UNIVERSIDADE FEDERAL DO PAMPA

Glener Lanes Pizzolato

Taxonomia de Ataques ao Pix e Desenvolvimento de Dataset de Comprovantes de Pagamento Reais

Alegrete
2026

Glener Lanes Pizzolato

Taxonomia de Ataques ao Pix e Desenvolvimento de Dataset de Comprovantes de Pagamento Reais

Dissertação apresentada ao Programa de Pós-graduação Stricto Sensu em Engenharia de Software da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Mestre em Engenharia de Software.

Orientador: Prof. Dr. Claudio Schepke

Coorientador: Prof. Dr. Diego Luis Kreutz

Alegrete
2026

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

P695t Pizzolato, Glener Lanes
Taxonomia de Ataques ao Pix e Desenvolvimento de Dataset de Comprovantes de Pagamento Reais / Glener Lanes Pizzolato.
87 p.

Dissertação(Mestrado)-- Universidade Federal do Pampa, MESTRADO EM ENGENHARIA DE SOFTWARE, 2026.
"Orientação: Claudio Schepke".

1. Pix. 2. Segurança. 3. Fraudes. 4. Inteligência Artificial. 5. Taxonomia. I. Título.

GLENER LANES PIZZOLATO

TAXONOMIA DE ATAQUES AO PIX E DESENVOLVIMENTO DE DATASET DE COMPROVANTES DE PAGAMENTO REAIS

Dissertação apresentada ao Programa de Engenharia de Software da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Mestre Engenharia de Software.

Dissertação defendida e aprovada em: 23/04/2026

Banca examinadora:

_____

Prof. Dr. Claudio Schepke

Orientador

(Unipampa)

_____

Profª. Drª. Isadora Garcia Ferrão

(Université de Bretagne Occidentale)

_____

Dr. João Otávio Massari Chervinski

(University of Sydney)

Prof. Dr. Silvio Ereno Quincozes

(Unipampa)

Assinado eletronicamente por **CLAUDIO SCHEPKE**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 23/04/2026, às 10:24, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **João Otávio Massari Chervinski**, **Usuário Externo**, em 23/04/2026, às 11:13, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **Isadora Garcia Ferrão**, **Usuário Externo**, em 23/04/2026, às 11:22, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **DIEGO LUIS KREUTZ**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 23/04/2026, às 11:30, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

Assinado eletronicamente por **SILVIO ERENO QUINCOZES**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 23/04/2026, às 15:40, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.

A autenticidade deste documento pode ser conferida no site https://sei.unipampa.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2015136** e o código CRC **FF58B546**.

Este trabalho é dedicado a todos que
fizeram parte da minha trajetória até aqui.
E a você, pelo tempo dedicado a essa leitura.

AGRADECIMENTOS

Este trabalho representa o encerramento de mais uma etapa desafiadora e significativa da minha trajetória acadêmica e profissional, pela qual devo expressar minha profunda gratidão a pessoas que me ajudaram a conquistá-la e facilitaram a trajetória.

Agradeço, primeiramente, à minha família, em especial ao meu pai e à minha mãe, pelo apoio incondicional e pelo incentivo constante aos estudos. A confiança de vocês foi essencial para que eu pudesse chegar até aqui.

À minha namorada, expresso minha profunda gratidão pelo apoio ao longo de todo o mestrado. Sua presença constante deixou o processo mais leve e foi determinante para a conclusão deste trabalho.

A todos os meus amigos, que, mesmo indiretamente, estiveram presentes ao longo deste percurso, proporcionando momentos de descontração que foram essenciais para aliviar a pressão e renovar as energias durante o desenvolvimento deste trabalho.

Agradeço ao meu orientador Claudio Schepke pela orientação técnica, pela disponibilidade, pelos ensinamentos e pelas valiosas contribuições que enriqueceram este trabalho e contribuíram de forma decisiva para o meu desenvolvimento acadêmico e profissional.

Estendo meus agradecimentos ao co-orientador Diego Kreutz, pelas sugestões e apoio ao longo do desenvolvimento da pesquisa, que foram fundamentais para o aprimoramento do trabalho.

"Vencerá aquele que souber quando lutar e quando evitar a luta"
- Sun Tzu

RESUMO

A consolidação do Pix como um dos principais meios de pagamento no Brasil trouxe, como efeito colateral, uma diversificação significativa de fraudes e estratégias criminosas, tornando a segurança do ecossistema um desafio crítico para instituições e usuários. Este trabalho apresenta uma investigação abrangente sobre o estado da segurança no Pix, com o objetivo de mapear metodologias de ataque e disponibilizar recursos inéditos para a comunidade científica. A metodologia adotada incluiu uma revisão sistemática da literatura, entrevistas exploratórias com especialistas de instituições bancárias e a coleta de dados reais para o desenvolvimento de um conjunto de dados. Como principais contribuições, o estudo propõe uma taxonomia de 15 fraudes distintas estruturada nos pilares de motivação, meio e execução, identificando quinze tipologias distintas de golpes. Além disso, foi desenvolvido um *dataset* contendo 142 comprovantes de pagamento reais de 13 instituições financeiras, submetidos a uma pipeline automatizada de anonimização de dados sensíveis utilizando LLMs. A análise destaca a dualidade da IA, que atua simultaneamente na escala de ataques, como em *deepfakes*, e no fortalecimento de mecanismos de defesa e detecção de anomalias. Conclui-se que a mitigação de fraudes exige uma evolução contínua que transcenda a conscientização do usuário, focando em tecnologias robustas para proteger o ecossistema do Pix.

Palavras-chave: Pix. Segurança. Fraudes. Inteligência artificial. Taxonomia. Anonimização de dados sensíveis.

ABSTRACT

The consolidation of Pix as one of the main means of payment in Brazil has brought, as a side effect, a significant diversification of fraud and criminal strategies, making the security of the ecosystem a critical challenge for institutions and users. This work presents a comprehensive investigation into the state of security in Pix, with the aim of mapping attack methodologies and providing unprecedented resources for the scientific community. The methodology adopted included a systematic literature review, exploratory interviews with experts from banking institutions, and the collection of real data for the development of a dataset. As main contributions, the study proposes a taxonomy of fraud structured on the pillars of motivation, means, and execution, identifying fifteen distinct types of scams. In addition, a dataset containing 142 real payment receipts from 13 financial institutions was developed, subjected to an automated pipeline for anonymizing sensitive data using LLMs. The analysis highlights the duality of AI, which acts simultaneously on the scale of attacks, such as deepfakes, and in strengthening defense mechanisms and anomaly detection. It concludes that mitigating fraud requires continuous evolution that transcends user awareness, focusing on robust technologies to protect the Pix ecosystem.

Key-words: Pix. Security. Fraud. Artificial intelligence. Taxonomy. Anonymization of sensitive data.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O Pix é um meio de pagamento coordenado pelo Banco Central do Brasil (BCB). A operação pode ser realizada a partir de uma conta corrente, conta poupança ou conta de pagamento pré-paga (Banco Central do Brasil, 2026e). Os recursos financeiros são transferidos entre contas em poucos segundos, podendo ser qualquer valor sem limite, a qualquer dia ou hora. Entretanto, as instituições financeiras que oferecem o Pix podem estabelecer limites máximos de valores com base em critérios de mitigação de riscos de fraude e em critérios de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

O Pix foi idealizado em 2018 e lançado em 16 de novembro de 2020. No primeiro mês de funcionamento, o Pix ultrapassou em quantidade as transações com Documento de Crédito (DOC). No começo do ano seguinte, em 2021, O Pix superou as transações com Transferência Eletrônica Disponível (TED). Já em março do mesmo ano, o Pix ultrapassou os boletos. Em maio de 2021, o Pix superou a soma de todas as transações (GOV-BR, 2022). Já em relação às operações com cartões, o Pix superou as transações de débito e crédito em janeiro e fevereiro de 2022, respectivamente. Desde então, o Pix tornou-se o meio de pagamento mais utilizado no Brasil (GOV-BR, 2022), onde 80% da população brasileira já realizou pelo menos um Pix durante a vida.

O crescimento do Pix por ano é surpreendente, tanto em quantidade quanto em valor. Conforme pode ser visto na Tabela 1, o número total de transações e o valor total em transações dobraram após o primeiro ano de lançamento. Segundo a lista de participantes ativos do Pix (instituições financeiras com a operação Pix disponível para seus usuários) de fevereiro de 2026 (Banco Central do Brasil, 2026b), existem 919 instituições financeiras que já aderiram a essa tecnologia, e outras 25 estão em processo de adesão.

