Processando o Saber
eISSN 2179-5150
FATEC Praia Grande · fatecpg.edu.br/revista
submetido: Jan/2025 · **aceito**: Mar/2025 · **publicado**: Jun/2025
DOI 10.5281/zenodo.15477217

Detecção de fraudes em transações bancárias utilizando inteligência artificial

Fraud detection in banking transactions using artificial intelligence

Pedro Lucas Maranini Tosta
Fatec Praia Grande
pedro.tosta@fatec.sp.gov.br

Jonatas Cerqueira Dias
Fatec Praia Grande
jonatas.dias2@fatec.sp.gov.br

RESUMO

O artigo analisa o impacto da Inteligência Artificial (IA) no setor bancário e financeiro, especificamente na detecção de fraudes em transações financeiras. Destaca-se a evolução da IA e seu papel transformador no contexto bancário e financeiro. O foco central é a complexidade das fraudes financeiras, abordando diversas modalidades e seu impacto econômico, são citados casos emblemáticos como a Fraude de Jerome Kerviel no Société Générale (2008) e a Fraude de Nick Leeson no Barings Banks (1995), evidenciando a necessidade de métodos eficazes na prevenção e identificação desses incidentes. O artigo delineia as técnicas modernas e IA empregadas na detecção de fraudes bancárias, destacando o uso de algoritmos avançados, como aprendizado de máquina e redes neurais. A proposta é utilizar essas abordagens para identificar padrões suspeitos em transações financeiras, ressaltando não apenas a eficácia, mas também o potencial dessas metodologias na mitigação de riscos e na proteção das instituições financeiras contra atividades fraudulentas. O estudo fornece uma visão detalhada desde os métodos mais antigos até os métodos mais atuais de IA destacando a utilização de algoritmos avançados para alcançar uma detecção mais precisa e eficiente. Os resultados ressaltam a capacidade desses métodos em identificar e prevenir incidentes similares aos casos apresentados. Espera-se que algoritmos avançados proporcionem uma resposta efetive na identificação de transações suspeitas. O estudo conclui enfatizando não apenas a eficácia das abordagens modernas de IA na detecção de fraudes bancárias, mas também o potencial dessas técnicas na proteção das instituições financeiras contra atividades fraudulentas. Destaca-se a importância contínua do desenvolvimento e implementação de métodos avançados de IA para fortalecer a segurança no setor bancário, mitigando riscos e protegendo os clientes e as instituições contra ameaças financeiras.

PALAVRAS-CHAVE: Inteligência Artificial; Detecção de fraudes; Aprendizado de Máquina; Segurança nas transações bancárias

ABSTRACT

The article analyzes the impact of Artificial Intelligence (AI) in the banking and financial sector, specifically in the detection of fraud in financial transactions. It highlights the evolution of AI and its transformative role in the banking and financial context. The central focus is on the complexity of financial frauds, addressing various types and their economic impact. Emblematic cases such as the Jerome Kerviel's fraud at Société Générale (2008) and Nick Leeson's Fraud at Barings Banks (1995) are mentioned, underscoring the need for effective methods in preventing and identifying these incidents. The article outlines modern techniques and AI employed in detecting banking frauds, emphasizing the use of advanced algorithms such as machine learning and neural networks. The proposal is to use these approaches to identify suspicious patterns in financial transactions, emphasizing not only their effectiveness but also their potential in mitigating risks and protecting financial institutions against fraudulent activities. The study provides a detailed overview from older to more current AI methods, highlighting the use of advanced algorithms to achieve more precise and efficient detection. The results underscore the capability of these methods in identifying and preventing incidents similar to the cases presented. It is expected that advanced algorithms will provide an effective response in identifying suspicious transactions. The study concludes by emphasizing not only the effectiveness of modern AI approaches in detecting banking frauds but also the potential of these techniques in protecting financial institutions against fraudulent activities. It highlights the ongoing importance of developing and implementing advanced AI methods to strengthen security in the banking sector, mitigating risks, and safeguarding clients and institutions against financial threats.

KEYWORDS: *Artificial Intelligence; Fraud detection; Machine Learning; Security in banking transactions;*

INTRODUÇÃO

No atual cenário global e mundial e transações financeiras eletrônicas, a segurança dos sistemas bancários e financeiros tornou-se uma grande preocupação para instituições financeiras e clientes. O avanço da tecnologia e o uso de novas ferramentas, embora tenha facilitado o acesso e a gestão dos recursos financeiros, também abriu novas portas para atividades fraudulentas e criminosas que ameaçam a integridade do sistema bancário e do sistema financeiro. A fraude é uma preocupação atual nas organizações, particularmente, no setor bancário, um dos grandes desafios para o setor tem sido otimizar a detecção de fraudes em transações bancárias usando Inteligência Artificial (IA), aumentando a precisão na identificação de fraudes, minimização de falsos positivos, fortalecendo a segurança das transações e reduzindo os prejuízos para seus respectivos clientes, além de causar um grande impacto nas organizações. A ocorrência de uma fraude pode pôr em causa os objetivos, a continuidade e a confiabilidade da instituição (SEMEDO, 2022).

