

Campus Porto Velho Zona Norte
Coordenação do Curso Superior de Tecnologia em Sistemas para Internet

LETÍCIA DAS NEVES LESSA

**FRAUDES POR CLONAGEM DE CARTÕES EM TRANSAÇÕES ONLINE NO
BRASIL: RISCOS E ESTRATÉGIAS DE PREVENÇÃO E DETECÇÃO**

PORTO VELHO

2026

LETÍCIA DAS NEVES LESSA

**FRAUDES POR CLONAGEM DE CARTÕES EM TRANSAÇÕES ONLINE NO
BRASIL: RISCOS E ESTRATÉGIAS DE PREVENÇÃO E DETECÇÃO**

Artigo tecnológico entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – (IFRO), *Campus* Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso de Sistemas Para Internet, sob a orientação da professora Juliana Braz da Costa

PORTO VELHO
2026

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Lessa, Leticia das Neves.

Fraudes por clonagem de cartões em transações online no Brasil: riscos e estratégias de prevenção e detecção / Leticia das Neves Lessa. - Porto Velho, 2026.

19 f. : il.

Orientador(a): Prof^{ra}. Juliana Braz da Costa.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Sistemas para Internet) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2026.

1. fraude digital. 2. clonagem de cartões. 3. comércio eletrônico. 4. engenharia social . 5. segurança em pagamentos . I. Costa, Juliana Braz da (orient.). II. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. III. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-11/914

LETÍCIA DASNEVES LESSA

**FRAUDES POR CLONAGEM DE CARTÕES EM TRANSAÇÕES ONLINE NO BRASIL:
RISCOS E ESTRATÉGIAS DE PREVENÇÃO E DETECÇÃO**

Artigo tecnológico entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – (IFRO), *Campus* Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso de Sistemas Para Internet, sob a orientação da professora Juliana Braz da Costa

Aprovado em: 19/08/2026 pela banca examinadora.

Documento assinado digitalmente
 **ALAN JHONE CARVALHO DE ARAUJO**
Data: 13/10/2026 19:22:12-0300
Verifique em <https://validar.iti.gov.br>

Alan Jhone Carvalho de Araujo

Documento assinado digitalmente
 **MARIA IVANILSE CALDERON RIBEIRO**
Data: 13/10/2026 17:24:16-0300
Verifique em <https://validar.iti.gov.br>

Maria Ivanilse Calderon Ribeiro

Documento assinado digitalmente
 **JULIANA BRAZ DA COSTA**
Data: 07/10/2026 17:19:51-0300
Verifique em <https://validar.iti.gov.br>

Juliana Braz da Costa (Orientadora)

FRAUDES POR CLONAGEM DE CARTÕES EM TRANSAÇÕES ONLINE NO BRASIL: RISCOS E ESTRATÉGIAS DE PREVENÇÃO E DETECÇÃO

RESUMO: O presente trabalho analisa a evolução das fraudes por clonagem de cartões e uso indevido de dados em transações online no Brasil entre 2019 e 2024. O objetivo central consiste em descrever as transformações do ecossistema de pagamentos digitais, os riscos associados e as principais estratégias de prevenção e detecção documentadas na literatura científica e em marcos regulatórios. Metodologicamente, a pesquisa caracteriza-se como bibliográfica e documental, de natureza qualitativa e descritivo-exploratória, fundamentada em 14 documentos, compreendendo artigos científicos, trabalhos acadêmicos e normativos institucionais. Os resultados indicam que o fenômeno sofreu uma mutação qualitativa: a tradicional clonagem física deu lugar a fraudes baseadas na apropriação remota de credenciais, *phishing*, engenharia social e exploração de vulnerabilidades em transações sem a presença física do titular (*Card-Not-Present*). Conclui-se que o enfrentamento do problema exige uma abordagem sistêmica, integrando barreiras técnicas de autenticação forte, modelos adaptativos de aprendizado de máquina, governança regulatória e educação continuada dos usuários.

Palavras-chave: Fraude digital; Clonagem de cartões; Comércio eletrônico; Engenharia social; Segurança em pagamentos.

