REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

AVALIAÇÃO DE RISCO EM TRANSAÇÕES BANCÁRIAS UTILIZANDO UM SISTEMA FUZZY BASEADO EM REGRAS LINGUÍSTICAS E PARÂMETROS COMPORTAMENTAIS

RISK ASSESSMENT IN BANKING TRANSACTIONS USING A FUZZY SYSTEM BASED ON LINGUISTIC RULES AND BEHAVIORAL PARAMETERS

EVALUACIÓN DE RIESGO EN TRANSACCIONES BANCARIAS UTILIZANDO UN SISTEMA DIFUSO BASADO EN REGLAS LINGÜÍSTICAS Y PARÁMETROS COMPORTAMENTALES

Lúcio Júnio Benfica Rosa[1]

e737322
https://doi.org/10.47820/recima21.v7i3.7322

PUBLICADO: 03/2026

RESUMO

Este artigo apresenta o desenvolvimento e a validação de um sistema *fuzzy* para avaliação de risco em transações bancárias, com foco na detecção de comportamentos suspeitos e potenciais fraudes financeiras. Diante do avanço da digitalização no setor bancário e do aumento da sofisticação das práticas fraudulentas, propõe-se uma abordagem baseada em lógica *fuzzy* do tipo Mamdani, capaz de lidar com incertezas, informações imprecisas e padrões comportamentais complexos, aproximando-se do raciocínio humano. O sistema foi modelado a partir de oito variáveis de entrada relacionadas a características financeiras, temporais e comportamentais das transações, e uma variável de saída representando o nível de risco. As regras linguísticas foram formuladas com base em conhecimento especializado e em dados empíricos provenientes de relatórios do Banco Central do Brasil (BACEN) e da Federação Brasileira dos Bancos (FEBRABAN). A implementação foi realizada em ambiente Python, utilizando a biblioteca *scikit-fuzzy*. Para validação, foram simulados 4.409 cenários distintos de transações, cujos resultados foram comparados com classificações atribuídas por um especialista em risco bancário. Os resultados indicaram elevada concordância entre o sistema *fuzzy* e o julgamento humano, alcançando 82% de concordância para cinco classes de risco e 88% quando as categorias foram agrupadas em três classes. Os achados demonstram que o modelo proposto é interpretável, robusto e eficaz como ferramenta de apoio à decisão, contribuindo para o fortalecimento dos mecanismos de segurança e mitigação de fraudes no ambiente financeiro digital.

PALAVRAS-CHAVE: Lógica Fuzzy. Detecção de Fraudes. Transações Bancárias.

ABSTRACT

This article presents the development and validation of a fuzzy system for risk assessment in banking transactions, focusing on the detection of suspicious behaviors and potential financial fraud. In light of the increasing digitalization of the banking sector and the growing sophistication of fraudulent practices, a Mamdani-type fuzzy logic approach is proposed, capable of handling uncertainty, imprecise information, and complex behavioral patterns, thereby approximating human reasoning. The system was modeled using eight input variables related to the financial, temporal, and behavioral characteristics of transactions, and one output variable representing the risk level. The linguistic rules were formulated based on expert knowledge and empirical data from reports issued by the Central Bank of Brazil and the Brazilian Federation of Banks. The implementation was carried out in a Python environment using the scikit-fuzzy library. For validation purposes, 4,409 distinct transaction scenarios were simulated, and the results were compared with classifications assigned by a banking risk specialist. The results indicated a high level of agreement

[1] Mestrando em Modelagem Computacional e Sistemas, UNIMONTES, Montes Claros-MG.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

between the system and human judgment, reaching 82% agreement for five risk classes and 88% when the categories were grouped into three classes. These findings demonstrate that the proposed model is interpretable, robust, and effective as a decision-support tool, contributing to the strengthening of security mechanisms and fraud mitigation in the digital financial environment.