Um dos objetivos principais na detecção de fraudes, é detectar um maior número de fraudes e transações suspeitas e fora do padrão com o menor número possível de alarmes falsos (falsos positivos) (KOVACH, 2011).

Uma transação legítima que é sinalizada/identificada como uma fraude ou fora do padrão, é caracterizado um alarme falsou. Por outro lado, o custo de não detectar uma fraude pode ser bem alto, mas também disparar alarmes mediante a toda suspeita gerando muitos alarmes falsos podem gerar uma insatisfação dos clientes legítimos. (KOVACH, 2011).

Este contexto explorou o seguinte objetivo para a pesquisa, explorar e analisar o potencial da Inteligência Artificial (IA) na detecção de fraudes bancárias, visando proporcionar uma abordagem mais eficaz e proativa para enfrentar esse desafio. Por meio da aplicação de algoritmos de aprendizado de máquina e técnicas avançadas de processamento de dados, busca-se estudar sistemas capazes de identificar padrões e atividades suspeitas em tempo real, minimizando assim os impactos financeiros e reputacionais decorrentes das fraudes (LIMA, 2022).

O presente estudo será estruturado em seções que abordarão, primeiramente, as bases conceituais da IA enfatizando sua aplicabilidade e potencialidades no contexto da detecção de fraudes, os fundamentos teóricos relacionados às fraudes bancárias e financeiras, delineando os tipos e métodos mais comuns empregados pelos fraudadores, as maiores fraudes já registradas e ferramentas que são usadas para detecção de fraudes financeiras no geral (OLIVEIRA, 2019).

Posteriormente, será discutida a metodologia atualmente usada para otimização e detecção de fraudes financeiras, incluindo a seleção de algoritmos, a escolha e a preparação dos dados, bem como a avaliação dos resultados obtidos. Adicionalmente, serão apresentados casos de estudo e comparativos com abordagens tradicionais, demonstrando a eficácia de aplicação da IA neste contexto.

1. FUNDAMENTAÇÃO TEÓRICA

A IA é um avanço tecnológico que pode ser definido como um sistema que utiliza a tecnologia para simular a inteligência humana, e que analisa banco de dados para tomar decisões de modo autônomo. Em síntese, a IA está relacionada à capacidade de captar dados do banco de dados e elaborar, a partir disso, um pensamento construtivo e relevante (DE LIMA, 2023).

Os Algoritmos nada mais são do que uma sequência finita de ações que resolve um certo problema, assim esse algoritmo consegue resolver problemas de vários tipos diferentes, cálculo

estrutural, processamento de dados ou planejamento (SICHMAN, 2021). A partir dos anos de 1980, a aplicação da IA na rede bancária e financeira em geral, trouxe avanços significativos. Começaram a surgir os primeiros sistemas de IA para análises de riscos de crédito e detecção de fraudes. Os sistemas eram capazes de processar grandes volumes de dados em tempo real, analisando e identificando padrões suspeitos de atividades.

Com o avanço da tecnologia, os *chatbots*, assistentes virtuais, todos baseados em IA, foram introduzidos em interface de atendimento ao cliente, proporcionando respostas mais rápidas e eficazes. Algoritmos de Aprendizado de Máquina passaram a ser utilizados para otimizar a gestão de portfólios de investimentos, adaptando-se às condições do mercado em tempo real.

Atualmente, a IA na rede bancária e financeira atingiu um nível de sofisticação altíssimo. Utilizada para análise de dados macroeconômicos, previsão de tendências de mercado, gestão de riscos e até mesmo para desenvolvimento de *blockchain* e criptomoedas. A IA se tornou um componente fundamental para eficiência e segurança do setor financeiro, transformando a maneira como transações e investimentos são gerenciados (OLIVEIRA, 2019).

1.1 FRAUDES, FRAUDES BANCÁRIAS E FRAUDES FINANCEIRAS

Fraudes refere-se a qualquer ação tomada de forma consciente ilícita, desonesta e punível por lei, com o objetivo de obter lucro próprio em contrapartida de prejudicar um terceiro. Intencional e premeditada, sendo por isso uma fuga à verdade, descurando ou lesando o interesse de terceiros (SEMEDO, 2022).

As fraudes bancárias e financeiras no geral referem-se a atividades ilegais e criminosas que visam obter ganhos financeiros de forma enganosa, muitas vezes à custa de instituições financeiras, organizações ou indivíduos. Essas práticas envolvem uma série de métodos e técnicas que exploram vulnerabilidades nos sistemas bancários e financeiros, bem como a confiança e a ingenuidade das vítimas. A prevenção de fraudes bancárias e financeiras consiste em evitar que medidas sejam tomadas antes do término de uma transação ou uma fraude (KOVACH, 2011).