ABSTRACT: This paper analyzes the evolution of card cloning fraud and data misuse in online transactions in Brazil between 2019 and 2024. The main objective is to describe the transformations in the digital payments ecosystem, the associated risks, and the primary prevention and detection strategies documented in scientific literature and regulatory frameworks. Methodologically, the research is bibliographic and documental, with a qualitative and descriptive-exploratory approach, based on a set of 14 documents, including scientific papers, academic works, and institutional regulations. The results indicate that the phenomenon has undergone a qualitative mutation: traditional physical cloning has given place to fraud based on remote credential appropriation, phishing, social engineering, and the exploitation of vulnerabilities in Card-Not-Present transactions. It is concluded that tackling the problem requires a systemic approach, integrating strong technical authentication barriers, adaptive machine learning models, regulatory governance, and continuous user education.

Keywords: Digital fraud; Card cloning; E-commerce; Social engineering; Payment security.

1.INTRODUÇÃO

Com o avanço da tecnologia, as formas de pagamento passaram por transformações significativas, em que o dinheiro físico cedeu espaço aos cartões e às transferências digitais, facilitando o comércio eletrônico e as operações remotas (Bacellar; Toporoski, 2024). Contudo, essa mesma evolução que trouxe conveniência financeira acarretou uma série de desafios de segurança. Em 2024, as tentativas de fraudes bancárias cresceram 10,4% no Brasil, gerando um prejuízo potencial estimado em R\$ 51,6 bilhões, cenário no qual 50,7% dos brasileiros afirmaram ter sido vítimas de algum golpe no último ano (Serasa Experian, 2025).

A agilidade e a praticidade dessas transações elevaram a suscetibilidade a uma variedade de ameaças, com destaque para a clonagem de cartões. Diferentemente da fraude tradicional, dependente da cópia física do plástico, atualmente os ataques evoluíram para o ambiente virtual por meio de *phishing*, engenharia social avançada e exploração de vulnerabilidades em transações sem a presença física, as chamadas operações *Card-Not-Present* (Fornasier; Knebel; Silva, 2020; ABECS, 2024). Diante desse cenário, a responsabilidade das instituições financeiras tem sido cada vez mais questionada pelos consumidores, que buscam reparação pelos danos decorrentes dessas invasões.

Para mitigar essas ameaças, a legislação brasileira passou por importantes atualizações. A implementação da Lei Geral de Proteção de Dados (LGPD) instituída pela Lei nº 13.709/2018, tornou-se essencial para garantir a privacidade dos titulares, exigindo dos operadores e controladores, como as instituições financeiras, a adoção de medidas rigorosas de segurança (Brasil, 2018; Bacellar; Toporoski, 2024). Posteriormente, a promulgação da Lei nº 14.155/2021 tornou mais graves os crimes de furto e estelionato cometidos de forma eletrônica, fortalecendo a responsabilização dos criminosos no ciberespaço (Brasil, 2021).

É neste contexto regulatório e tecnológico que se insere a presente pesquisa, desenvolvida no Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), Campus Porto Velho Zona Norte. O problema central deste estudo consiste em investigar: como a literatura e a documentação institucional descrevem a evolução das fraudes por clonagem de cartões em transações online no Brasil, seus riscos e as principais estratégias de

prevenção e detecção no período de 2019 a 2024? Para responder a esta questão, o objetivo geral é analisar essa evolução, enquanto os objetivos específicos desdobram-se em contextualizar a expansão online, conceituar a clonagem digital, mapear as técnicas fraudulentas e os riscos sistêmicos, e sistematizar as barreiras de contenção tecnológica.

A relevância deste trabalho transcende a análise teórica, conectando-se diretamente à prática e à responsabilidade técnica dos futuros profissionais de Sistemas para Internet. Seja atuando no suporte operacional a infraestruturas corporativas, na configuração de redes e manutenções de sistemas, ou no desenvolvimento de soluções voltadas para a web, esses especialistas encontram-se na vanguarda da defesa cibernética. Portanto, compreender a fundo as mecânicas das fraudes financeiras e as diretrizes de governança exigidas pela LGPD é indispensável. Dessa forma, almeja-se que este estudo contribua para a formação de tecnólogos capazes de integrar a segurança da informação desde a concepção dos sistemas, fortalecendo a credibilidade das plataformas de pagamento e promovendo um ambiente digital mais seguro para a sociedade.

2. REVISÃO DE LITERATURA

2.1 CONTEXTO DA EXPANSÃO DAS TRANSAÇÕES ONLINE NO BRASIL

A expansão das transações online no Brasil integra um processo mais amplo de digitalização dos meios de pagamento e dos serviços financeiros, que se intensificou de forma expressiva na última década. Segundo o Banco Central do Brasil (2022) "o uso de meios digitais para fins de transações financeiras no Brasil cresceu de forma acelerada", impulsionado pela convergência entre reformas regulatórias, inovações tecnológicas e o acirramento da competitividade no setor financeiro (*open banking* e arranjos instantâneos).