KEYWORDS: *Fuzzy Logic. Fraud Detection. Banking Transactions.*

RESUMEN
Este artículo presenta el desarrollo y la validación de un sistema difuso para la evaluación del riesgo en transacciones bancarias, con énfasis en la detección de comportamientos sospechosos y posibles fraudes financieros. Ante el avance de la digitalización en el sector bancario y el aumento de la sofisticación de las prácticas fraudulentas, se propone un enfoque basado en lógica difusa de tipo Mamdani, capaz de manejar la incertidumbre, la información imprecisa y los patrones de comportamiento complejos, aproximándose al razonamiento humano. El sistema fue modelado a partir de ocho variables de entrada relacionadas con las características financieras, temporales y comportamentales de las transacciones, y una variable de salida que representa el nivel de riesgo. Las reglas lingüísticas fueron formuladas con base en conocimiento especializado y en datos empíricos provenientes de informes del Banco Central de Brasil y de la Federación Brasileña de Bancos. La implementación se realizó en un entorno Python utilizando la biblioteca scikit-fuzzy. Para la validación, se simularon 4.409 escenarios distintos de transacciones, cuyos resultados fueron comparados con las clasificaciones asignadas por un especialista en riesgo bancario. Los resultados indicaron un alto nivel de concordancia entre el sistema difuso y el juicio humano, alcanzando un 82% de concordancia para cinco clases de riesgo y un 88% cuando las categorías se agruparon en tres clases. Los hallazgos demuestran que el modelo propuesto es interpretable, robusto y eficaz como herramienta de apoyo a la toma de decisiones, contribuyendo al fortalecimiento de los mecanismos de seguridad y a la mitigación de fraudes en el entorno financiero digital.

PALABRAS CLAVE*: Lógica Difusa. Detección de Fraudes. Transacciones Bancarias.*

INTRODUÇÃO

O setor bancário tem se tornado progressivamente mais dependente de tecnologias digitais para a execução de operações financeiras, oferecendo aos clientes serviços cada vez mais rápidos e eficientes. Entretanto, essa digitalização crescente também tem ampliado a vulnerabilidade das instituições e dos usuários a fraudes financeiras, que podem ocorrer de diversas formas (Al-Ghamdi, 2023; Islam *et al.,* 2023). A sofisticação das táticas fraudulentas impõe um desafio contínuo às instituições financeiras, que buscam aprimorar seus sistemas de detecção para mitigar perdas e proteger seus clientes (Stojanović; Božić, 2022). Tais operações englobam transações não autorizadas, clonagem de cartões, transferências suspeitas e manipulação indevida de contas. As perdas decorrentes dessas práticas ilícitas são significativas, afetando diretamente a confiança do cliente, a reputação das instituições e a estabilidade do sistema financeiro. Além disso, geram custos operacionais elevados relacionados à detecção, análise e mitigação de fraudes. Estima-se que milhões de reais sejam desviados anualmente por meio dessas ações, tornando a prevenção e o monitoramento automatizado de transações um desafio central para o setor bancário. Desse modo, a detecção de fraudes bancárias é um campo

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

de pesquisa ativo que se beneficia significativamente de avanços em inteligência artificial e aprendizado de máquina para identificar e prevenir atividades ilícitas em tempo real (Mytnyk *et al.,* 2023).

Entre as abordagens mais promissoras, a lógica fuzzy destaca-se por sua capacidade de lidar com incertezas e informações imprecisas, características inerentes aos padrões comportamentais de clientes e aos indicadores de fraude. Diferentemente de modelos tradicionais baseados em classificações rígidas os sistemas fuzzy permitem representar graus de pertinência e transições suaves entre categorias, possibilitando a análise de situações ambíguas e oferecendo respostas graduais. Como afirma Sundararamaiah *et al.,* (2024), sistemas fuzzy se destacam por não se basearem em lógica booleana (sim ou não), mas sim, serem adaptativos e mais próximos do raciocínio humano, avaliando e considerando opções intermediárias

Essa flexibilidade torna o modelo mais sensível na detecção de comportamentos anômalos sem provocar um excesso de falsos positivos, que geralmente sobrecarregam os sistemas de auditoria. Além disso, a aplicação da lógica fuzzy em operações bancárias possibilita a integração de múltiplos parâmetros de risco, como valor transacionado, frequência de operações, saldo anterior, localização geográfica e variação do comportamento histórico do cliente, promovendo uma avaliação holística e adaptativa. Assim, o sistema torna-se capaz de gerar inferências interpretáveis, que auxiliam analistas humanos e sistemas automatizados de segurança na tomada de decisão, superando assim as limitações de metodologias tradicionais, que muitas vezes são baseadas exclusivamente em regras rígidas ou limiares fixos de classificação, otimizando o tempo de execução e a geração excessiva de regras, resultando em análises de risco mais intuitivas (Sánchez *et al.,* 2008).