1.2 AVANÇO DA IA NA DETECÇÃO DE FRAUDES BANCÁRIAS

No caso da detecção de fraude, não existe um conjunto de instituições pré-definidas que consiga mapear diretamente uma transação e classificá-la como fraude ou não fraude. Para tentar fazer esse mapeamento, é necessário analisar as informações de uma grande quantidade de instâncias e, a partir desses dados, extrair um algoritmo que seja capaz de executar essa tarefa, mesmo que ele não acerte com total precisão (CAIRES, 2022).

O avanço da IA na detecção e prevenção de fraudes bancárias foi marcado por uma evolução constante em técnicas e capacidades analíticas. É de extrema importância analisar e entender algumas etapas desse processo.

1.2.1 Regras manuais e heurísticas (1980-1990)

No seu período inicial os bancos e instituições financeiras dependiam principalmente de regras manuais e heurísticas para identificar atividades suspeitas. Isso envolvia a definição de padrões de comportamento e transações consideradas anômalas ou suspeitas.

1.2.2 Sistemas baseados em regras (1990-2000)

Nesta etapa do processo, os sistemas começaram a utilizar algoritmos mais avançados, baseados em regras pré-definidas. Estes sistemas eram capazes de analisar padrões de transações em tempo real e acionar alertas e avisos em casos de atividades ou transações suspeitas.

Pela facilidade de implementação e entendimento, os sistemas de regras são amplamente utilizados pela indústria, entretanto, a complexidade de manutenção e a limitação na detecção de padrões deram espaço para utilização de métodos e previsão mais complexos (CRISTOVÃO, 2023).

1.2.3 Introdução de algoritmos de aprendizado de máquina (2000-2010)

Com o surgimento de algoritmos de aprendizado de máquina, como árvores de decisão, redes neurais e *support vector machines* (SVMs), os sistemas de detecção de fraudes tornaram-se mais sofisticados. Eles podiam aprender com grandes conjuntos de dados históricos e identificar padrões complexos de comportamento fraudulento. O algoritmo SVM pode ser

utilizado tanto em casos de regressão quanto de classificação, sendo o seu principal uso na classificação de bases de dados complexas de pequeno e médio porte (DE SOUZA, 2023). Englobando estudos de métodos computacionais para adquirir novos conhecimentos, novas habilidades e novos meios de organizar o conhecimento já existente (SANCHES, 2003).

1.2.4 Aprendizado profundo (*deep learning*) e redes neurais (2010-presente)

O advento *deep learning* revolucionou a detecção de fraudes. Ao invés de utilizar o os próprios dados para desempenhar funções pré-estabelecidas, ele habilita o computador a desenvolver um reconhecimento de padrões sozinho e com base nos fatores básicos de dados (DE LIMA, 2023).

As redes neurais profundas, em particular, provaram ser altamente eficazes na identificação de padrões complexos e sutis em grandes volumes de dados. São capazes de aprender automaticamente e adaptar-se a novas formas de fraude sem a necessidade de regras explícitas.

No geral, Redes neurais são modelos matemáticos criados inspirados no funcionamento do cérebro humano (CRISTOVÃO, 2023).

1.2.5 Processamento e análise em tempo real (atual)

A capacidade de processar e analisar dados em tempo real tornou-se crucial na detecção de fraudes bancárias e financeiras. Com a IA, os sistemas podem avaliar transações em tempo real e identificar padrões suspeitos instantaneamente, o que permite a intervenção imediata.

1.2.6 Integração de dados diversificados e tecnologia avançada (atual)

A IA na detecção de fraudes agora integra uma ampla variedade de fontes de dados, incluindo transações financeiras, geolocalização, padrões de comportamento do usuário e até mesmo informações provenientes de redes sociais. A combinação de múltiplos tipos de dados e a aplicação de técnicas avançadas de IA resultam em sistemas altamente precisos.

1.2.7 Adoção de modelos produtivos e análise de anomalias (atual)

Atualmente são utilizados modelos preditivos que não apenas identificam atividades fraudulentas conhecidas, mas também são capazes de detectar anomalias sutis que podem indicar novos tipos de fraudes e ações.

O avanço da IA na detecção de fraudes bancárias foi uma jornada de constante aprimoramento de técnicas analíticas, desde abordagens manuais até a aplicação de técnicas de aprendizado profundo e processamento em tempo real. Evolução continua é essencial para manter a segurança e a integridade do setor financeiro em geral em um mundo digital cada vez mais complexo.

Utilizando algoritmos de detecção de anomalias, como Isolation Forest, os sistemas podem analisar continuamente as transações para identificar comportamentos fora do padrão. *Iforest* é um algoritmo baseado em árvore, construído em torno da teoria das arvores de decisão. O princípio básico do *Iforest* é as anomalias serem poucas e estão distantes do restante das outras observações (DE SOUZA, 2023).