No rastro dessa digitalização, os pagamentos eletrônicos evoluíram em paralelo à consolidação do comércio eletrônico. Dados do Ministério do Desenvolvimento, Indústria, Comércio e Serviços apontam que o e-commerce brasileiro movimentou R\$ 196,1 bilhões em 2023, registrando expansão contínua e atestando a centralidade das plataformas digitais no consumo cotidiano (Brasil, 2024). Tal dinamismo foi viabilizado pela ampliação da conectividade estrutural: em 2023, o IBGE (2024) registrou acesso à internet em 72,5 milhões de domicílios (92,5% do total

nacional), com avanços significativos inclusive nas zonas rurais.

Paralelamente, a Pesquisa de Tecnologia Bancária da Febraban (2024) indicou que os canais digitais responderam por 79% de todas as transações bancárias realizadas em 2023, com mais de 130 bilhões de operações conduzidas via smartphones. Esse cenário foi drasticamente catalisado pela pandemia da Covid-19 e consolidado pela introdução do Pix em novembro de 2020. Entre 2019 e 2024, portanto, consolidou-se um ecossistema altamente integrado, que, embora tenha gerado inclusão financeira e conveniência, elevou a dependência de operações remotas e intensificou os riscos de exposição de dados sensíveis.

2.2 CONCEITO DE CLONAGEM DE CARTÕES E FRAUDES EM AMBIENTE DIGITAL

A compreensão da clonagem de cartões no contexto das transações online exige uma profunda ampliação conceitual em relação à acepção tradicional de cópia física do plástico bancário. Historicamente vinculada à duplicação de trilhas magnéticas ou à instalação de dispositivos de captura (*skimmers*) em caixas eletrônicos e POS (*Point of Sale*), a fraude no ambiente digital assume características fluidas. Em operações não presenciais (*Card-Not-Present*), a conduta delituosa concretiza-se pela obtenção, armazenamento e uso não autorizado de dados primários da conta (PAN, data de validade e código CVV), ainda que o instrumento físico permaneça sob a guarda do titular.

Essa transmutação conceitual é respaldada pelo *PCI Security Standards Council* (PCI SSC, 2023), que distingue rigorosamente as operações presenciais daquelas concluídas sem a apresentação material do cartão. Em convergência, especificações técnicas da EMVCo (2022) destacam que protocolos como o EMV 3-D *Secure* foram desenvolvidos precisamente para mitigar o risco inerente às transações eletrônicas remotas. Maragno e Yamazato (2026) corroboram ao observar que, no período recente, a clonagem física perdeu relevância relativa frente ao roubo cibernético de credenciais e a testes automatizados de cartões em *e-commerces*.

Ademais, essas fraudes não se limitam a falhas de arquitetura tecnológica, envolvendo de maneira central a manipulação comportamental. Conforme o Ministério Público do Estado de Mato Grosso (Mato Grosso, 2025, p. 2), o pilar que sustenta grande parte dessas ações é a engenharia social, técnica voltada a induzir a vítima a

entregar voluntariamente seus dados ou autorizar transações contra os próprios interesses.

2.3 ENGENHARIA SOCIAL: O PHISHING E OS VETORES COMPORTAMENTAIS

A engenharia social consolidou-se como o vetor primário das fraudes digitais contemporâneas por direcionar seus ataques ao elo mais vulnerável da cadeia de segurança: o ser humano. Conforme apontam Fornasier, Knebel e Silva (2020), o método abrange estratégias voltadas a manipular o indivíduo mediante o esgotamento de sua capacidade crítica, explorando vieses cognitivos como urgência, medo e autoridade.

Tetri e Vuorinen (2013) estruturam esses ataques em três dimensões complementares: a persuasão (*persuasion*), a fabricação de personas ou cenários fidedignos (*fabrication*) e o mapeamento prévio de informações sobre a vítima (*data gathering*). No ecossistema de pagamentos, o *phishing* destaca-se como a principal ferramenta dessa categoria. Hadnagy (2018) define o *phishing* como o uso de comunicações fraudulentas simulando fontes legítimas (bancos, *e-commerces*, órgãos públicos) para extrair credenciais ou injetar códigos maliciosos.