1.1 Justificativa

Como qualquer transação financeira, é necessário tratar os aspectos de segurança ligados às operações. Os próprios benefícios do Pix para os usuários tornam-se motivações para os atacantes, conforme a Figura 1. Embora o BCB tenha implementado aspectos

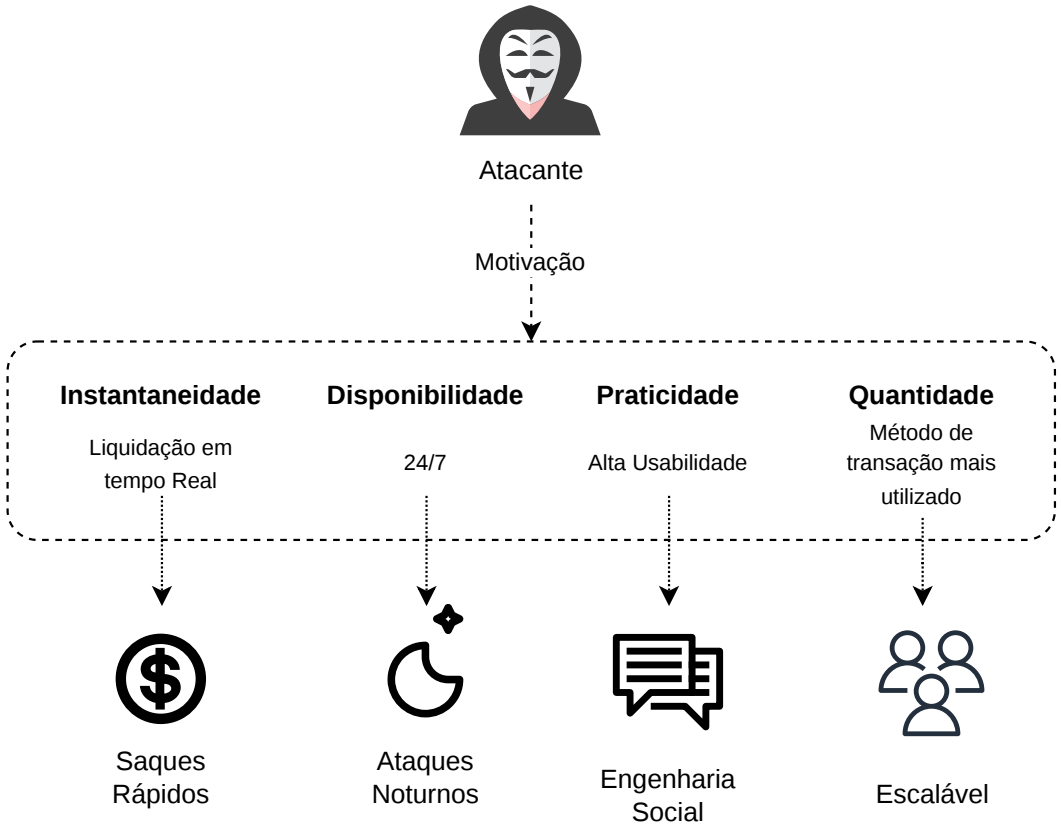
Tabela 1 – Número e valor total de transações Pix por ano desde a sua implantação (Banco Central do Brasil, 2026c)

Ano	**Número total de transações Pix (em bilhões)**	**Movimentações de recursos pelo Pix (em trilhões R$)**
2021	10,89	5,21
2022	24,10	10,89
2023	41,90	17,18
2024	63,51	26,46
2025	79,78	35,32

Fonte: Elaboração própria, baseado em (Banco Central do Brasil, 2026c)

de segurança para garantir a integridade das ações financeiras, ele próprio relata o vazamento de dados cadastrais (Banco Central do Brasil, 2026d) e publica campanhas de conscientização sobre a segurança.

Figura 1 – Motivação dos atacantes



Fonte: Elaboração própria

Uma consequência do sucesso do Pix é a queda da circulação de dinheiro vivo/-moeda. Segundo (GLOBO, 2024), o Pix é considerado a principal forma de pagamento do Brasil desde 2021. Nos anos subsequentes a sua implantação, ocorreu um recuo na utilização de dinheiro vivo no país. (PERNAMBUCO, 2024) afirma que foi registrada uma queda significativa nos saques realizados no Brasil nos últimos anos. Segundo (PRIDEMORE; ROCHE; ROGERS, 2018), a substituição do dinheiro físico por meios de pagamento tecnológicos pode alterar a forma como a criminalidade atua, pois, conforme a circulação de dinheiro em espécie diminui, dando espaço para os cartões e meios de pagamento digitais, as pessoas nas ruas tornam-se menos atraentes para os criminosos. Essa informação foi validada por um estudo realizado em 67 países; as nações com maior quantidade de pagamentos sem dinheiro apresentavam menores taxas de criminalidade

patrimonial.

Outro aspecto relacionado à segurança é o aumento de ataques por engenharia social. Em 2020, foi registrado um aumento de 200% de ataques que usam engenharia social (TECH, 2021). O Brasil foi o segundo país da América Latina com maior incidência desse tipo de estratégia fraudulenta. Coincidentemente, esse aumento foi registrado no mesmo ano em que o Pix foi lançado. A notícia não tem ligação direta com o Pix, mas é claro que o Pix trouxe facilidades para realizar transferências monetárias e, consequentemente, facilitou a execução de golpes. Além dos ataques de engenharia social, logo após o lançamento do Pix, em 2021, ocorreu um aumento significativo de 40% em extorsões por sequestros-relâmpago (CBN, 2021).

Dois grandes incidentes com o Pix ocorreram recentemente. Uma invasão ocorreu no dia 29 de agosto de 2025 na empresa *Sinqia*, uma companhia que conecta bancos ao Pix. O ataque foi realizado por meio da exploração de credenciais de fornecedores legítimos (G1, 2025). Já no maior roubo da história do Brasil, ocorrido em julho de 2025, estima-se que o prejuízo tenha sido de R$ 1 bilhão. O ataque ocorreu através da empresa C&M Software e utilizou um funcionário interno e suas credenciais (EXAME, 2025).

Dado o aumento de fraudes e a carência de estudos técnicos aprofundados sobre tais métodos, conforme evidenciado pela revisão da literatura no Capítulo 3, a disponibilidade de dados categorizados torna-se um gargalo para o avanço da área. O mapeamento e a categorização das metodologias de golpes desenvolvidos neste trabalho contribuem diretamente para a redução dessa lacuna, ao fornecer uma base estruturada e sistematizada que permite não apenas a compreensão dos padrões de ataque, mas também sua utilização em análises comparativas, treinamento de modelos e desenvolvimento de mecanismos de detecção mais eficazes.

Por outro lado, a escassez de conjuntos de dados limita o treinamento de modelos de linguagem de grande escala (*Large Language Models* - LLMs) e outras arquiteturas de IA voltadas à segurança. Conjuntos de dados diversificados em termos de volume, tipologia e formato são imperativos para o desenvolvimento de mecanismos resilientes contra incidentes. Além de servirem como base para testar, comparar e aprimorar a eficácia de algoritmos de detecção de fraude e processamento de imagens, esses *datasets* permitem que pesquisadores decomponham táticas e padrões de ataque, antecipando-se a novas ameaças. Adicionalmente, tais dados viabilizam estudos sobre a percepção humana e detecção de detalhes em evidências digitais, como o reconhecimento de adulterações em documentos, vídeos e comprovantes sintéticos.

Nesse contexto, o *dataset* de comprovantes de pagamento Pix proposto neste trabalho destaca-se por sua natureza realista e representativa, sendo construído a partir de amostras reais de diferentes instituições financeiras e refletindo a heterogeneidade presente no ecossistema. Diferentemente de bases sintéticas ou excessivamente padronizadas, o conjunto preserva variações de layout, estrutura e conteúdo, aspectos essenciais para o

desenvolvimento de modelos capazes de generalizar para cenários do mundo real. Essa característica é particularmente relevante em aplicações de segurança, nas quais pequenas diferenças visuais ou textuais podem ser determinantes para a identificação de fraudes.

Adicionalmente, o processo de anonimização desenvolvido permite conciliar a utilidade analítica dos dados com a preservação da privacidade, viabilizando o compartilhamento seguro do *dataset* com a comunidade científica. Ao disponibilizar um recurso que equilibra realismo e conformidade com requisitos de proteção de dados, este trabalho não apenas reduz a dependência de dados proprietários, como também fomenta a reprodutibilidade e a comparabilidade de estudos na área. Dessa forma, o *dataset* proposto estabelece uma base concreta para experimentação, desenvolvimento e validação de soluções voltadas à detecção e mitigação de fraudes no contexto de pagamentos digitais.