1.3 MAIORES FRAUDES BANCÁRIAS E PREJUÍZOS FINANCEIROS REGISTRADOS

As maiores fraudes e prejuízos financeiros já registrados ao longo da história, eventos marcantes que abalaram o sistema financeiro e tiveram impacto significativo tanto nas instituições envolvidas quanto na confiança do público. Todas as maiores fraudes eletrônicas consistem em grandes problemas internos a serem combatidos pelas instituições financeiras, tendo em vista as perdas do sistema financeiro. (MATHIJSSEN; OVEREEM; JANSEN, 2020).

A aplicação de técnicas e ferramentas de Inteligência Artificial pode ser um dos componentes mais valiosos na detecção de fraudes bancárias e financeiras. A prevenção ou detecção de fraudes é, cada vez mais, um assunto delicado, devido às variadas formas e meios adotados na perpetração dos atos fraudulentos, e a intervenção da Auditoria Interna mais significativa, daí está “interseção”, entre Auditoria Interna e Fraude, ter sio considerado como desafiante e relevante para ser estudado no âmbito de fraudes em instituições bancárias (SEMEDO, 2022).

Abaixo será apresentado alguns casos de uso do problema citado acima e como proposto no estudo, vamos avaliar formas e tecnologias dos dias atuais que possivelmente preveniriam e alertariam as instituições sobre tais fraudes, assim evitando enormes perdas.

1.3.1 Fraude de Jerome Kerviel no Société Générale (2008)

Jerome Kerviel foi um operador do banco Société Générale que se envolveu em uma das maiores fraudes da história financeira. Em 2008, *Kerviel* foi responsável por realizar operações não autorizadas e arriscadas, especulando no mercado de futuros. Ele criou posições massivas e não autorizadas em contratos futuros, assumindo enormes riscos sem o conhecimento ou permissão do banco (HERMANN FILHO, 2011).

O total de perdas acumuladas pelo banco alcançou a incrível soma de quatro bilhões e novecentos milhões de euros e, são decorrentes de operações não autorizadas que foram, no decorrer do tempo, escondidas por operações fictícias, que anulavam o impacto nos relatórios que monitoravam os riscos de mercado (HERMANN FILHO, 2011).

1.3.2 Fraude de Nick Leeson no Barings Banks (1995)

Nick Leeson, um corretor britânico, operava na filial de Cingapura do Barings Bank. Ele realizou operações não autorizadas em contratos futuros de índice Nikkei, assumindo posições excessivamente arriscadas. Leeson ocultava suas perdas através de uma série de transações fraudulentas e manipulações contábeis (DE QUEIROZ MACHADO, 2015).

As perdas acumuladas por Leeson atingiram um montante colossal de aproximadamente 1,4 bilhão de dólares, levando à falência do Barings Bank em 1995. Este caso ilustrou a importância da supervisão e controle rigorosos nas operações de trading em instituições financeiras.

Cabe mencionar a falha na gestão de risco do Banco Barings, que desde sua origem e em sua evolução histórica mostrou-se ser uma instituição envolvida com transações altamente arriscadas. Isso envolve, por outro lado, a questão da profissionalização da gestão, que é essencial em qualquer tipo de instituição (DE QUEIROZ MACHADO, 2015, p. 327).

1.4 USANDO IA PARA PREVENIR FRAUDES DOS CASOS DE USO

Como proposto na seção acima, serão avaliados os dois casos de uso citados acima e demonstrar como essas fraudes poderiam ter sido evitadas caso na sua respectiva época a tecnologia tivesse em um nível significativamente avançado.

1.4.1 Fraude de Jerome Kerviel no Société Générale (2008)

No caso do *Jerome Kerviel* podemos citar alguns algoritmos e métodos de IA para prevenção desse tipo de fraude, como: Algoritmos de clusterização e Árvore de decisão.

Algoritmos de clusterização podemos citar K-means, esse algoritmo tem o objetivo de encontrar grupos nos dados. O agrupamento dos pontos de dados é realizado pela similaridade do recurso encontrados na base, onde esse algoritmo busca de forma iterativa atribuir cada ponto de dados a um dos grupos (MATHIJSSEN; OVEREEM; JANSEN, 2020, KOHILAN; et al., 2023).

Árvore de decisão é uma técnica que divide dados em várias subcategorias com base em diferentes critérios. Pode ser usado para identificar padrões em transações que podem ser indicativos de atividades fraudulentas (BELTRAN, 2019).

Os modelos denominados de Árvore de decisão como o próprio nome sugere trata-se de uma árvore onde existem nós e em cada nó tem a função de representar um teste em algum atributo e assim cada ramo de árvore representa um resultado desse teste (MATHIJSSEN; OVEREEM; JANSEN, 2020, KOHILAN; et al., 2023).

1.4.2 Fraude de Nick Leeson no Barings Banks (1995)

No caso da Fraude de Nick Leeson no Barings Banks poderíamos citar alguns métodos de prevenção, como: Monitoramento de riscos em tempo real e Análise de padrões de negociação. Sistemas de IA poderiam ter sido usados para monitorar continuamente as posições e os riscos de trading, alertando os gestores quando as operações ultrapassassem limites predefinidos.