O CERT.br ([s.d.]) complementa que o emprego de artifícios como mensagens falsas em SMS (*smishing*), aplicativos de mensagens e páginas web clonadas reproduz com exatidão a identidade visual de instituições financeiras, induzindo o usuário a decisões precipitadas.

2.4 PRINCIPAIS TÉCNICAS UTILIZADAS NAS FRAUDES ONLINE

Nas operações classificadas como *Card-Not-Present* (CNP), termo técnico validado pela ABECS (2024), a fraude dispensa o contato físico com o cartão, exigindo apenas a transcrição remota de dados. No direito regulatório brasileiro, o Banco Central distingue os golpes (onde o cliente colabora ativamente sob indução em erro) das fraudes estritas, onde o sistema é invadido ou dados são vazados sem anuência direta. Dentre as principais tipologias descritas na literatura, destacam-se:

- **Falsa central de atendimento:** O fraudador simula contato telefônico ou utiliza técnicas de *spoofing* para mascarar números oficiais, alertando sobre falsas transações irregulares ou clonagens, coagindo o correntista a revelar senhas e

códigos de segurança (FEBRABAN, 2024).

- **Golpe do acesso remoto ("mão fantasma"):** O golpista convence a vítima a instalar softwares de acesso remoto sob o pretexto de prestar suporte técnico ou segurança, assumindo o controle do dispositivo móvel ou computador para efetuar transferências e compras (FEBRABAN, 2024).
- **Fraudes híbridas (falso motoboy e maquininha adulterada):** Casos em que a abordagem inicial física (como a entrega de mercadorias com cobrança em maquininhas de visor danificado ou a retirada de cartões supostamente bloqueados por falsos portadores) resultam imediatamente em transações digitais fraudulentas (Banco Central do Brasil, 2024).

2.5 RISCOS PARA CONSUMIDORES, EMPRESAS E INSTITUIÇÕES FINANCEIRAS

As repercussões das fraudes por clonagem e uso indevido de dados geram impactos multidimensionais. Para os consumidores, além da perda patrimonial direta que atinge 54,2% das vítimas de golpes segundo a Serasa Experian (2025), há a erosão da privacidade e o aumento do risco percebido nas compras online, fator que afeta a confiança digital (Kovacs; Farias, 2004).

Para as empresas de comércio eletrônico, os riscos abarcam perdas por *chargebacks*, contestações de compra, custos operacionais com sistemas de barreira e acentuado desgaste reputacional (Coelho *et al.*, 2006). No plano institucional, as instituições financeiras enfrentam pressões regulatórias rigorosas, expressas na Resolução BCB nº 85/2021, política de segurança cibernética, e na Resolução CMN nº 4.935/2021, responsabilidade sobre correspondentes e canais terceirizados, além do impacto macroeconômico decorrente de bilhões de reais em tentativas de fraude evitadas ou consumadas anualmente (Serasa Experian, 2025).

2.6 ESTRATÉGIAS DE PREVENÇÃO E DETECÇÃO

A defesa contra fraudes em cartões exige a articulação síncrona entre barreiras preventivas e mecanismos de detecção. No âmbito preventivo, destacam-se a autenticação multifatorial, a tokenização de credenciais e os protocolos de dupla checagem baseados em risco, a exemplo do EMV 3DS (ABECS, 2024).

No campo da detecção, a literatura enfatiza a insuficiência de regras estáticas, exigindo o emprego de inteligência computacional. Souza e Bordin Júnior (2023) demonstram a eficácia de algoritmos de *ensemble learning* para lidar com bases transacionais altamente desbalanceadas (onde transações legítimas superam em ordens de grandeza os eventos fraudulentos).

Da Pozzolo *et al.* (2018) e Paldino *et al.* (2024) reforçam que os sistemas modernos precisam ser adaptativos, combatendo o conceito de desvio de conceito (*concept drift*) — mudança contínua no comportamento dos fraudadores — por meio da diversificação e atualização contínua de classificadores inteligentes.

3. METODOLOGIA

Esta pesquisa caracteriza-se como bibliográfica e documental, dotada de abordagem qualitativa e caráter descritivo-exploratório, com o propósito de examinar a evolução das fraudes por clonagem de cartões em transações online no Brasil entre 2019 e 2024.