1.2 Objetivos

Diante do cenário exposto, o objetivo principal deste trabalho é a disponibilização de dois conjuntos de dados inéditos para a comunidade científica: um voltado à estruturação e análise de ameaças e, primordialmente, um *dataset* de comprovantes de pagamento Pix anonimizados. Para viabilizar tais recursos, o estudo propõe-se a identificar e detalhar as principais modalidades de ataques no ecossistema Pix, estabelecendo uma taxonomia que organiza essas ameaças por meio da atribuição de múltiplos rótulos distribuídos em três pilares analíticos.

Além disso, busca-se promover discussões sobre a maturidade do mercado e as vulnerabilidades percebidas pelas instituições parceiras, mapeando as técnicas de mitigação vigentes e analisando o papel dual da inteligência artificial, tanto como vetor de ataque quanto como ferramenta de defesa.

O presente trabalho oferece as seguintes contribuições:

(a) **Repositório público da taxonomia de ataques**: Um repositório estruturado que categoriza as metodologias de fraude mapeadas, fundamentado em três pilares estratégicos sob a ótica do atacante: motivação, meio e execução;

(b) ***Dataset* de comprovantes Pix**: Um conjunto de dados inédito contendo comprovantes de pagamento reais, coletados de diversas instituições financeiras e submetidos a uma *pipeline* customizada de anonimização para a proteção de dados sensíveis em formatos de imagem e PDF.

1.3 Organização do trabalho

Todo trabalho está organizado focado nas 2 contribuições citadas, a respectiva ordem é mantida na medida do possível em todos capítulos, trazendo de forma paralela

no Capítulo 3 e Capítulo 7 discussões sobre as contramedidas adotadas pelas instituições financeiras e pelo Banco Central para evitar os ataques.

O restante do documento está estruturado da seguinte forma. O Capítulo 2 discute conceitos abordados em todo trabalho. O Capítulo 3 traz a revisão da literatura aplicada, discussão dos trabalhos selecionados e a preocupação das instituições parceiras com os incidentes de segurança, o Capítulo 4 apresenta uma visão geral da metodologia aplicada nas duas trilhas da pesquisa.

Na sequência, o Capítulo 5 lista as metodologias mapeadas e define a taxonomia proposta. O Capítulo 6 traz detalhes das amostras coletadas para o *dataset*.Por fim, a conclusão e as perspectivas futuras são apresentadas no Capítulo 7.

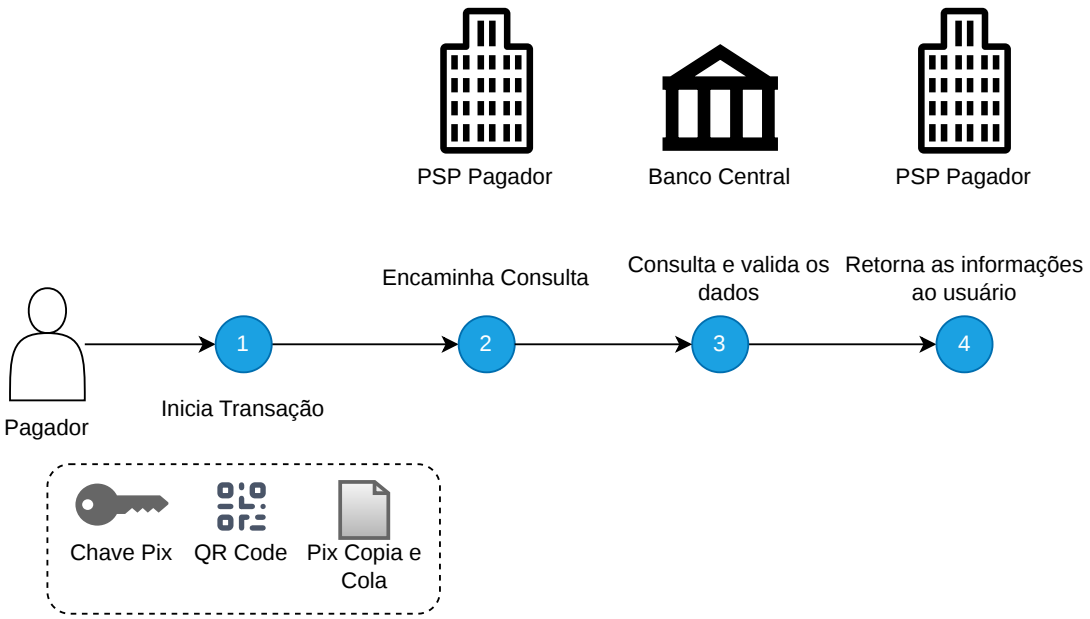
2 ASPECTOS CONCEITUAIS

2.1 Como funciona o Pix

O método de pagamento instantâneo brasileiro Pix possui 2 etapas no fluxo da transação. O primeiro é a busca dos dados do destinatário e a segunda é a efetuação do pagamento.

Uma grande vantagem do Pix é não diferenciar transferências entre contas da mesma instituição (transferência simples) ou entre contas de instituições diferentes (anteriormente conhecidas como TED e DOC). Com o Pix, não é mais necessário saber a conta bancária do destinatário. Ou seja, ao invés de pedir a agência, a conta e os dados pessoais do recebedor, basta informar a chave Pix, que é a identificação preferencial. Essa chave pode ser CPF, CNPJ, e-mail, número de celular ou chave aleatória (uma sequência alfanumérica gerada aleatoriamente que poderá ser utilizada por usuários que não queiram vincular seus dados pessoais às informações de sua conta transacional) (Banco Central do Brasil, 2026e). Ao fazer um Pix, o sistema identifica as informações da conta do credor a partir dessa chave (Banco Central do Brasil, 2026e), fluxo da identificação do destinatário ilustrado na Figura 2.

Figura 2 – Busca dos dados do destinatário



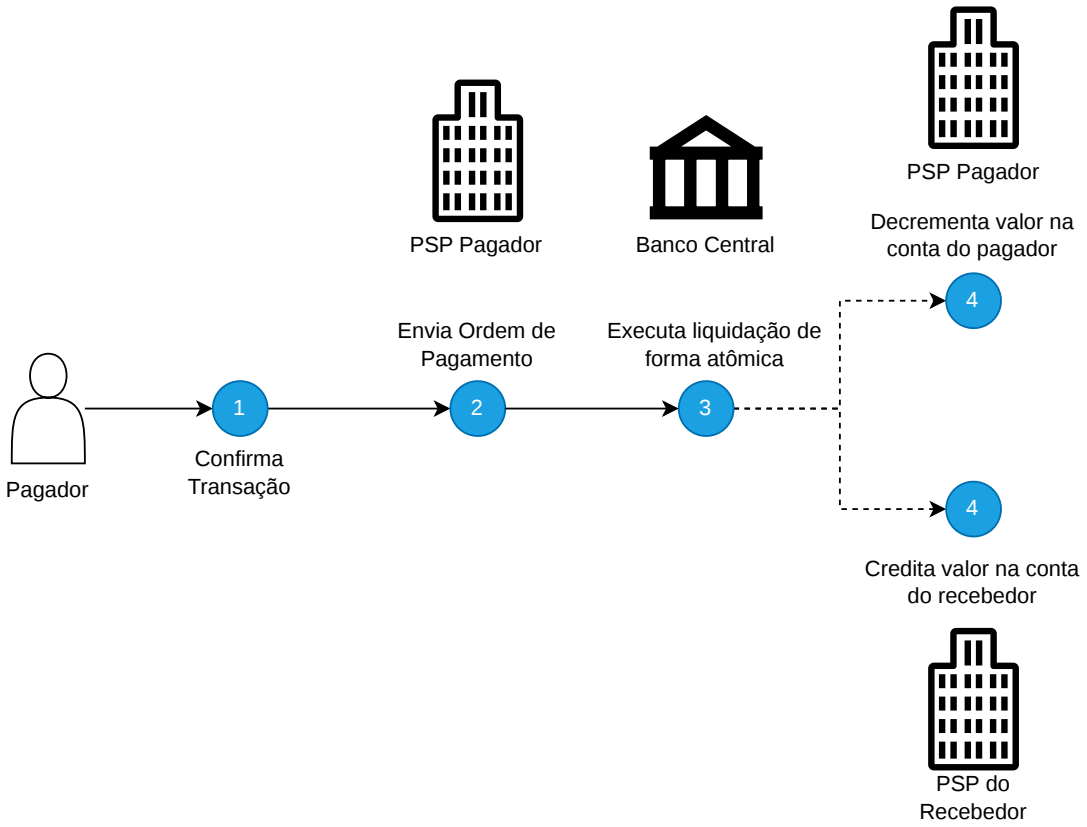
Fonte: Elaboração própria

Durante a busca dos dados, é consultado o DICT (Diretório de Identificadores de Contas Transacionais), o DICT é o "coração"operacional das chaves Pix.