Este artigo apresenta o desenvolvimento de um sistema fuzzy para identificação de riscos em transações bancárias, detalhando sua estrutura de modelagem, regras de inferência e processo de validação. O objetivo é demonstrar como a utilização de um modelo Mamdani, configurado com variáveis linguísticas representativas do comportamento financeiro, pode contribuir para a detecção eficiente de padrões de fraude, reduzindo perdas e fortalecendo a segurança operacional das instituições financeiras.

1. MÉTODOS

O sistema proposto para a identificação de riscos em transações bancárias foi desenvolvido com base em um modelo de inferência fuzzy do tipo Mamdani, amplamente utilizado em aplicações que envolvem incerteza, imprecisão e análise linguística. Essa abordagem possibilita representar o raciocínio humano por meio de regras lógicas do tipo “Se... então...”, permitindo que o sistema atribua graus de risco a cada operação financeira de forma contínua e interpretável. O modelo foi projetado para analisar múltiplos parâmetros relacionados ao

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

comportamento das transações, refletindo diferentes padrões de risco observados em situações reais de fraude bancária. O desenvolvimento e a validação foram conduzidos em ambiente Python, utilizando a biblioteca *scikit-fuzzy*, que oferece ferramentas para definição de variáveis, funções de pertinência, regras de inferência e defuzzificação.

1.1. Modelagem do Sistema Fuzzy

Foram definidas oito variáveis de entrada (antecedentes) e uma variável de saída (consequente), conforme apresentado na Tabela 1. A definição dessas variáveis, bem como a formulação das regras fuzzy, baseou-se em conhecimento especializado e em referências empíricas sobre fraudes bancárias. Foram considerados os principais indícios de golpes registrados em levantamentos recentes da Federação Nacional dos Bancos (FEBRABAN) e os resultados da Pesquisa de Letramento Financeiro e Inclusão Financeira de 2023, conduzida pelo Banco Central do Brasil (BACEN) em parceria com a Rede Internacional de Educação Financeira (INFE) da Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Os dados dessas fontes possibilitaram identificar os cenários mais recorrentes de ocorrência de fraudes e golpes financeiros, como transações de alto valor realizadas em horários atípicos, operações repetitivas em curto intervalo de tempo e movimentações incompatíveis com o perfil do cliente. Essas evidências foram incorporadas à modelagem fuzzy, permitindo o estabelecimento de regras linguísticas coerentes com o comportamento real das transações suspeitas, garantindo assim maior representatividade e realismo ao sistema desenvolvido.

Tabela 1. Relação das variáveis consideradas para identificação de riscos em transações bancárias

Variável	Descrição	Faixa
type_trans	Tipo de transação: depósito, saque, débito, crédito, pagamento, transferência	0 – 5
amount	Valor da transação (R$)	0 – 20.000
oldbalanceOrig	Saldo anterior	0 – 50.000
newbalanceOrig	Saldo após a transação	0 – 50.000
hour	Horário em que a transação foi efetuada	0 – 23
freq	Frequência de transações recentes	0 – 20
rel_balance	Relação entre saldos (novo/antigo)	0 – 2
amt_vs_balance	Relação entre valor da transação e saldo disponível	0 – 2
risco	Nível de risco associado à transação	0 – 20

Fonte: Autor (2025).