A coleta de dados bibliográficos e documentais foi conduzida mediante buscas sistemáticas nas plataformas *Google Scholar* e *Portal de Periódicos CAPES*. Para o mapeamento do acervo, foram empregados descritores combinados em português e inglês, tais como: "clonagem de cartões", "fraude em cartão de crédito", "engenharia social", "cartão não presente" (*Card-Not-Present*), "prevenção e detecção de fraude" e "*credit card fraud detection*".

Complementarmente, a pesquisa documental englobou relatórios estatísticos, cartilhas técnicas e atos normativos emitidos por órgãos reguladores e entidades do setor financeiro, como o Banco Central do Brasil (BCB), a Federação Brasileira de Bancos (FEBRABAN) e a Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS).

A seleção do material seguiu critérios rigorosos de elegibilidade. Como critérios de inclusão, adotaram-se: aderência direta à temática de fraudes em transações online, publicação no recorte temporal entre 2019 e 2024, autoria identificada e redação nos idiomas português ou inglês. Como critérios de exclusão, descartaram-se artigos duplicados entre as bases, estudos com abordagem genérica sobre

segurança cibernética sem foco em pagamentos eletrônicos e materiais sem validação acadêmica ou institucional.

Após a aplicação desses filtros, o conjunto documental final foi consolidado em exatamente 14 documentos, abrangendo 10 artigos científicos publicados em periódicos nacionais e internacionais, 1 trabalho acadêmico de conclusão de curso (TCC) focado em algoritmos de detecção, e 3 documentos institucionais e normativos regulatórios. A relação detalhada dos materiais que compõem o material de análise é estruturada a seguir:

RELAÇÃO CONSOLIDADA DO CONJUNTO DOCUMENTAL DA PESQUISA (14 DOCUMENTOS)

ARTIGOS CIENTÍFICOS E PERIÓDICOS (10 DOCUMENTOS):

1. BACELLAR, Leandro Wünsche; TOPOROSKI, Elizeu Luiz (2024). Clonagem de cartão de crédito sob a perspectiva da Lei Geral de Proteção de Dados. *Academia de Direito*.
2. CHERIF, Asma et al. (2023). Credit card fraud detection in the era of disruptive technologies. *Journal of King Saud University*.
3. COELHO, Leandro dos sintomas et al. (2006). FControl: sistema inteligente inovador para detecção de fraudes. *Gestão & Produção*.
4. DAL POZZOLO, Andrea et al. (2018). Credit card fraud detection: a realistic modeling and a novel learning strategy. *IEEE Transactions*.
5. FORNASIER, Mateus de Oliveira; KNEBEL, Norberto; SILVA, Daniel (2020). Phishing e engenharia social. *Meritum*.
6. KOVACS, Michelle Helena; FARIAS, Salomão Alencar de (2004). Dimensões de riscos percebidos nas compras pela internet. *RAE-eletrônica*.
7. MARAGNO, Ryan; YAMAZATO, Fauzi Anderson (2026). O estado da fraude e do estelionato digital no Brasil. *Revista do Ministério Público Militar*.
8. PALDINO, Gian Marco et al. (2024). The role of diversity and ensemble learning in credit card fraud detection. *Advances in Data Analysis*.
9. SOUZA, Daniel Henrique Miguel de; BORDIN JÚNIOR, Claudio José (2023). Novo algoritmo ensemble para detecção de fraude. *Revista Tecnologia e Sociedade*.
10. TETRI, Pekka; VUORINEN, Jukka (2013). Dissecting social engineering.

Behaviour & Information Technology.

TRABALHO DE CONCLUSÃO DE CURSO - TCC (1 DOCUMENTO):

1. PICCIN, Luiz Eduardo. Métodos de detecção de fraude em cartões de crédito: um estudo comparativo. 2022. Trabalho de Conclusão de Curso (Graduação em Estatística) – Universidade Federal de São Carlos (UFSCar), São Carlos, 2022.

DOCUMENTOS INSTITUCIONAIS, RELATÓRIOS E NORMATIVOS (3 DOCUMENTOS PRINCIPAIS):

1. BANCO CENTRAL DO BRASIL. Relatório de Economia Bancária (2022) e Resoluções correlatas.
2. FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). Relatórios de Tecnologia Bancária (2024).
3. SERASA EXPERIAN. Relatórios estatísticos de tentativas de fraudes bancárias no Brasil (2025).