A etapa da confirmação e liquidação dos valores é representada na Figura 3. Onde através de uma operação atômica o Banco Central transfere o valor da transação do PSP

do pagador para o PSP do destinatário.

Figura 3 – Fluxo de pagamento após confirmação



Fonte: Elaboração própria

Quando falarmos de PSP, estamos nos referindo a *payment service provider*, ou seja, provedor de serviços de pagamento. Se refere a toda instituição que intermedeia pagamentos entre usuários e o Banco Central.

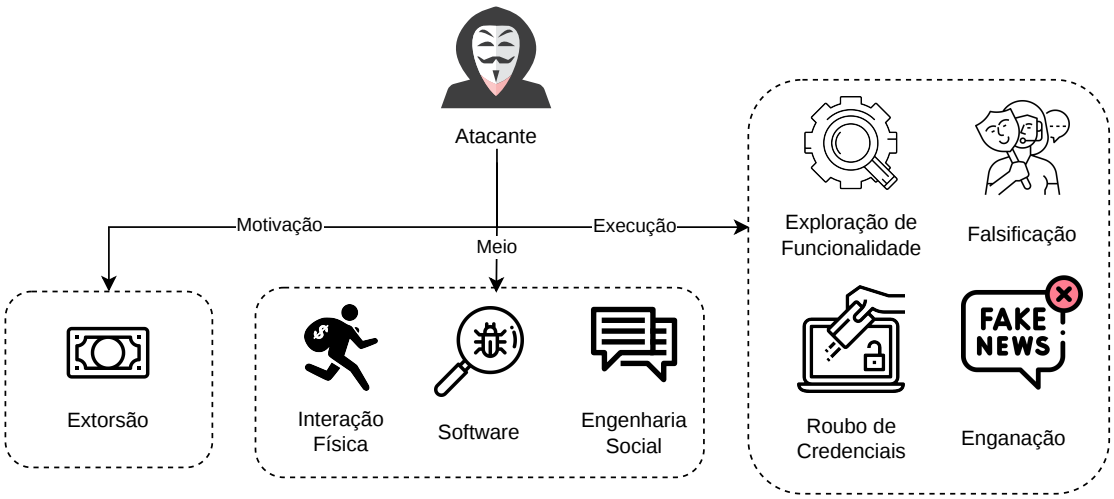
2.2 Tipos de fraudes no Pix

Golpes, fraudes e ataques são todos sinônimos que se referem a uma ação exercida por um atacante para extorquir, manipular, persuadir ou roubar credenciais de usuários e/ou roubar ou invadir sistemas.

O atacante é um indivíduo que age de má fé para aplicar golpes, utilizando um ou mais meios para estabelecer contato e efetuar uma ou várias "metodologias de execução", a fim de extorquir monetariamente usando a tecnologia Pix, conforme a Figura 4.

Dentro dos golpes mapeados temos vários tipos e formas de ataques que precisam ser conceituados. Um deles é a Engenharia social, no contexto da segurança, refere-se a técnicas que os atacantes utilizam visando manipular psicologicamente a vítima, com o

Figura 4 – Definindo atacante



Fonte: Elaboração própria

intuito de obter acesso a informações privadas ou de fazer com que o indivíduo realize ações com o objetivo de extorquir ou praticar transações monetárias. Há diversos tipos de ataques baseados em engenharia social. Dentre as metodologias mapeadas, pelo menos um ataque de cada item foi identificado, como citado e explicado abaixo:

1. *Phishing*: A tática de engenharia social mais difundida, *phishing*, envolve invasores passando-se por entidades legítimas — como bancos, agências governamentais ou empresas — para enganar os usuários e fazê-los compartilhar informações confidenciais. Os invasores enviam e-mails ou mensagens que imitam fontes legítimas, solicitando que os usuários cliquem em um link ou baixem um anexo. Isso geralmente leva a um site falso que parece real, onde os usuários inserem suas credenciais ou informações financeiras sem saber.

2. *Baiting*: *Baiting* usa a promessa de algo atraente (como downloads gratuitos, prêmios ou conteúdo exclusivo) para atrair usuários a fornecer informações ou baixar malware. Um invasor pode deixar unidades USB infectadas em locais visíveis (como saguões ou estacionamentos) ou usar anúncios online para promover downloads falsos de software. Quando os usuários se envolvem, eles involuntariamente concedem acesso aos seus sistemas ou expõem informações pessoais.

3. *Pretexting*: Esta técnica envolve criar um cenário falso para ganhar a confiança do alvo e extrair informações. O invasor pode fingir ser uma figura de autoridade, como um funcionário da Receita ou pessoal de suporte de TI, que precisa de informações

confidenciais para resolver um problema. Eles podem pedir credenciais de login sob o pretexto de verificar a identidade ou corrigir problemas técnicos.

4. *Spear Phishing*: É uma forma direcionada de *phishing* na qual os invasores personalizam mensagens para um indivíduo ou organização específica. Os invasores geralmente pesquisam seus alvos para personalizar os e-mails, fazendo com que pareçam mais confiáveis. Por exemplo, eles podem fazer referência a um projeto recente ou enviar mensagens que parecem vir de colegas ou supervisores, aumentando a chance de os usuários divulgarem informações ou autorizarem pagamentos.

5. *Quid Pro Quo*: Em ataques *quid pro quo*, os invasores prometem um benefício em troca de informações ou acesso. Os invasores podem se passar por suporte técnico, oferecendo ajuda gratuita com problemas de TI e pedindo credenciais de login em troca. Outro exemplo é oferecer um prêmio gratuito, mas exigir que os usuários forneçam detalhes pessoais para reivindicá-lo.

6. *Vishing*: *Vishing* usa ligações telefônicas em vez de e-mails para se passar por fontes confiáveis. Os invasores geralmente se passam por representantes de atendimento ao cliente de bancos ou empresas de tecnologia. Eles alegam problemas urgentes na conta ou ameaças à segurança, podendo pressionar os usuários a fornecer detalhes bancários ou acesso à conta, alegando que estão verificando ou protegendo as contas.

Outro tipo de ataque é via software malicioso, ou em outras palavras, *malware*. Refere-se a qualquer programa ou código desenvolvido com o propósito de infiltrar-se, causar danos ou realizar ações não autorizadas em um sistema computacional.

2.3 Mecanismos de segurança

Alguns termos são utilizados para descrever mecanismos de segurança, um deles é o *zero trust* (Confiança Zero), arquitetura de segurança baseado no princípio de que nenhuma entidade, seja ela interna ou externa à rede da organização, deve receber confiança automática. O *zero trust* exige a verificação contínua de cada solicitação de acesso, independentemente da origem.

Também falaremos sobre autenticação de dois fatores (*2FA*), é um mecanismo de segurança que exige que o usuário forneça duas formas diferentes de identificação para acessar uma conta ou autorizar uma transação. Geralmente, combina algo que o usuário sabe (como uma senha) com algo que ele possui (como um código enviado por SMS ou gerado em um aplicativo de token) ou algo que ele é (biometria).

2.4 Inteligência artificial

Large Language Model (LLM), ou na tradução grande modelo de linguagem. É um tipo de inteligência artificial generativa que foi treinada com um grande conjuntos de dados, utilizada para realizar N diversas tarefas.

Os provedores de LLMs como Google disponibilizam via API ("*Application Programming Interface*" ou "Interface de Programação de Aplicações", é uma forma de diferentes aplicações expor seus serviços e se comunicarem) consultas a seus modelos de Inteligência Artificial. Essas consultas tem um custo que depende dos *tokens* (dados enviados na consulta que o modelo utiliza para processar e gerar informação) (entrada/saída) e o modelo utilizado.

Nesse trabalho é utilizado o *Ollama* para rodar modelos de LLM localmente (OLLAMA, 2026).

Prompt é a instrução, comando ou contexto em linguagem natural fornecido para um modelo. Ele atua como o guia que direciona o comportamento do modelo, delimitando o escopo da tarefa, o tom da resposta e as restrições operacionais. A eficácia da saída gerada pela IA está diretamente ligada à clareza e à estruturação do *prompt*.

Dataset é um termo utilizado para conjuntos de dados criados com o objetivo de treinar modelos de inteligência artificial para realizar uma determinada tarefa.

Um *dataset* é formado por N amostras, que são os elementos que formam o *dataset*.

Para a criação do *dataset*, foi utilizado processamento de imagem/pdf em conjunto com modelos de inteligência artificial, utilizando técnicas de sobreposição para adicionar tarjas pretas com o intuito de ocultar dados sensíveis anonimizando as amostras do *dataset*.

Esses processo são executados via *scripts*, que são um conjunto de instruções ou comandos escritos em linguagem natural ou de programação para serem executados por um interpretador, visando automatizar tarefas específicas e repetitivas.

Durante a anonimização é mencionado o termo *Personally Identifiable Information* (PII), se trata de dados sensíveis de identificação.