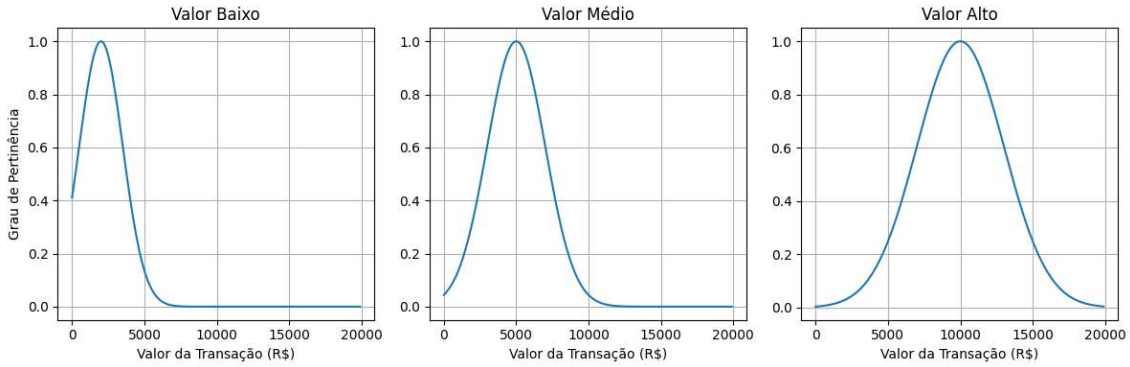
Cada variável foi associada a funções de pertinência específicas, projetadas para representar de forma realista a variação observada em dados financeiros. A Figura 1 mostra os gráficos de pertinência da variável '*amount*'. Outro exemplo, a variável *'amt_vs_balance'* utiliza funções trapezoidais e triangulares para identificar situações em que o valor transacionado é maior que o saldo disponível, um indicador clássico de risco elevado. É importante destacar a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

diferença conceitual entre as variáveis '*amt_vs_balance*' e '*rel_balance*'. Enquanto a primeira descreve a relação entre o valor da transação e o saldo disponível em conta, permitindo identificar casos em que o cliente tenta movimentar quantias superiores ao limite existente, situação frequentemente associada a tentativas de fraude, a segunda está relacionada ao impacto da operação sobre o saldo.

Em outras palavras, '*rel_balance'* mede o quanto o saldo da conta foi alterado após a transação, independentemente de o valor transacionado ser superior ou não ao saldo inicial. Essa distinção é fundamental para garantir que o sistema fuzzy consiga captar tanto a intenção de uma movimentação irregular quanto o efeito da operação no comportamento financeiro do cliente.

Figura 1. Gráficos que ilustram a função de pertinência da variável 'amount' indicando o valor da transação que pode ser classificado como baixo, médio, alto



Fonte: Dados da Pesquisa (2025).

1.2. Base de Regras Fuzzy

A base de conhecimento foi estruturada com 17 regras linguísticas, formuladas com base em padrões típicos de fraude bancária observados na prática e com base nos estudos já citados. Alguns exemplos incluem:

- Regra 1: Se tipo de transação é "depósito", então risco é baixíssimo.
- Regra 8: Se mudança do saldo for 'queda forte', risco moderado;
- Regra 14: Se valor é maior que saldo disponível, então risco é altíssimo.
- Regra 17: Se tipo da transação é crédito ou débito e frequência é alta, risco é alto.

Essas regras foram implementadas por meio da classe *ctrl.Rule* do módulo *skfuzzy.control*, permitindo combinações de múltiplos antecedentes com operadores lógicos & (E) e | (OU).

1.3. Processo de Inferência e Defuzzificação

O sistema executa quatro etapas principais, sendo elas: a) Fuzzificação, onde ocorre a conversão dos valores de entrada em graus de pertinência nos conjuntos fuzzy; b) Inferência:

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

aplica as regras definidas combinando antecedentes e consequentes; c) Agregação que combina os resultados parciais em um conjunto fuzzy de saída; e por fim d) Defuzzificação: transforma o conjunto fuzzy resultante em um valor numérico representando o risco, usando o método do centroide. Esse processo gera uma saída contínua, normalmente variando de 0 a 20, interpretada conforme a Tabela 2.

Tabela 2. Relação das faixas numéricas, categorias linguísticas e interpretação de risco do sistema fuzzy

Faixa de saída	Categoria Linguística	Interpretação
0-4	Baixíssimo	Operação segura
4-8	Baixo	Risco Residual
8-12	Moderado	Atenção recomendada
12-16	Alto	Transação suspeita
16-20	Altíssimo	Possível fraude

Fonte: Autor (2025).