Nesse caso um “Sistema de Gerenciamento de Riscos em Tempo Real” (Real-Time Risk Management System). Este tipo de sistema utiliza técnicas avançadas de análise de dados em tempo real, incluindo aprendizado de máquina, processamento de eventos complexos (CEP) e outras técnicas estatísticas para avaliar e monitorar em tempo real uma ampla gama de riscos em diversos contextos, como financeiros, operacionais, regulatórios, de segurança, entre outros (LIMA, 2022).

A Inteligência Artificial de Análise de Padrões de Negociação poderia ser usada para analisar padrões de negociação e identificar desvios significativos, sinalizando atividades potencialmente fraudulentas.

Nesse caso um "Sistema de Análise Técnica Assistida por IA" *(AI-Powered Technical Analysis System)*. Este tipo de sistema utiliza algoritmos de aprendizado de máquina e técnicas avançadas de processamento de dados financeiros para analisar padrões de negociação em mercados financeiros (LIMA, 2022).

1.5 FERRAMENTAS E MÉTODOS DE IA USADOS ATUALMENTE PARA PREVENIR E IDENTIFICAR ATIVIDADES FRAUDULENTAS

É de extrema importância ressaltarmos que a implementação e a aplicação eficaz de IA na prevenção de fraudes bancárias/financeiras requerem uma grande combinação de algoritmos avançados, um número grande de dados e de alta qualidade e profissionais capacitados para interpretar os alertas e avisos gerados por esses algoritmos. Além disso, a IA também deve ser vista como uma ferramenta complementar às práticas de governança e regulamentações existentes, não como um substituto.

A segurança no setor bancário e no setor financeiro em geral é para proteger os ativos financeiros dos clientes e manter a integridade do sistema financeiro como um todo. Com o avanço da tecnologia, métodos tradicionais de detecção de fraudes tornaram-se menos eficazes diante da sofisticação das táticas empregadas pelos criminosos e fraudadores. Neste contexto, a aplicação de técnicas de IA tem se destacado e aumentado como uma abordagem promissora para preveni e identificar atividades fraudulentas. Como proposto no nosso estudo, iremos descrever e exemplificar abaixo algumas ferramentas e métodos que são no dia usados atualmente pelas empresas do setor financeiro e bancário.

1.5.1 *Machine learning* e redes neurais

No contexto de fraudes bancárias, graças às técnicas de Aprendizado de Máquina é possível melhorar a gestão de uma possível fraude em tempo real (MATHIJSSEN; OVEREEM; JANSEN, 2020). A detecção de fraudes bancárias com IA é baseada principalmente em técnicas de Aprendizado de Máquina, uma disciplina que capacita os sistemas a aprenderem padrões a partir de grandes conjuntos de dados.

Dentro do Aprendizado de Máquina, as Redes Neurais têm se mostrado especialmente eficazes em tarefas complexas como essa. Elas são capazes de identificar padrões não-lineares em dados multidimensionais, o que as torna ideais para a detecção de fraudes, que muitas vezes envolve relações sutis e interações complexas.

1.5.2 Processo de seleção, transformação ou criação de novas características *(feature engineering)*

A preparação dos dados é uma etapa crucial no desenvolvimento de modelos de detecção de fraudes. *Feature Engineering* envolve a seleção e transformação das variáveis relevantes para o problema em questão. No contexto de fraudes bancárias, isso pode incluir informações como transações anteriores, comportamento do cliente, localização geográfica, entre outros. Além disso, técnicas avançadas, como a redução de dimensionalidade, podem ser aplicadas para melhorar a eficiência dos modelos.

O K-means é um algoritmo de agrupamento, ou de clusterização, que é um tipo de categoria de aprendizado não supervisionado. Seu funcionamento consiste em agrupar os dados a partir de suas características (DE SOUZA, 2023, BELTRAM, 2019).

1.5.3 Algoritmos de aprendizado supervisionado

O aprendizado supervisionado busca por padrões pré-definidos utilizando bases pré-rotuladas para encontrar novas fraudes (AZEVEDO, 2021). Ela envolve a construção de modelos a partir de um conjunto de dados rotulados, no qual as instâncias são marcadas como "fraude" ou "não fraude". Algoritmos como *Random Forest*, *Support Vector Machines* e Redes Neurais Convolucionais são amplamente utilizados nesse contexto.

Os algoritmos para aprendizado supervisionado relacionam uma instrução a uma entrada baseada em dados aleatórios. Nesse caso, o usuário alimenta o algoritmo com pares de entradas e saídas conhecidas, muitas vezes na forma de vetores. Cada saída recebe um rótulo, que pode ser uma classe ou um valor numérico. O algoritmo determina uma forma de prever qual rótulo de saída com base em uma entrada forte (SANTOS, 2023).