Para o processo de anonimização foram utilizados *templates*, que basicamente são modelos a se seguir. No nosso caso, *template* é dito com o intuito de representar um conjunto composto por um comprovante de pagamento Pix já anonimizado e um mapa de coordenadas referente as localizações dos dados sensíveis daquele dado comprovante.

Após o processo de ocultação dos dados sensíveis, temos uma etapa denominada *guardrails* utilizada para evitar que nenhum dado sensível seja vazado no dataset, esse é um mecanismo de segurança utilizado (nesse caso) explicitamente para barrar comprovantes de pagamento Pix com dados sensíveis, sendo uma camada de segurança programática essencial aplicada ao processamento de dados.

Um termo amplamente utilizado no presente trabalho é *deepfake*, o termo deriva da junção de *deep learning* (aprendizado profundo) e *fake* (falsidade). Trata-se de uma

tecnologia baseada em modelos generativos de inteligência artificial que permite a criação ou manipulação de conteúdos sintéticos altamente realistas. Pode ser aplicado para gerar conteúdos falsos em imagens, vídeos ou áudios:

- Imagem: Permite a geração de fotos de rostos inexistentes ou a substituição de faces em fotos reais (*face swap*), criando identidades falsas convincentes para perfis em redes sociais.
- Áudio: Utiliza a clonagem de voz para mimetizar o timbre, a entonação e o sotaque de uma pessoa real, sendo comumente aplicado em golpes de *vishing* ou falsas emergências familiares.
- Vídeo: Combina a manipulação visual e sonora para simular pessoas reais dizendo ou fazendo coisas que nunca ocorreram, dificultando a distinção entre conteúdos autênticos e fraudulentos durante interações digitais.

3 REVISÃO DA LITERATURA E DO MERCADO

Neste capítulo, apresenta-se uma revisão sistemática da literatura, uma busca por informações públicas a respeito de mapeamento de metodologias de golpes no Pix, categorização e agrupamento dos mesmos. Mecanismos de segurança aplicados por agências financeiras e a iniciativa de obtenção de respostas restritas de bancos sobre fraudes, prevenção e desafios enfrentados por eles.

3.1 Revisão da literatura

O Protocolo de Mapeamento Sistemático *Systematic Mapping Study* (SMS) foi utilizado para a busca na literatura, a fim de contemplar ataques ao Pix. Após algumas versões e evoluções, foi definida a seguinte string de busca:

("attacks" OR "security incident" OR "information leak" OR "fraud" OR "cybercrime" OR "vulnerability exploitation" OR "cybersecurity") AND ("instant payment" OR "instant payment system" OR "financial system") AND ("Brazil")

A única base de dados utilizada foi o Google Acadêmico. Como o Pix foi lançado em 2020, foi aplicado um filtro para buscar trabalhos a partir desse ano. Um total de 294 artigos foi encontrado. Em seguida, foram desconsiderados trabalhos com os seguintes critérios de exclusão (CEs):

- CE-1 Trabalhos publicados antes de 2020;
- CE-2 Trabalhos com quatro páginas ou menos;
- CE-3 Trabalhos similares (ou seja, com versões diferentes) dos mesmos autores;

Os trabalhos não excluídos foram avaliados de acordo com os critérios de inclusão (CIs):

- CI-1 Apenas trabalhos que abordam ataques, incidentes ou golpes de forma central e relevante;
- CI-2 Apenas trabalhos que tratam do Pix de maneira substancial e detalhada;
- CI-3 A pontuação mínima de qualidade para inclusão é 2,5.

Os trabalhos relacionados encontrados a partir da busca e aplicação dos critérios de inclusão e exclusão estão descritos na Tabela 2. Note que um dos critérios de inclusão é uma avaliação de qualidade mínima. Para chegar a esses números, os trabalhos foram avaliados em 4 questões de qualidade (QQs):

- QQ1 - O artigo é baseado em pesquisa (ou é apenas um relatório de "lições aprendidas" baseado na opinião de especialistas)?

Tabela 2 – Estudos relacionados

Estudo	**Título do Estudo e URL**
01	A responsabilidade civil das instituições bancárias diante do cenário de fraudes digitais envolvendo vítimas idosas por meio do sistema de pagamentos instantâneos (Pix) no Brasil (MENDES, 2023) <https://pantheon.ufrj.br/handle/11422/25307>
02	Post-Quantum Cryptography methods applied to the Brazilian instant payment system (Pix): A feasibility study (NETO, 2022) <https://cryptoid.com.br/wp-content/uploads/2022/04/quantum-cryptography-Pix-en.pdf>
03	A responsabilidade das instituições financeiras nas fraudes em transações via Pix (RIBEIRO, 2023) <https://repositorio.ufu.br/handle/123456789/40959>
04	Tecnologia de pagamento instantâneo: Pix e criminalidade patrimonial: uma análise econométrica (DELLABARBA, 2023) <https://repositorio.unb.br/handle/10482/49899?locale=es>
05	A consumer-centric approach for Inclusion in Digital Public Infrastructures (BELLI et al., 2024) <https://www.global-solutions-initiative.org/wp-content/uploads/2025/03/GS_journal_10_Meira_Draper_Contri_Cruz_Barbosa.pdf>
06	CEMLA's survey on central bank digital currencies in Latin America and the Caribbean (VALLE et al., 2024) <https://www.sciencedirect.com/science/article/pii/S2666143824000176>
07	Central bank digital currencies: a high-level overview (COSTA et al., 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4271644>

Fonte: Elaboração própria

- QQ2 - O estudo apresenta dados empíricos?
- QQ3 - Foram apresentados dados suficientes para apoiar as conclusões?
- QQ4 - As limitações do estudo são discutidas explicitamente?

Cada questão de qualidade tem três notas possíveis: 0 - Não atende; 0,5 - Atende parcialmente; 1 - Atende.

A pontuação máxima para um estudo relacionado nesse caso é 4, quando recebe "Atende" em todas as questões de qualidade. Vale ressaltar que a avaliação foi resultante da média de uma avaliação feita pelo autor e revisada pelos co-autores, além das validações realizadas pelos modelos *GPT-4* (OPENAI, 2026) e *Gemini 2.5 Pro* (GOOGLE, 2026a). A média resultante das avaliações pode ser conferida na Tabela 3.

O critério de inclusão CI-3 define que somente trabalhos com pontuação maior do que 2,5 sejam considerados. Então, os trabalhos que passaram por todos os filtros foram: [01], [02], [04], [06] e [07]. O resumo dos trabalhos selecionados pode ser acompanhado

Tabela 3 – Média avaliações estudos relacionados

Estudo	**Média**
01	3,75
02	4,00
03	0,50
04	3,75
05	1,50
06	3,75
07	3,00

Fonte: Elaboração própria

abaixo. Através desta revisão, buscou-se obter uma visão abrangente sobre o conteúdo da literatura que detalha metodologias de ataques no Pix.

01 **A responsabilidade civil das instituições bancárias diante do cenário de fraudes digitais envolvendo vítimas idosas por meio do sistema de pagamentos instantâneos (Pix) no Brasil**: O foco deste trabalho é especificamente a responsabilidade ética das instituições parceiras do Pix para com as vítimas idosas. São apresentados estudos que comprovam que as pessoas idosas são mais suscetíveis a cair em golpes e que não existem procedimentos jurídicos para beneficiar essas vítimas no Brasil atualmente. O trabalho cita alguns ataques (p. 39), mas apenas para exemplificar certos estudos de caso, retornando ao foco principal do trabalho.

02 ***Post-Quantum Cryptography methods applied to the Brazilian instant payment system (Pix): A feasibility study***: Este trabalho fala sobre algoritmos de Criptografia Pós-Quântica (PQC), que são métodos para evitar ataques feitos por computação quântica. Os autores destacaram, dentre tantos citados, o algoritmo *Picnic*. Foram realizadas simulações de ataques quânticos no Pix usando o algoritmo *Picnic* como proteção. Porém, esse algoritmo não satisfaz as obrigatoriedades do Pix, como o tempo de resposta máximo, pois o processamento é pesado e aumenta o *throughput* de mensagens. O trabalho conclui que os algoritmos PQC existentes atualmente não garantem proteção suficiente contra ataques de computação quântica. Os melhores algoritmos não se adéquam as obrigatoriedades do Pix, pois são pesados e dão vazão a mensagens de 4 a 5 vezes mais do que o permitido. Como alternativa, seria necessário otimizar o algoritmo *Picnic*. O que chama a atenção é a necessidade de realizar os testes em um ambiente real e não em um simulado, como foi feito. Essa limitação é difícil de ser quebrada, pois, para ter acesso a *API* é necessário um longo processo burocrático e complexo junto ao BCB para se tornar uma instituição parceira do Pix.