1.4. Condução de testes e checagem dos resultados

A etapa de verificação da acurácia do modelo teve como objetivo avaliar a capacidade do sistema fuzzy em reproduzir, de forma consistente, o raciocínio humano aplicado à avaliação de risco em transações bancárias. Para tanto, foram conduzidos testes que simulam situações reais e plausíveis de movimentações financeiras, abrangendo uma ampla variedade de cenários. Cada variável de entrada do modelo, como tipo de operação, valor da transação, saldo anterior, horário de execução, frequência de movimentações e relação entre o valor e o saldo, recebeu uma lista de valores representativos, previamente definidos com base em padrões de comportamento observados no ambiente bancário.

Essas listas foram combinadas entre si, gerando um total de 4.409 cenários distintos. Cada cenário foi processado pelo sistema fuzzy, que produziu um consequente valor de risco associado àquela transação. O resultado de todas as simulações foi exportado para um arquivo em formato CSV, que serviu como base para a etapa de validação comparativa.

Nessa etapa, os mesmos cenários foram analisados por um especialista em risco bancário, que atribuiu uma classificação de risco a cada situação com base em sua experiência e critérios técnicos. Para sistematizar o processo e reduzir a subjetividade, a avaliação do especialista foi implementada de forma automatizada, por meio da atribuição de pesos diferenciados a características específicas dos cenários, como o valor transacionado em relação ao saldo disponível, o horário da operação e a frequência de movimentações. Dessa forma, buscou-se representar de maneira quantitativa o julgamento humano, permitindo a comparação direta posterior com as inferências do sistema fuzzy.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

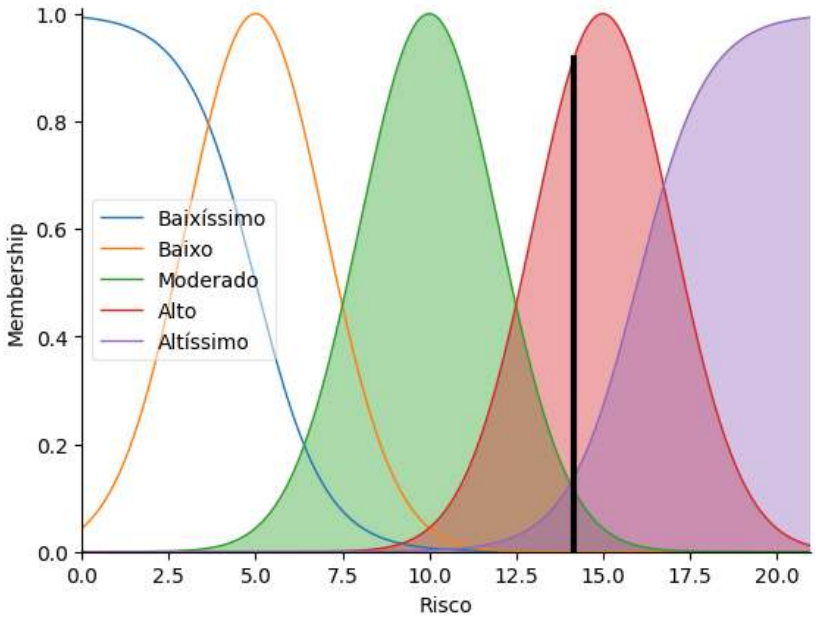
2. RESULTADOS

As simulações demonstraram que o sistema respondeu de forma coerente às combinações de variáveis que representam comportamentos típicos de transações legítimas e fraudulentas. Nos cenários isolados testados, observou-se que o modelo foi capaz de captar com precisão as principais nuances das variáveis propostas, refletindo corretamente o grau de risco associado a cada situação.