Podem ser caracterizados como algoritmos supervisionado e não supervisionado, caso seus exemplos estejam rotulados com sua classe correspondente, utiliza-se algoritmos de aprendizado supervisionado, os quais induzem padrões a partir dos dados. Exemplos não rotulados, faz-se necessária a utilização dos não-supervisionados, esses algoritmos buscam por padrões nos dados a partir de uma caracterização de similaridade (SANCHES, 2003).

1.6 METODOLOGIA DE DETECÇÃO DE FRAUDES BANCÁRIAS

A detecção de fraudes bancárias utilizando a IA, representa um grande e significativo avanço na segurança do setor bancário e financeiro em geral. Com diversas técnicas como de Aprendizado de Máquina, Redes Neurais, *Feature Engineering*, Algoritmos de aprendizado supervisionado e o uso de diversos outros algoritmos avançados, é possível construir modelos capazes de detectar e identificar padrões extremamente complexos para agir proativamente na prevenção de todas e quaisquer atividades suspeitas e fraudulentas. Esses modelos e construções seguem hoje uma metodologia, para que possa ser aplicado em todo seu contexto.

1.6.1 Preparação dos dados

Nesta fase, os dados transacionais e comportamentais são coletados e pré-processados. Isso inclui a normalização de variáveis, tratamento de outliers (valores atípicos) e a seleção das características mais relevantes.

Algoritmos de clusterização, como K-means, podem ser utilizados nessa etapa para preparar os dados, mas é importante mencionar que seu uso na preparação dos dados depende do contexto específico do problema. O algoritmo K-means é utilizado para agrupar dados considerados semelhantes, através de cálculos de distância, isso permite diferenciar os grupos em questão (MARTINS; GALEGALE, 2022, BARCELOS; DOS SANTOS, 2023).

1.6.2 Construção do modelo

Diferentes técnicas de aprendizado supervisionado são exploradas para determinar qual se adequa melhor ao problema em questão. É essencial considerar a sensibilidade ao desequilíbrio de classes, uma vez que fraudes bancárias são eventos raros em comparação com transações legítimas. *Support Vector Machine* (SVM) é um algoritmo de aprendizado de máquina supervisionado que pode ser utilizado para desafios de classificação ou regressão (SANTOS, 2023).

1.6.3 Avaliação e ajuste

O modelo é avaliado utilizando métricas como precisão (todas as classificações de **classe Positivo que o modelo fez**, **quantas estão corretas**), *recall* (todas as situações de **classe Positivo como valor esperado, quantas estão corretas**), *F1-score* (**média harmônica entre**

precisão e *recall*). É importante realizar ajustes e otimizações para melhorar o desempenho do modelo, garantindo uma detecção eficaz de fraudes sem gerar um alto número de falsos positivos.

Além dos métodos citados acima, a IA pode ser integrada com sistemas de gerenciamento de segurança e vulnerabilidade, permitindo assim a priorização e categorização das falhas identificadas. Ela também pode monitorar atividades maliciosas na *dark web*, coletando e fornecendo informações altamente valiosas sobre potenciais ameaças e vulnerabilidades específicas que possivelmente possam impactar o setor bancário, para que os modelos citados acima possam agir, bloqueando todo tipo de tentativa fraudulenta.

Em análise do estudo e das informações, a IA não substitui, mas sim complementam uma abordagem holística de segurança cibernética. Políticas de segurança bem definidas, treinamento contínuo de equipes e pessoas, monitoramento constante são itens igualmente cruciais. A utilização de IA na identificação e correção de vulnerabilidades em instituições bancárias representa um avanço significativo na defesa contra as ameaças digitais que rodeiam nosso mundo cada vez mais conectado.

2. PROCEDIMENTOS METODOLÓGICOS

Está pesquisa pode ser classificada como uma pesquisa descritiva, com o objetivo de investigar e entender o fenômeno das fraudes bancárias, buscando entender tanto sua recorrência quanto os métodos de tratamento atualmente empregados para sua resolução. Visou-se identificar potenciais oportunidades de otimização no processo de detecção e prevenção de fraudes em instituições financeiras.

Adotando uma abordagem metodológica com algumas fases, combinando diversas técnicas para obter uma compreensão abrangente do fenômeno de fraudes bancárias, as fases foram:

1) Revisão bibliográfica
2) Análise de dados secundários obtidos via plataforma digital Dimensions AI
3) Extração de conhecimento do portfólio de artigos por meio de leitura crítica e analítica

A revisão bibliográfica proporciona uma base teórica sólida, permitindo mapeamento do estado atual do conhecimento sobre fraudes bancárias. A análise de dados secundários conduzida para explorar conjuntos de dados existentes relacionados ao tema de fraudes bancárias.

Além da revisão bibliográfica abrangente, foram realizadas leituras críticas e analíticas GIL (2002) de artigo científicos relevantes. A combinação destas abordagens metodológicas permitiu uma investigação abrangente e detalhada do tema, oferecendo uma visão completa do panorama atual e identificando áreas de possíveis melhorias nos processos de detecção e prevenção.