04 **Tecnologia de pagamento instantâneo: Pix e criminalidade patrimonial: uma análise econométrica**: O trabalho é muito rico em conteúdo e em citações.

O trabalho detalha a metodologia de alguns ataques físicos, como furtos e roubos, mas não trata do sequestro relâmpago. Dentre todos os trabalhos selecionados, foi o que mais se aprofundou em detalhar uma metodologia de golpe.

06 ***CEMLA's survey on central bank digital currencies in Latin America and the Caribbean***: O trabalho cita o Pix como estudo de caso, mas não estabelece a conexão entre o Pix e ataques ou incidentes de segurança. O trabalho, por mais que tenha passado na avaliação com uma nota alta, devido aos tópicos das questões de qualidade serem de contexto geral e não específicos do tema dos ataques, não discute os ataques de forma relevante.

07 ***Central bank digital currencies: a high-level overview***: O texto fala abrangentemente sobre moedas digitais. O Pix é citado apenas como um caso de sucesso. Ataques são citados superficialmente em alguns momentos, mas apenas para o problema que os ataques trazem com o crescimento do Pix. Não existe um detalhamento da metodologia desses ataques.

Com base na revisão sistemática da literatura realizada, nota-se que há uma falta de trabalhos que detalham as metodologias dos ataques no Pix. O trabalho [04], que foi um destaque por conter citações e *insights* valiosos, ainda assim possui limitações. Ele detalha alguns ataques físicos, mas não o sequestro relâmpago, que é um ataque recorrente mencionado. É um trabalho que foca apenas no estado do Rio de Janeiro e é de 2021. Não se têm dados atualizados sobre o cenário atual desses golpes. Dessa forma, fica evidente a falta na literatura em detalhar como os ataques acontecem.

Outro trabalho interessante que foi encontrado durante o desenvolvimento desta pesquisa foi o trabalho de monografia intitulado "Negação plausível em sequestros relâmpagos: implementação do modo pânico em aplicativos bancários" (D'OLIVEIRA; FERNANDES, 2024), que traz uma proposta de mecanismo para mitigar os danos causados por ataques de sequestro relâmpago. O objetivo principal é proteger os usuários contra o acesso indevido a informações financeiras durante situações de emergência. O sistema proposto utiliza senhas alternativas e altera temporariamente os dados financeiros visíveis para mitigar riscos e aumentar a segurança bancária. Mas não há nada confirmado de que as instituições financeiras adotaram ou irão adotar o mesmo, pois existem problemas burocráticos para a adoção, validação, etc.

3.2 Entrevistas com representantes de instituições parceiras do Pix

Essa seção apresenta uma síntese das informações de mercado obtidas por meio de entrevistas com representantes de três instituições bancárias: Banco do Brasil, Sicredi e Banrisul. O objetivo foi identificar os principais tipos de fraudes observadas, os meca-

Tabela 4 – Resumo das entrevistas com as instituições parceiras do Pix

Instituição	**Descrição**
Banco do Brasil	**Perfil:** Gerente da agência. **Principais fraudes:** Engenharia Social; Phishing; Clonagem de WhatsApp. **Grupos afetados:** Todos igualmente vulneráveis. **Desafios:** Contas laranjas e pulverização dos valores. **Medidas preventivas citadas:** Autenticação em duas etapas (2FA).
Sicredi	**Perfil:** Gerente da agência. **Principais fraudes:** Engenharia social. **Grupos afetados:** Todos igualmente vulneráveis. **Desafios:** Dependência da rapidez da vítima; uso de múltiplas contas por criminosos. **Medidas preventivas citadas:** Alertas em redes sociais e mídia; Educação do cliente; Monitoramento de transações; Bloqueio rápido (até 30 min); Alertas internos.
Banrisul	**Perfil:** Gerente Geral. **Principais fraudes:** Engenharia social. **Grupos afetados:** Idosos; baixa familiaridade tecnológica. **Desafios:** Conscientização dos usuários; apoio da mídia e familiares. **Medidas preventivas citadas:** Monitoramento; Bloqueio de contas; Uso de IA; Alertas preventivos; Limites transacionais.

Fonte: Elaboração própria

nismos de prevenção adotados e os desafios enfrentados por cada instituição no combate a golpes relacionados ao sistema Pix.

Foi aplicado o formulário disponível no Apêndice A, o resumo de cada entrevista por representante pode ser conferida na Tabela 4.

As investigações revelaram que os tipos de fraude mais comuns incluem *phishing*, clonagem de aplicativos de mensagens (como o WhatsApp) e o uso de contas de fachada ou "laranjas" para pulverizar os valores subtraídos, dificultando o rastreamento e a recuperação.

No que tange aos mecanismos de prevenção, as instituições adotam uma abordagem multifacetada. O Banco do Brasil aponta o uso da autenticação em duas etapas (2FA) como uma barreira de segurança, embora sua eficácia seja considerada parcial. De forma análoga, Sicredi e Banrisul investem massivamente no monitoramento de transações suspeitas, no bloqueio ágil de contas de destino e no uso de inteligência artificial para analisar padrões de comportamento e identificar atividades fraudulentas.

Um ponto de destaque é a forte ênfase na educação e conscientização dos clientes.

O Sicredi, por exemplo, utiliza campanhas em mídias sociais e locais para alertar a população, tratando a prevenção como uma política central. O Banrisul corrobora essa visão, ressaltando a importância do papel da mídia e do apoio familiar, especialmente para os grupos mais vulneráveis, como idosos e pessoas com baixa familiaridade tecnológica, que são identificados como alvos preferenciais. Em contrapartida, tanto o Banco do Brasil quanto o Sicredi consideram que todos os perfis de clientes estão suscetíveis a golpes, bastando um momento de desatenção.

Entre os maiores desafios identificados está a velocidade das operações fraudulentas. A recuperação dos valores depende da agilidade da vítima em reportar o ocorrido, idealmente em menos de 30 minutos, pois os criminosos rapidamente transferem os fundos para múltiplas contas. Para as instituições entrevistadas, o combate eficaz às fraudes no Pix depende fundamentalmente da ampliação contínua de campanhas de conscientização, aliado a sistemas de detecção cada vez mais sofisticados e a uma maior diligência na abertura de contas. Essa estratégia emerge como a mais promissora para mitigar os riscos e proteger o ecossistema financeiro.

3.3 Mecanismos de segurança para evitar as fraudes

Para compreender a maturidade do ecossistema, além das entrevistas semiestruturadas com especialistas de três instituições parceiras: Banco do Brasil, Sicredi e Banrisul. Alguns mecanismos de segurança utilizados pelas PSPs foram mapeados através de buscas por técnicas de segurança no Pix, através da internet e modelos de inteligência artificial usando *GPT-4o* (OPENAI, 2026) e *Gemini 2.5 Pro* (GOOGLE, 2026a) em conjunto de revisões dos autores.

As instituições financeiras, junto ao BCB, estão constantemente criando e/ou evoluindo mecanismos de segurança para evitar os golpes no Pix. Algumas técnicas exigidas pelo Banco Central são obrigatórias, e outras são específicas das instituições. Dentre os obrigatórios, tem-se:

- Motores antifraude: Esses motores bloqueiam as transações suspeitas feitas durante o dia ou à noite, por um tempo específico; ou seja, as transações que não se mostrarem seguras são rejeitadas.

- Marcadores de fraude: O Banco Central identifica transações suspeitas (ou de fraude já consumada) e marca o fraudador no DICT. A partir disso, toda a rede de instituições que oferece o Pix e participa do sistema é alertada.

- Confirmação de identidade: Uso de autenticação para validar transações (e.g., senhas, biometria ou autenticação de dois fatores).

- Limites de transações: Limites para transações, especialmente no período noturno (de 20h às 6h), com valores reduzidos para transferências e possibilidade de personalização pelo cliente.
- Compartilhamento de informações de fraude: Participação em um ecossistema de informações antifraude, compartilhando alertas e informações sobre tentativas de fraude com o BACEN e outras instituições.
- Bloqueio cautelar: Possibilidade de bloquear valores transferidos por até 72 horas caso haja suspeita de fraude.

Há alguns mecanismos específicos de algumas instituições, como, por exemplo, o Modo Rua (NU, 2022). Esse mecanismo foi pioneiro no banco Nu. Mas outros bancos também estão adotando, como o modo vigilante do banco Inter, locais seguros do C6, *wi-fi* seguro do pagbank, dentre outros.