Os dados foram submetidos à análise qualitativa de conteúdo, realizada mediante a leitura parcial e orientada dos documentos selecionados. Essa abordagem pautou-se na exploração de seções estratégicas de cada obra — priorizando o exame de resumos, introduções, seções metodológicas, resultados e considerações finais — a fim de extrair de forma objetiva as evidências pertinentes ao problema de pesquisa. A partir dessa triagem analítica, os achados foram categorizados e sintetizados em cinco eixos temáticos centrais: expansão digital, conceito ampliado de clonagem, tipologias de fraude, impactos sistêmicos e estratégias de contenção tecnológica.

4. APRESENTAÇÃO DE RESULTADOS

A análise integrada dos documentos permitiu sistematizar os resultados em cinco categorias temáticas fundamentais:

1. **Expansão das transações online:** Identificou-se um crescimento exponencial do comércio eletrônico e a universalização da conectividade domiciliar, acompanhados pela migração predominante das operações cotidianas para canais móveis de pagamento (*smartphones*).
2. **Conceito ampliado de clonagem:** Observou-se o deslocamento estrutural da duplicação física de cartões para a apropriação remota de credenciais e dados

em transações sem presença física (*Card-Not-Present*).

- 3. **Técnicas de fraude:** Constatou-se a preponderância de vetores baseados em engenharia social, destacando-se o *phishing*, as falsas centrais de atendimento, os golpes de acesso remoto ("mão fantasma") e as fraudes híbridas.
- 4. **Riscos associados:** Apontou-se a ocorrência de perdas financeiras expressivas para os correntistas, a erosão da privacidade do consumidor, o aumento de custos operacionais e de *chargebacks* nas empresas, e a forte pressão regulatória e sistêmica sobre as instituições financeiras.
- 5. **Prevenção e detecção:** Destacou-se a indispensabilidade de adotar conjugadamente a autenticação forte, a tokenização, a criptografia e modelos analíticos adaptativos baseados em aprendizado de máquina (*machine learning*).

A análise integrada do acervo da pesquisa permitiu sintetizar os achados da pesquisa em cinco categorias fundamentais. A relação entre os eixos temáticos, os principais autores e as abordagens tecnológicas identificadas estão consolidados no Quadro 1.

Quadro 1 – Síntese dos eixos temáticos, referências e tecnologias mapeadas nos documentos

Eixo Temático	Principais Autores / Fontes	Abordagem / Tecnologias Envolvidas
Contexto Econômico	Banco Central (2022); IBGE (2024); MDIC (2024)	Crescimento do e-commerce, expansão da banda larga móvel e Pix.
Engenharia Social	Fornasier et al. (2020); Tetri & Vuorinen (2013)	<i>Phishing</i> , manipulação de vieses cognitivos, <i>spoofing</i> e engenharia humana.
Tipologias de Fraude	FEBRABAN (2024); ABECS (2024); MP-MT ([s.d.])	Transações <i>Card-Not-Present</i> (CNP), falsa central e golpe da mão fantasma.
Modelos de Detecção	Da Pozzolo et al. (2018); Souza & Bordin Jr. (2023)	Algoritmos de <i>Ensemble Learning</i> e combate ao desvio de conceito (<i>concept drift</i>).

Fonte: Elaborado pela autora (2026).

Os achados demonstram que a fraude com cartões no Brasil consolidou-se

como um problema multifatorial. A transição do ambiente físico para o digital alterou o eixo do risco: o perigo deixou de residir primariamente na segurança das tarjas magnéticas e passou a concentrar-se na vulnerabilidade da interface humana e na circulação desprotegida de dados transacionais.

5. DISCUSSÃO

Os resultados evidenciam que o agravamento das fraudes por clonagem de cartões entre 2019 e 2024 decorre de uma mutação qualitativa do sistema financeiro. A conveniência das transações digitais reduziu a fricção operacional, criando um cenário em que a agilidade e a facilidade de uso convivem com a ampliação da superfície de ataque.

Verifica-se uma nítida assimetria estrutural entre defesa e ataque. Enquanto as instituições e empresas operam sob rigorosas amarras regulatórias e padrões técnicos de conformidade, os agentes criminosos demonstram alta flexibilidade tática, pivotando rapidamente de falhas sistêmicas para a exploração de vieses comportamentais por meio da engenharia social. A eficácia desses golpes apoia-se na criação artificial de urgência e na simulação de autoridades legítimas, convertendo o usuário no elo mais vulnerável da cadeia de segurança (Fornasier; Knebel; Silva, 2020; Tetri; Vuorinen, 2013).