A Figura 2 ilustra um exemplo de cenário simulado em que foi realizada uma transação no valor de R$ 5.000,00, enquanto a conta possuía apenas R$ 1.000,00 de saldo disponível. Nessa simulação, foram efetuadas cinco tentativas consecutivas de pagamento de boleto às duas horas da manhã. Considerando o horário atípico, a repetição de tentativas e o valor superior ao saldo existente, o sistema fuzzy classificou a operação como de alto risco, identificando o padrão característico de uma possível tentativa de fraude ou golpe eletrônico.

O resultado obtido mostra que o modelo é sensível a combinações complexas de fatores, avaliando simultaneamente condições temporais, financeiras e comportamentais.

Figura 2. Gráfico de saída do sistema de classificação de risco fuzzy, para uma transação de R$ 5.000,00 reais feita às 2 horas da manhã, após cinco tentativas



Fonte: Dados da Pesquisa (2025).

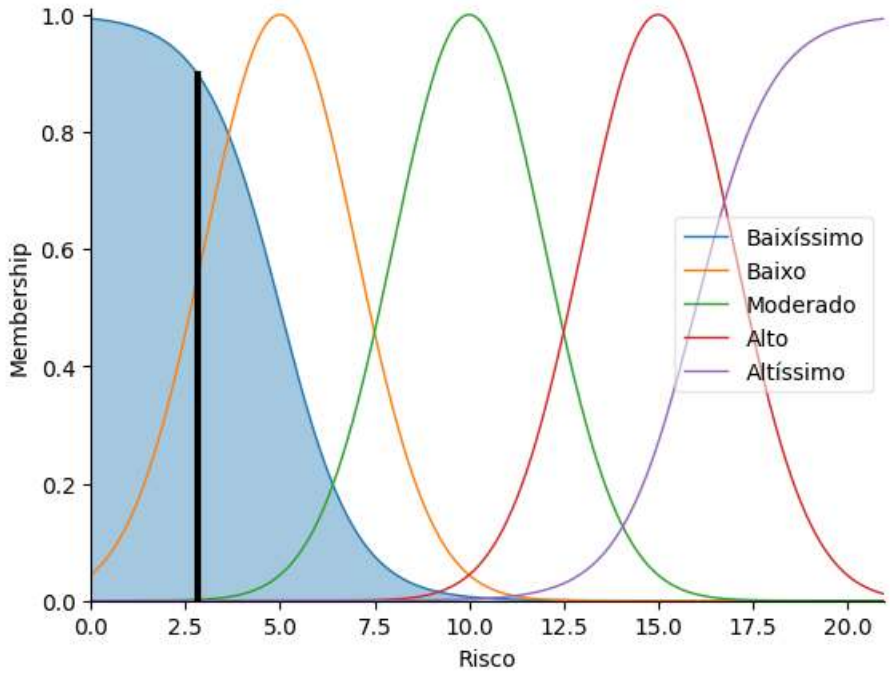
Do mesmo modo, o sistema demonstrou capacidade de interpretar e ponderar as regras conforme sua relevância contextual, evitando classificações precipitadas em situações que, embora atípicas, não representam efetivamente risco de fraude. A Figura 3 apresenta um exemplo

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

desse comportamento: uma simulação de depósito bancário no valor de R$ 2.000,00, realizado às 3 horas da manhã. Apesar de o horário ser incomum e o valor relativamente elevado, o sistema fuzzy classificou corretamente a transação como de Baixo/Baixíssimo risco, reconhecendo que depósitos representam entrada de recursos e, portanto, não configuram ameaça direta à integridade da conta.

Esse resultado evidencia a capacidade interpretativa do modelo, que consegue distinguir operações potencialmente suspeitas daquelas inerentemente seguras, analisando o significado semântico de cada tipo de transação e não apenas seus parâmetros numéricos.

Figura 3. Inferência fuzzy em cenário de depósito bancário no valor de R$ 2.000,00 feito às 3 horas da manhã



Fonte: Dados da Pesquisa (2025).

2.1. Comparação cenários hipotéticos com especialista

Os resultados demonstraram um elevado grau de concordância entre as classificações fornecidas pelo sistema fuzzy e aquelas atribuídas pelo especialista. Quando consideradas as cinco categorias originais de risco (Baixíssimo, Baixo, Moderado, Alto e Altíssimo) a concordância alcançada foi de 82%, o que indica uma correspondência substancial entre o modelo e o julgamento humano. Esse índice evidencia que o sistema foi capaz de aprender e reproduzir, com alto nível de precisão, a lógica subjacente às decisões do especialista.