A inteligência artificial é amplamente utilizada pelo banco central e pelas PSPs para evitar os golpes, como a segurança evolutiva, que é o termo utilizado para prever problemas e propor soluções antes mesmo que eles aconteçam (NU, 2024b). A utilização da Inteligência Artificial começa antes mesmo de entrar no aplicativo da instituição. Quando o reconhecimento facial está habilitado, modelos avançados são utilizados para validar a autenticidade do usuário e bloquear acessos não autorizados. Também é amplamente utilizada por diversas instituições para detectar e prevenir fraudes e golpes, ajudando a identificar transações e compras suspeitas. Ou seja, atividades que não condizem com o habitual de um dado usuário.

Contudo, este procedimento apresenta limitações técnicas, como a restrição da amostra qualitativa ao grupo de instituições participantes, o que pode não capturar a totalidade das variações operacionais de todos os Provedores de Serviços de Pagamento (PSPs). Adicionalmente, a busca por técnicas de segurança via internet está sujeita à transparência estratégica das instituições, que frequentemente não divulgam detalhes técnicos de suas contramedidas para evitar a exposição de vulnerabilidades a potenciais atacantes.

4 METODOLOGIA

Este capítulo detalha o design metodológico adotado para o desenvolvimento das contribuições centrais desta dissertação. A pesquisa caracteriza-se como aplicada e exploratória, estruturada em duas trilhas de investigação que convergem para a entrega das contribuições descritas nos capítulos subsequentes.

O design experimental foi organizado de forma a permitir o desenvolvimento das duas trilhas em frentes técnicas e teóricas, conforme ilustrado na Figura 5. As atividades foram divididas em: (a) repositório de uma taxonomia de fraudes no Pix: Focada no mapeamento e categorização por meio da atribuição de múltiplos rótulos das metodologias de ataque ao ecossistema Pix; e (b) *dataset* de comprovantes de pagamento Pix: Dedicada à coleta, organização e anonimização de comprovantes de pagamento reais. Em paralelo, é realizada à investigação das contramedidas adotadas pelas instituições financeiras e pelo órgão regulador.

4.1 Construção da taxonomia de fraudes

O alicerce de todas as trilhas foi o Mapeamento Sistemático da Literatura (SMS), conduzido via Google Acadêmico. Foram aplicados filtros cronológicos (trabalhos a partir de 2020) e critérios de qualidade (QQ) para garantir que a fundamentação teórica refletisse o estado da arte e as lacunas reais do mercado brasileiro pós-implementação do Pix.

Para a construção do repositório de fraudes, os dados foram extraídos de fontes heterogêneas, incluindo portais de notícias especializados, relatórios de incidentes e estatísticas oficiais de vazamentos do Banco Central do Brasil.

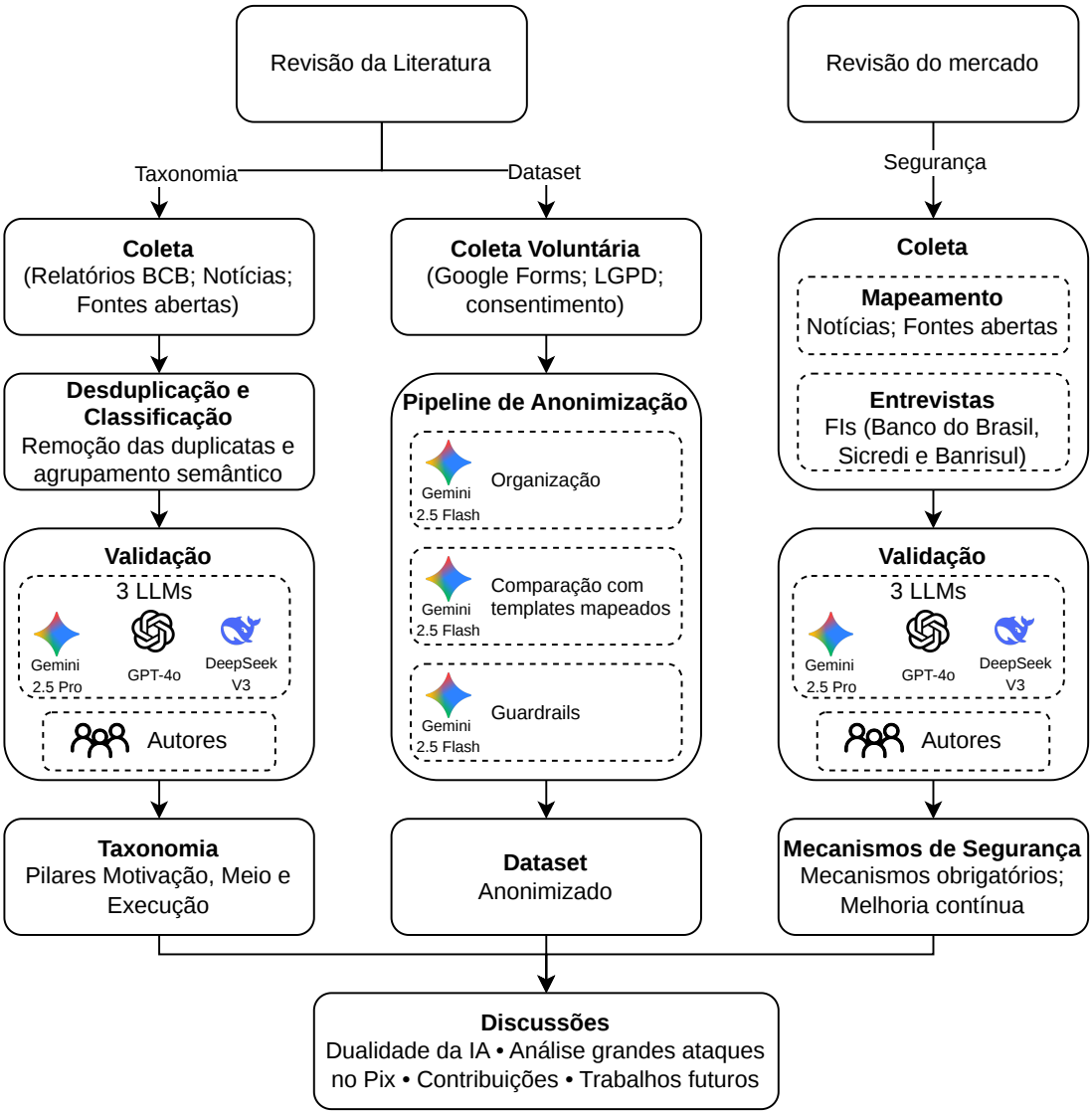
O processo de refinamento envolveu a desduplicação semântica, reduzindo 18 metodologias inicialmente mapeadas para 15 metodologias distintas. A estrutura resultante foi submetida a uma validação híbrida, contando com a revisão dos autores e o suporte analítico de três modelos de inteligência artificial: *GPT-4o* (OPENAI, 2026), *Gemini 2.5 Pro* (GOOGLE, 2026a) e *DeepSeek-V3*, garantindo a consistência dos pilares de Motivação, Meio e Execução.

4.2 Desenvolvimento e anonimização do *dataset*

A trilha técnica de dados seguiu um protocolo rigoroso de ética e privacidade, realizada por meio de formulário estruturado, com a participação voluntária de 16 colaboradores e plena conformidade com a Lei Geral de Proteção de Dados (LGPD). Um fluxo automatizado que utiliza modelo de visão computacional foi desenvolvido, utilizando a *API* paga para confrontar comprovantes de entrada com *templates* de coordenadas pré-mapeados.

Foi desenvolvido um fluxo automatizado de processamento (pipeline), utilizando *scripts* Python e o modelo *Gemini 2.5 Flash* detalhado nos seguintes estágios:

Figura 5 – Metodologia geral do trabalho



Fonte: Elaboração própria

1. **Organização e classificação**: Organiza os comprovantes de pagamento da coleta, identificando automaticamente a instituição bancária de cada comprovante.

2. **Mascaramento baseado em *templates***: Implementação de uma lógica de *matching* que confronta o comprovante de entrada com *templates* de coordenadas pré-mapeados (JSON e imagem ou pdf já anonimizado).

3. **Camada de segurança**: Utiliza inteligência artificial para validar a ausência de Identificadores Pessoais (PII) residuais após o mascaramento, garantindo a integridade do *dataset* público.

5 REPOSITÓRIO DA TAXONOMIA DE FRAUDES NO PIX

Diante da celeridade com que novas modalidades de crimes financeiros emergem, torna-se imperativo estabelecer um arcabouço teórico que organize as táticas ofensivas de forma sistemática. Este capítulo constitui o desenvolvimento e estruturação de um repositório público de uma taxonomia de fraudes no Pix, um agrupamento e categorização através da atribuição de múltiplos rótulos inédito voltado à golpes no ecossistema do Pix.