Como procedimento técnico, a pesquisa foi realizada através de algumas plataformas de busca como: *Dimensions AI* e *Google Scholar,* pelo portal de busca geral. Os artigos seguiram o proposto por GIL (2002) com a leitura crítica e analítica feita com base nos textos selecionados. As buscas por materiais foram filtradas de forma que fosse selecionado textos que abordam assuntos sobre o tema da pesquisa onde possuíam algum tipo de apontamento ou relevância direta com o tema.

3. RESULTADOS E DISCUSSÃO

A aplicação de técnicas de ML (*Machine Learning*) e RN (Redes Neurais) representa um marco significativo na detecção de fraudes no setor bancário. Dentro do espectro do ML (*Machine Learning*), as RN (Redes Neurais) destacam-se por sua eficácia singular na identificação de padrões não lineares em conjuntos de dados multidimensionais. Sua capacidade de discernir nuances e complexidades em transações financeiras torna-as uma ferramenta ideal para detectar atividades fraudulentas que frequentemente envolvem interações intricadas e sutis.

O foco central é a complexidade de fraudes financeiras no geral, abordando diversas modalidades e analisando seu impacto econômico. O estudo destaca casos emblemáticos, como o Fraude de *Jerome Kerviel* no *Société Générale* (2008) e a Fraude de Nick Leeson no Barings Bank (1995), para evidenciar a necessidade de métodos eficazes na prevenção, identificação e otimização desses incidentes.

Buscamos explorar e analisar a potência da IA na detecção de fraudes bancárias, visando uma abordagem mais eficaz e proativa. Através da aplicação de algoritmos de ML (*Machine Learning*) e técnicas avançadas de processamento de dados, identificando algoritmos/sistemas

que identifique padrões e atividades suspeitas em tempo real, para que possa ser minimizado os impactos financeiros e reputacionais gerados por fraudes.

A eficácia das abordagens modernas de IA, ressalta a capacidade desses métodos em identificar e otimizar incidentes provenientes de fraudes, assim como citado nos casos emblemáticos apresentados. Entenda-se que, os algoritmos avançados, como ML (*Machine Learning*) e RN (Redes Neurais), proporcionam uma resposta mais efetiva e conclusiva na identificação de padrões suspeitos.

4. CONSIDERAÇÕES FINAIS

O objetivo dessa pesquisa foi investigar e entender o fenômeno das fraudes bancárias, buscando entender tanto sua recorrência quanto os métodos de tratamento atualmente empregados para sua resolução. Visou-se identificar potenciais oportunidades de otimização de processo de detecção e prevenção de fraudes em instituições financeiras.

A análise dos dados sugere que o avanço tecnológico e a crescente digitalização de diversos serviços, principalmente financeiro, tem sido de grande impacto para o aumento das fraudes bancárias e financeiras. A contribuição para a crescente vulnerabilidade dos sistemas financeiros, se dá pela facilidade de acesso ás informações pessoais dos clientes, alinhada com a sofisticação das táticas utilizadas pelos fraudadores.

Fatores como a falta de investimento em medidas de segurança cibernética, juntamente com a falta de conscientização dos consumidores sobre práticas de segurança digital, desempenham um papel crucial nesse cenário. Além disso, a rápida evolução das tecnologias proporcionou um ambiente muito mais propício para o surgimento de novos métodos de fraude.

Os resultados dessa pesquisa nos mostram que, o uso da Inteligência Artificial (IA) tem sido de grande importância para detecção e prevenção dessas fraudes, nesse estudo foi mostrado e comparado os métodos que antigamente eram usados, com os métodos aplicados hoje pelas instituições, que nos provam ser bem mais eficazes e assertivos na prevenção e detecção de fraudes bancárias/financeiras.

Foram exemplificados alguns casos de uso que ocorreram em tempos em que não contávamos com uma grande e ampla tecnologia, casos como Fraude de Jerome Kerviel no Société Générale (2008) e o caso de Fraude de Nick Leeson no Barings Banks (1995) seriam rapidamente detectados e prevenidos por sistemas que utilizam de IA para reconhecer padrões e atividades suspeitas.

Deste modo, torna-se inegável que o uso da IA nas instituições financeiras, para detecção e prevenção de fraudes entre outros serviços, é imprescindível. É importante sempre atualizar os métodos assim que possível e buscar inovação tecnológica para essas áreas, para que a otimização sempre esteja em avanço.

REFERÊNCIAS

AZEVEDO, Frederico Luis de. **Detecção de fraudes de cartão de crédito em uma base brasileira utilizando Autoencoder**. 2021. 55 f. Dissertação (Mestrado em Computação Aplicada) - Programa de Pós-graduação em Computação Aplicada, Instituto Federal do Espírito Santo, Serra, 2021.