Adicionalmente, ao se agrupar as categorias Baixíssimo e Baixo e Alto e Altíssimo em uma única classe, de modo a reduzir a granularidade do problema para três classes de risco, a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

concordância observada elevou-se para 88%. Na Tabela 3 podemos ver o comparativo geral e a matriz de confusão considerando cinco e três classes, entre as classificações do sistema fuzzy e do especialista. Podemos notar que a simplificação, que reflete uma visão mais prática da análise de risco no ambiente bancário, reforça a robustez e a generalização do modelo, indicando que o sistema fuzzy é capaz de capturar adequadamente os padrões de risco de maneira coerente com a percepção humana, mesmo sob diferentes níveis de categorização.

Tabela 3. Matriz de confusão detalhada das predições feitas pelo analista e pelo sistema fuzzy

Classe prevista pelo especialista / Classe prevista pelo sistema Fuzzy	**Baixíssimo**	**Baixo**	**Moderado**	**Alto**	**Altíssimo**	**Total Especialista**
Baixíssimo	491	70	5	8	14	588
Baixo	33	326	11	3	1	374
Moderado	55	120	1986	135	38	2334
Alto	6	7	34	439	79	565
Altíssimo	2	9	72	74	391	548
Total Previsto	567	536	2014	824	468	**4409**

Classe prevista pelo especialista / Classe prevista pelo sistema Fuzzy	**Baixo**	**Moderado**	**Alto**	**Total Especialista**
Baixo	920	16	26	962
Moderado	175	1986	173	2334
Alto	24	106	983	1113
Total Previsto	1119	2108	1182	**4409**

Fonte: Autor (2025).

De acordo com a Tabela 3 – Matriz de confusão detalhada das predições feitas pelo analista e pelo sistema fuzzy, observa-se que a redução do número de classes de cinco para três resultou em um ganho significativo de desempenho. Essa simplificação diminuiu as fronteiras de decisão entre as categorias, reduzindo as ambiguidades e, consequentemente, elevando a acurácia global das predições.

No modelo com cinco classes (Baixíssimo, Baixo, Moderado, Alto e Altíssimo), há uma distribuição mais granular de níveis de risco, o que proporciona maior sensibilidade, porém aumenta a probabilidade de erros em regiões de transição, especialmente entre *Moderado* e *Alto*, e entre *Alto* e *Altíssimo*. Já no modelo agrupado em três classes (Baixo, Moderado e Alto), observa-se uma melhor consistência nas classificações, com maior alinhamento entre as predições do sistema e as avaliações do especialista humano. Essa agregação reduziu a sobreposição entre conjuntos fuzzy adjacentes, simplificando o processo de inferência e favorecendo resultados mais estáveis.

Os casos de falso-positivo e falso-negativo, situações em que o especialista classificou uma transação com um grau de risco distinto do previsto pelo sistema, ocorrem principalmente

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

nas extremidades da escala. Por exemplo, em alguns casos, o especialista classificou uma operação como de risco Altíssimo, enquanto o sistema fuzzy a interpretou como 'Baixíssimo'. Tais discrepâncias são explicadas pela não priorização de determinadas variáveis críticas no processo de inferência ou pela combinação de regras com baixo grau de ativação, que, somadas, podem deslocar o resultado para uma classe mais amena.

Situações desse tipo tendem a ocorrer em transações de valor intermediário**,** realizadas em horários de menor risco (como o horário comercial) e em uma única tentativa, mas que apresentam alto valor relativo de '*amount*' e '*rel_balance'*, ou seja, movimentações que, embora pareçam normais sob alguns critérios, implicam variações abruptas de saldo ou magnitude elevada em relação ao histórico da conta. Nessas condições, o especialista humano, considerando contexto e intuição, tende a atribuir risco mais elevado (*Alto* ou *Altíssimo*), enquanto o sistema fuzzy, por depender exclusivamente das funções de pertinência definidas, pode suavizar o resultado para Moderado *ou* Baixo.