Essa dinâmica explica por que os prejuízos extrapolam a dimensão financeira individual. Quando mais de metade da população relata episódios de fraudes ou tentativas (Serasa Experian, 2025), a segurança deixa de ser um atributo técnico marginal e passa a condicionar a própria confiança social nos meios eletrônicos de pagamento.

No plano macroeconômico, a necessidade de investimentos contínuos em barreiras adaptativas, autenticação multifatorial e suporte a contestações gera um encarecimento sistêmico dos serviços financeiros. Diante disso, constata-se que o enfrentamento dessas ameaças não se restringe à implementação de barreiras técnicas isoladas. Torna-se imprescindível a construção de uma arquitetura de segurança integrada, que alie modelos de aprendizado de máquina adaptativos à governança regulatória e à conscientização digital contínua.

6. CONSIDERAÇÕES FINAIS

A presente pesquisa investigou a evolução das fraudes por clonagem de cartões em transações online no Brasil entre 2019 e 2024, analisando seus riscos e as principais estratégias de prevenção e detecção mapeadas na literatura e em documentos institucionais.

O estudo demonstrou que o fenômeno sofreu uma reconfiguração profunda: a clonagem tradicional, vinculada à duplicação física de cartões, deu lugar a ataques remotos baseados no roubo de credenciais e na exploração do fator humano por meio de engenharia social. Constatou-se que os impactos reverberaram de forma ampla sobre consumidores, empresas e instituições financeiras, ameaçando a estabilidade e a confiança no ecossistema digital de pagamentos.

A hipótese inicial foi integralmente confirmada, visto que o crescimento vertiginoso das transações online no período ampliou a exposição a fraudes por uso indevido de dados, tornando ineficientes as abordagens de segurança estáticas e isoladas. Evidenciou-se que a proteção eficaz do ambiente digital demanda uma estratégia integrada, combinando barreiras tecnológicas avançadas (como *machine learning* adaptativo e tokenização) com governança institucional e conscientização dos usuários.

Como limitação do estudo, aponta-se o recorte focado preponderantemente na literatura documental e acadêmica nacional, sugerindo-se para trabalhos futuros a análise empírica de bases de dados transacionais reais para investigar a efetividade técnica dos protocolos de autenticação multifatorial contra ataques baseados em engenharia social.

REFERÊNCIAS

ABECS. **Normativo n. 31**: dispõe sobre a disponibilização de documento técnico de padronização para a aplicação de autenticações via versão 2.0 ou superior do protocolo global EMV 3DS. São Paulo: ABECS, 2024. Disponível em: <https://www.abecs.org.br>. Acesso em: 20 jul. 2026.

BANCO CENTRAL DO BRASIL. **Relatório de Economia Bancária 2022**. Brasília: BCB, 2022.

BANCO CENTRAL DO BRASIL. **Resolução BCB n. 85, de 8 de abril de 2021**. Dispõe sobre a política de segurança cibernética. Brasília: BCB, 2021.

BANCO CENTRAL DO BRASIL. **Vítima caiu no golpe do falso entregador/motoboy**. *Meu BC*, Brasília, DF, 28 mar. 2024. Disponível em: <https://www.bcb.gov.br/meubc/faqs/p/vitima-caiu-no-golpe-do-falso-entregador-motoboy>. Acesso em: 20 jul. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 jul. 2026.

BRASIL. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. **E-commerce no Brasil cresce 4% e alcança R\$ 196 bi em 2023.** Brasília: MDIC, 2024. Disponível em: <https://www.gov.br/mdic>. Acesso em: 20 jul. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. **Diário Oficial da União**, Brasília, DF, 28 maio 2021.

BACELLAR, Leandro Wünsche; TOPOROSKI, Elizeu Luiz. Clonagem de cartão de crédito sob a perspectiva da Lei Geral de Proteção de Dados. **Academia de Direito**, Mafra, v. 6, p. 4374-4388, 2024. Disponível em: <https://doi.org/10.24302/acaddir.v6.5673>. Acesso em: 31 ago. 2026.

CAMPÊLO, Maria Adriana. **Engenharia social:** como aspectos psicológicos podem se relacionar com golpes e fraudes. Brasília: Portal do Investidor, 2024. Disponível em: <https://www.gov.br/investidor>. Acesso em: 20 jul. 2026.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Phishing e outros golpes.** São Paulo: CERT.br, [s.d.]. Disponível em: <https://www.cert.br>. Acesso em: 23 jul. 2026.