BARCELOS, Vanessa Azevedo; DOS SANTOS, André Moraes. **Transformação digital e seguro: uma revisão sistemática da literatura.** Revista de Gestão e Secretariado (Management and Administrative Professional Review), v. 14, n. 6, p. 8849-8874, 2023.

BELTRAN, Rafael Duarte. **Detecção de fraudes bancárias utilizando métodos de clustering.** Orientador: Alessandro Bof de Oliveira. 2019. 61 p. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) - Universidade Federal do Pampa, Curso de Ciência da Computação, Alegrete, 2019.

CAIRES, Daniel de Oliveira. **Técnicas de interpretabilidade para aprendizado de máquina: um estudo abordando avaliação de crédito e detecção de fraude**. 2022. Dissertação (Mestrado em Matemática, Estatística e Computação) - Instituto de Ciências Matemáticas e de Computação, University of São Paulo, São Carlos, 2022. doi:10.11606/D.55.2022.tde-16122022-180337.

CRISTOVÃO, Rafael Belmiro. **Detecção de fraudes em cartão de crédito**: um caso de uso de modelos supervisionados no e-commerce brasileiro. 2023. Dissertação (Mestrado em Matemática, Estatística e Computação) - Instituto de Ciências Matemáticas e de Computação, *University* of São Paulo, São Carlos, 2023.

DE LIMA, J. D. N. KOCHHANN, A. **A Inteligência Artificial na educação: as implicações no futuro do trabalho docente**. *CONTRIBUCIONES A LAS CIENCIAS SOCIALES, [S. l.]*, v. 16, n. 9, p. 17307–17318, 2023.

DE QUEIROZ MACHADO, Diego et al. **O Caso Barings: As Lições Foram Aprendidas.** Revista Alcance, v. 22, n. 2 (Abr-Jun), p. 316-329, 2015.

DE SOUZA, Daniel Henrique Miguel; BORDIN JR, Claudio J. **Detecção de fraude de cartão de crédito por meio de algoritmos de aprendizado de máquina**. Revista Brasileira de Computação Aplicada, v. 15, n. 1, p. 1-11, 2023.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

HERMANN FILHO, Roberto Max. **Escândalos financeiros: a problemática das falhas de controle de mesas de instituições financeiras durante os anos de 1995 a 2008**. 2011. 88 f. Dissertação (Mestrado em Administração) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2011.

KOHILAN, Rasenthiran et al. **A Machine Learning-based Approach for Detecting Smishing Attacks at End-user Level.** In: 2023 IEEE International Conference on e-Business Engineering (ICEBE). IEEE, 2023. p. 149-154.

KOVACH, Stephan. **Detecção de fraudes em transações financeiras via Internet em tempo real**. 2011. Tese (Doutorado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2011.

LIMA, Jardielma Queiroz de. **Detecção de fraudes em cartões de crédito utilizando técnicas de aprendizado de máquina.** 2022. 74 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Instituto Federal do Espírito Santo, Serra, 2022.

MARTINS, Emerson; GALEGALE, Napoleão Verardi. **Detecção de fraudes no segmento de crédito financeiro utilizando aprendizado de máquina: uma revisão da literatura.** Revista e-TECH: Tecnologias para Competitividade Industrial-ISSN-1983-1838, v. 15, n. 3, 2022.

MATHIJSSEN, Max; OVEREEM, Michiel; JANSEN, Slinger. **Identification of practices and capabilities in API management: a systematic literature review**. arXiv preprint arXiv:2006.10481, 2020.

OLIVEIRA, Rafael Barros de. **Aprendizado de máquinas e desafios da gestão na era dos dados: um estudo de caso na área de prevenção a fraudes bancárias**. 2019. 52 f. Trabalho de Conclusão de Curso (Bacharelado em Administração) Universidade de Brasília, Brasília, 2019.

SANCHES, Marcelo Kaminski. **Aprendizado de máquina semi-supervisionado**: proposta de um algoritmo para rotular exemplos a partir de poucos exemplos rotulados. 2003. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2003.

SANTOS, Evandro da Silva dos. **Aplicação de algoritmos de aprendizagem supervisionada de máquina em sistemas embarcados no auxílio à aplicação de defensivos agrícolas**. 2023. Dissertação (Mestrado em Tecnologias Computacionais para o Agronegócio) - Universidade Tecnológica Federal do Paraná, Medianeira, 2023.

SEMEDO, D. (2022) **Auditoria interna no setor bancário e a sua importância na prevenção e deteção da fraude**. (Dissertação de mestrado não publicada). Instituto Politécnico de Lisboa, Instituto Superior de Contabilidade e Administração de Lisboa.

SICHMAN, J. S. **Inteligência Artificial e sociedade: avanços e riscos. Estudos Avançados**, [S. l.], v. 35, n. 101, p. 37-50, 2021. DOI: 10.1590/s0103-4014.2021.35101.004. Disponível em: https://www.revistas.usp.br/eav/article/view/185024. Acesso em: 10 jan. 2024.