Em síntese, a análise das matrizes evidencia que a redução de classes trouxe ganhos em desempenho e estabilidade, sem comprometer a interpretabilidade do sistema. Além disso, destaca-se a importância de refinar os pesos das variáveis mais sensíveis, como '*amount'*, '*rel_balance'* e '*hour'*, além de ajustar as funções de pertinência e regras de inferência para aproximar ainda mais o comportamento do sistema fuzzy ao julgamento do especialista. Esse ajuste fino é essencial para minimizar as divergências extremas e aprimorar a confiabilidade do modelo em contextos de análise de risco financeiro.

3. CONSIDERAÇÕES

Assim, os resultados obtidos demonstram que o modelo proposto apresenta excelente desempenho preditivo e interpretabilidade, validando sua aplicação como uma ferramenta de apoio à decisão no contexto de monitoramento e classificação de risco em transações bancárias. A alta taxa de concordância com o julgamento especializado evidencia que o sistema fuzzy pode atuar como um instrumento confiável e transparente, apto a complementar o processo de análise humana e a contribuir para a mitigação de fraudes e comportamentos suspeitos no ambiente financeiro. Em síntese, o modelo fuzzy desenvolvido valida-se como uma ferramenta de apoio à decisão eficiente no contexto de detecção de riscos e fraudes bancárias, capaz de complementar a análise humana e fortalecer os mecanismos automatizados de segurança utilizados pelas instituições financeiras.

Como perspectivas de trabalhos futuros, recomenda-se: a integração do sistema fuzzy com algoritmos de aprendizado de máquina supervisionado, formando um modelo híbrido (neuro-fuzzy) para aprimorar o desempenho preditivo; a incorporação de variáveis comportamentais adicionais, como geolocalização e dispositivo utilizado e a validação do sistema em bases de

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

dados reais de transações bancárias, com o objetivo de aferir métricas quantitativas de acurácia e tempo de resposta em ambiente operacional. Dessa forma, o sistema fuzzy proposto confirma seu potencial como solução inteligente, adaptativa e explicável para a mitigação de fraudes e o fortalecimento da segurança financeira digital.

REFERÊNCIAS

AL-GHAMDI, B. A. M. A. -R. Selection of a Trustworthy Technique for Fraud Prevention in the Digital Banking Sector. **International Journal of Advanced Computer Science and Applications**, v. 14, n. 11, 2023. DOI: 10.14569/IJACSA.2023.0141124.

BACEN. **Relatório de Letramento Financeiro**. Brasília: Banco Central do Brasil, 2023. Disponível em: https://www.bcb.gov.br/cidadaniafinanceira/letramento_financeiro. Acesso em 10 nov. 2025.

FEBRABAN. **Fraudes Bancárias**. Brasília: Federação Brasileira dos Bancos, s. d. Disponível em: https://portal.febraban.org.br/AntiFraude/. Acesso em 10 nov. 2025.

ISLAM, S.; HAQUE, M. M.; KARIM, A. N. M. R. *A rule-base machine learning model for financial fraud detection.* **International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer**, v. 14, n. 1, 2023. DOI: http://doi.org/10.11591/ijece.v14i1.pp759-771.

MYTNYK, B.; TKACHYK, O.; SHAKHOVSKA, N. *Application of Artificial Intelligence for Fraudulent Banking Operations Recognition.* **Big Data Cogn. Comput**., v. 7, n. 2, 93, 2023. DOI: 10.3390/bdcc7020093.

SANCHEZ, D.; VILA, M. A.; CERDA, L.; SERRANO, J. -M. *Association rules Applied to credit card fraud detection*. **Expert Systems with Applications**, v.36, n. 2, 2008. DOI: https://doi.org/10.1016/j.eswa.2008.02.001.

STOJANOVIĆ, B.; BOŽIĆ, J. Robust Financial Fraud Alerting System Based in the Cloud Environment. **Sensors,** v. 22, n. 23, 9461, 2022. DOI: https://doi.org/10.3390/s22239461.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.