CHERIF, Asma et al. Credit card fraud detection in the era of disruptive technologies: a systematic review. **Journal of King Saud University Computer and Information Sciences**, v. 35, n. 1, p. 145-174, 2023.

COELHO, Leandro dos Santos et al. FControl: sistema inteligente inovador para detecção de fraudes em operações de comércio eletrônico. **Gestão & Produção**, v. 13, n. 1, p. 129-139, 2006.

DAL POZZOLO, Andrea et al. Credit card fraud detection: a realistic modeling and a novel learning strategy. **IEEE Transactions on Neural Networks and Learning Systems**, v. 29, n. 8, p. 3784-3797, 2018.

EMVCO. **EMV 3-D Secure:** protocol specifications and remote payment security. Wilmington: EMVCo, 2022. Disponível em: <https://www.emvco.com>. Acesso em: 20 jul. 2026.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Transações bancárias pelo celular crescem 251% em cinco anos.** São Paulo: Febraban, 2024. Disponível em: <https://portal.febraban.org.br>. Acesso em: 20 jul. 2026.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Segurança em canais digitais e o golpe do acesso remoto.** São Paulo: Febraban, [s.d.]. Disponível em: <https://portal.febraban.org.br>. Acesso em: 23 jul. 2026.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva; SILVA, Daniel Adamy da. Phishing e engenharia social: entre a criminalização e a utilização de meios sociais de proteção. **Meritum: Revista de Direito da Universidade FUMEC**,

v. 15, n. 4, p. 239-262, 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Internet foi acessada em 72,5 milhões de domicílios do país em 2023**. Rio de Janeiro: IBGE, 2024. Disponível em: <https://www.ibge.gov.br>. Acesso em: 22 jul. 2026.

KOVACS, Michelle Helena; FARIAS, Salomão Alencar de. Dimensões de riscos percebidos nas compras pela internet. **RAE-eletrônica**, v. 3, n. 2, 2004.

MARAGNO, Ryan; YAMAZATO, Fauzi Anderson. O estado da fraude e do estelionato digital no Brasil: evolução sistêmica, tipologias emergentes e a nova arquitetura de segurança (2020-2025). **Revista do Ministério Público Militar**, ano 53, n. 50, p. 13-42, 2026.

MATO GROSSO. Ministério Público do Estado de Mato Grosso. **Anatomia da fraude digital no Brasil: um guia abrangente de proteção**. Cuiabá: MPMT, 2025. Disponível em: <https://www.mpmt.mp.br>. Acesso em: 22 jul. 2026.

PALDINO, Gian Marco et al. The role of diversity and ensemble learning in credit card fraud detection. **Advances in Data Analysis and Classification**, v. 18, n. 1, p. 193-217, 2024.

PCI SECURITY STANDARDS COUNCIL (PCI SSC). **Card-Not-Present security guidelines**. Wakefield: PCI SSC, 2023. Disponível em: <https://www.pcisecuritystandards.org>. Acesso em: 22 jul. 2026.

PICCIN, Luiz Eduardo. **Métodos de detecção de fraude em cartões de crédito: um estudo comparativo**. 2022. Trabalho de Conclusão de Curso (Graduação em Estatística) — Universidade Federal de São Carlos, São Carlos, 2022.

RESOLUÇÃO CMN Nº 4.935, de 29 de julho de 2021. Dispõe sobre a política de contratação de correspondentes no País e dá outras providências. **Banco Central do Brasil**, Brasília, 2021. Disponível em: <https://www.bcb.gov.br>. Acesso em: 22 jul. 2026.

SERASA EXPERIAN. **Tentativas de fraudes bancárias cresceram 10,4% em 2024 e poderiam gerar prejuízo de até R\$ 51,6 bilhões**. São Paulo: Serasa Experian, 2025. Disponível em: <https://www.serasaexperian.com.br>. Acesso em: 20 jul. 2026.

SOUZA, Daniel Henrique Miguel de; BORDIN JÚNIOR, Claudio José. Novo algoritmo ensemble para detecção de fraude em transações de cartão de crédito. **Revista Tecnologia e Sociedade**, v. 19, n. 56, p. 129-146, 2023.

TETRI, Pekka; VUORINEN, Jukka. Dissecting social engineering. **Behaviour & Information Technology**, v. 32, n. 10, p. 1014-1023, 2013.