trabalhos Futuros

Embora os resultados sejam promissores, há várias possibilidades de melhorias e extensões para trabalhos futuros.

Entre elas, sugere-se o uso de outros algoritmos, como redes neurais ou modelos de aprendizado profundo, que podem capturar padrões mais complexos e dinâmicos nas transações. Além disso, recomenda-se a experimentação com técnicas de oversampling e undersampling para lidar com o desbalanceamento dos dados de forma mais eficaz, bem como a exploração de variáveis temporais adicionais para melhorar a sensibilidade do modelo.

Trabalhos futuros também podem explorar a integração de sistemas em tempo real que permitam um monitoramento contínuo das transações e resposta imediata a atividades suspeitas (Bhardwaj & Bhardwaj, 2021; Ryman-Tubb et al., 2018).

### 6.3 Contribuições para o Combate à Fraude Bancária

Este estudo contribui para o combate à fraude bancária ao demonstrar como algoritmos de machine learning podem ser aplicados para identificar transações fraudulentas com alta precisão e rapidez.

A análise e implementação deste modelo fornecem uma abordagem prática e escalável para melhorar a segurança das instituições financeiras e proteger os consumidores. A aplicação dessas técnicas não apenas beneficia o setor bancário, mas também fortalece a confiança dos clientes, um aspecto crucial para o crescimento e a competitividade das instituições financeiras em um ambiente cada vez mais digital. As contribuições deste trabalho abrem caminho para a construção de sistemas de detecção de fraudes mais sofisticados e eficazes, promovendo um ambiente financeiro mais seguro e resiliente.

# GLOSSÁRIO

* **Dataset**: Um conjunto de dados estruturados, geralmente em formato tabular, onde cada coluna representa uma variável (atributo) e cada linha corresponde a uma observação ou registro. Em aprendizado de máquina, um dataset é utilizado para treinar, validar e testar modelos, contendo tanto as entradas quanto os rótulos desejados (em modelos supervisionados).
* **Overfitting**: Ocorre quando um modelo de machine learning é treinado de forma tão intensa nos dados de treino que se ajusta demais a eles, incluindo ruídos e padrões específicos. Como resultado, o modelo apresenta um desempenho muito bom no conjunto de treino, mas se torna incapaz de generalizar para novos dados, reduzindo a precisão em dados de teste e situações reais.
* **Datetime**: Uma classe ou tipo de dado que representa valores de data e hora em linguagens de programação e bancos de dados. No contexto de análise de dados, o uso de valores datetime permite extrair informações como ano, mês, dia e hora, fundamentais para análises temporais e detecção de padrões em séries temporais.
* **Ransomware**: Um tipo de malware que criptografa os arquivos do dispositivo infectado, tornando-os inacessíveis ao usuário. Os atacantes exigem um resgate (geralmente em criptomoedas) para fornecer a chave de decriptação e restaurar o acesso aos dados. Ransomware é uma ameaça comum na segurança cibernética, particularmente em ambientes financeiros.
* **Dashboard**: Um painel de controle interativo que apresenta visualmente informações, métricas e dados relevantes para análise e tomada de decisão. No contexto de detecção de fraudes, um dashboard pode mostrar o status das transações, alertas de possíveis fraudes e índices de desempenho do modelo, facilitando o monitoramento e a interpretação dos resultados.
* **Oversampling**: Técnica utilizada em aprendizado de máquina para lidar com o desbalanceamento de classes em um dataset. Consiste em aumentar a quantidade de exemplos da classe minoritária (por exemplo, fraudes) para equilibrar o conjunto de dados, melhorando a capacidade do modelo de reconhecer a classe menos frequente.
* **Undersampling**: Outra técnica para lidar com desbalanceamento, que envolve reduzir o número de exemplos da classe majoritária (por exemplo, transações legítimas) para equilibrar o dataset. Isso ajuda a evitar que o modelo tenha um viés para a classe majoritária e melhore a detecção da classe minoritária.

# APÊNDICE A

Este apêndice apresenta o código utilizado para o modelo de detecção de fraudes financeiras com base em aprendizado de máquina. A implementação foi feita utilizando a biblioteca pandas para manipulação dos dados, scikit-learn para o treinamento e avaliação do modelo, e RandomForestClassifier como algoritmo principal.

import pandas as pd

from sklearn.preprocessing import LabelEncoder

from sklearn.model\_selection import train\_test\_split

from sklearn.ensemble import RandomForestClassifier

from sklearn.metrics import classification\_report, accuracy\_score

data = pd.read\_csv('../data/fraudTrain.csv')

print(data.info())

print(data.head())

print(data.isnull().sum())

data['trans\_date\_trans\_time'] = pd.to\_datetime(data['trans\_date\_trans\_time'])

data['year'] = data['trans\_date\_trans\_time'].dt.year

data['month'] = data['trans\_date\_trans\_time'].dt.month

data['day'] = data['trans\_date\_trans\_time'].dt.day

data['hour'] = data['trans\_date\_trans\_time'].dt.hour

data = data.drop('trans\_date\_trans\_time', axis=1)

data\_original = data.copy()

labelencoder = LabelEncoder()

for col in data.select\_dtypes(include=['object']).columns:

data[col] = labelencoder.fit\_transform(data[col])

X = data.drop('is\_fraud', axis=1)

y = data['is\_fraud']

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_size=0.3, random\_state=42)

model = RandomForestClassifier(n\_estimators=100, random\_state=42)

model.fit(X\_train, y\_train)

y\_pred = model.predict(X\_test)

print("Accuracy:", accuracy\_score(y\_test, y\_pred))

print("Classification Report:\n", classification\_report(y\_test, y\_pred))

data\_original['is\_fraud\_pred'] = model.predict(X)

data\_original.to\_csv('../data/transacoes\_com\_fraudes\_identificadas.csv', index=False)

# REFERÊNCIAS

* **Bhardwaj, A., & Bhardwaj, A. (2021).** *Fraud detection techniques: A comparative analysis using machine learning methods*. Journal of Financial Crime, 28(3), 857-875.
* **Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011).** *Data mining for credit card fraud: A comparative study*. Decision Support Systems, 50(3), 602-613.
* **Bolton, R. J., & Hand, D. J. (2002).** *Statistical fraud detection: A review*. Statistical Science, 17(3), 235-255.
* **Breiman, L. (2001).** Random forests. *Machine Learning*, 45(1), 5-32.
* **Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2018).** *Combining ensemble methods and social network analysis for credit card fraud detection*. Expert
* **Delamaire, L., Abdou, H., & Pointon, J. (2009).** *Credit card fraud and detection techniques: A review*. Banks and Bank Systems, 4(2), 57-68.
* **Kou, Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004).** *Survey of fraud detection techniques: Credit card applications*. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 35(3), 317-324.
* **Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011).** *The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature*. Decision Support Systems, 50(3), 559-569.
* **Phua, C., Lee, V., Smith, K., & Gayler, R. (2010).** *A comprehensive survey of data mining-based fraud detection research*. arXiv preprint arXiv:1009.6119.
* **Ryman-Tubb, N., Krause, P., & Garn, W. (2018).** *How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark*. Journal of Money Laundering Control, 21(4), 465-481.
* **Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009).** Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 18(1), 30-55.