A fundamentação deste repositório baseia-se em um rigoroso levantamento de dados provenientes de fontes de notícias heterogêneas e estatísticas oficiais de vazamentos do Banco Central do Brasil (Banco Central do Brasil, 2026d). A metodologia empregada transcende a mera catalogação, envolvendo processos de desduplicação e um ciclo de validação híbrido. A etapa de validação contou com a revisão crítica do autor e os co-autores e o suporte analítico de modelos de linguagem de larga escala (*LLMs*), como *GPT-4o* (OPENAI, 2026), *Gemini 2.5 Pro* (GOOGLE, 2026a) e *DeepSeek-V3*.

A estrutura do capítulo está organizada de modo a conduzir o leitor desde o mapeamento empírico até a abstração taxonômica. Inicialmente, detalham-se as 15 metodologias de ataque distintas identificadas, seguidas por uma análise sobre a influência catalisadora da inteligência artificial na sofisticação desses delitos. Por fim, apresenta-se a taxonomia consolidada, estruturada sob os pilares de Motivação, Meio e Execução, oferecendo uma visão multidimensional que abrange desde o gatilho psicológico explorado na vítima até o mecanismo técnico de exaurimento financeiro.

5.1 Mapeamento dos principais golpes no Pix

O primeiro passo da investigação foi realizar o levantamento de dados sobre os incidentes de segurança e golpes ocorridos utilizando o Pix por meio de buscas na internet, em sites de notícias e pelas estatísticas de vazamentos divulgadas pelo Banco Central (Banco Central do Brasil, 2026d). Com esses dados, foi possível identificar e remover duplicatas; ou seja, agrupar golpes que possuíam descrições semelhantes de ações ou com diferenças mínimas, porém com nomes distintos e dados de diferentes fontes.

Através do levantamento de dados, mapearam-se 18 metodologias de ataque. Dentre elas, temos duplicatas. Estes são ataques semelhantes, com pequenas peculiaridades. Entende-se que se trata da mesma metodologia, porém detalhada de forma diferente por outra fonte. Retirando as duplicadas, temos um total de 15 metodologias de ataque distintas, sendo elas:

1. **QR Code adulterado**: Criminosos baixam transmissões legítimas (como lives de ONGs) e as retransmitem com um QR Code fraudulento para desviar doações (UFRJ, 2021).

2. **Ataques com Interação Física**: Incluem assaltos, furtos, invasões domiciliares e sequestros-relâmpago, nos quais as vítimas são coagidas a realizar transferências

Pix (SINDICONET, 2025; BRASIL, 2022).

3. **Esquema da Madonna**: Golpistas enviam mensagens em nome de celebridades solicitando doações via Pix, explorando empatia e confiança (TEMPO, 2024).

4. **Falsificação de Recibo (Pix)**: Falsificação de comprovantes de Pix com alto realismo, induzindo as vítimas a acreditarem em pagamentos inexistentes (BRASIL, 2024).

5. **Fraude do Falso Agendamento**: O criminoso envia um comprovante falso de Pix agendado e solicita a devolução imediata do valor; após receber, cancela o agendamento (RUDDER, 2023).

6. **Mão Fantasma**: Também chamado de "acesso remoto", um *malware* é instalado no celular, permitindo ao golpista operar a conta da vítima (NU, 2024a).

7. **Golpe do "Bug do Pix"**: Circulação de vídeos e mensagens afirmando falsamente que há um suposto erro no sistema Pix, que multiplicaria os valores transferidos (SERASA, 2024).

8. **Falsas Centrais Telefônicas**: A vítima é induzida a ligar para números fraudulentos após receber alertas falsos sobre supostas atividades suspeitas (UFRJ, 2021).

9. **Golpe por Engenharia Social no WhatsApp**: O golpista usa uma foto e o nome da vítima em um número novo e pede dinheiro aos contatos, alegando emergências (MAX, 2021).

10. **Golpe do perfil falso**: Criação de perfis falsos em redes sociais usando dados básicos da vítima para solicitar uma transferência Pix a seus contatos (RUDDER, 2023).

11. **Falso Funcionário de Banco**: O criminoso faz-se passar por atendente bancário, oferecendo suporte ao Pix para obter acesso à conta (FCDL/SC, 2023).

12. **Clonagem do WhatsApp**: O golpista engana a vítima ao fornecer o código SMS de ativação, clonando o aplicativo e pedindo Pix aos contatos (STONE, 2024b).

13. **Golpe do Pix Errado**: A vítima recebe um Pix inesperado e, depois, é induzida a devolver o valor, sem perceber a manipulação envolvida (DINHEIRO, 2024).

14. **Golpe do Falso Leilão**: Sites de leilão falsos exigem pagamento via Pix para garantir produtos inexistentes, explorando urgência e descontos irreais (STONE, 2024a).

15. **Esquema dos Preços Baixos**: Após comprometer redes sociais, criminosos anunciam produtos com valores atrativos e pedem pagamento antecipado (G1, 2022).

Vale salientar que, os golpes mapeados não são necessariamente exclusivos e foram criados a partir do Pix. Porém, as características do Pix, como a instantaneidade, praticidade e usabilidade, facilitam e potencializam a execução desses ataques.

Apesar do rigor metodológico aplicado na coleta e categorização, este mapeamento apresenta limitações intrínsecas. A dependência de fontes abertas e bases noticiosas pode omitir ataques que não tiveram exposição pública. Ademais, dada a natureza dinâmica das fraudes digitais, o inventário apresentado não exaure todas as modalidades possíveis, o que reforça a necessidade de atualização contínua da pesquisa.

5.1.1 Impacto da inteligência artificial nos golpes

A partir do agrupamento e da categorização, é possível dizer qual é a influência da IA nos golpes. Cada golpe foi classificado como do tipo "Pode usar IA como potencializadora" em: (a) Sim; (b) Não. Para determinar se um ataque possui potencial de ser potencializado por tecnologias emergentes, os autores conduziram estudos de possibilidade técnica fundamentados em buscas em fontes abertas e consultas aos modelos de *LLM GPT-4o* (OPENAI, 2026) e *Gemini 2.0 Pro* (GOOGLE, 2026a). Os cenários resultantes desses estudos foram analisados e validados humanamente pelos autores.

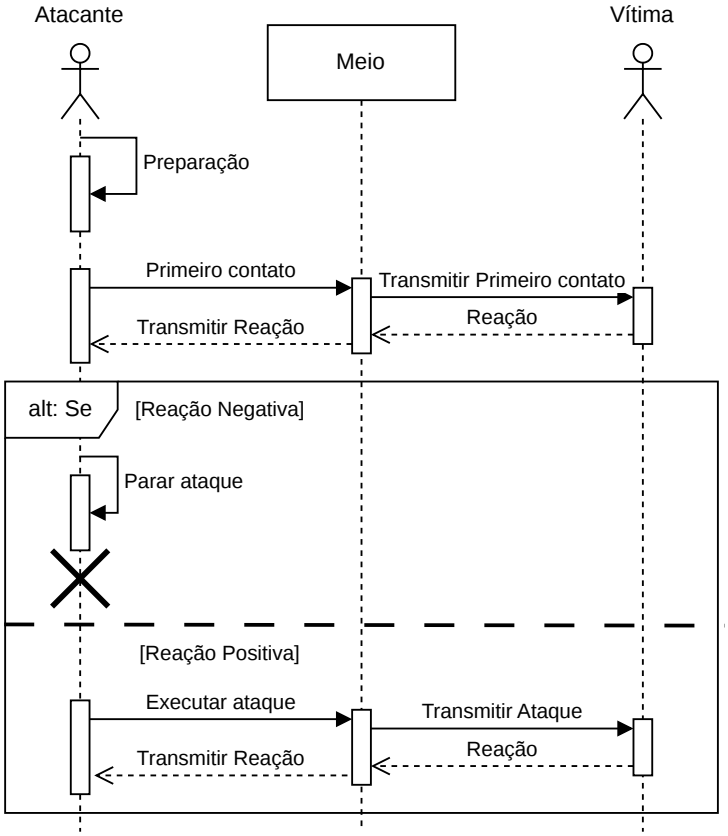
O uso de IA refere-se a situações como a produção computacional de texto ou a geração de identidades falsas, nas quais o golpista pode tentar se passar por alguém. Neste caso, o golpe utiliza IA para gerar mensagens, áudios, fotos ou vídeos para enganar potenciais vítimas. Por exemplo, um *phishing*, no qual o atacante se passa por alguém, pode ser potencializado usando *deepfake* para aumentar as chances de que uma vítima caia no golpe.

A investigação confirmou que todos os golpes mapeados podem ser potencializados por técnicas modernas de inteligência artificial. Alguns métodos de potencialização que se destacam são a capacidade da IA em aprender com as respostas automáticas e utilizar apenas as mais eficazes de acordo com o perfil do cliente, sendo extremamente adaptável para cada vítima.

Dentre as formas de potencialização com inteligência artificial destaca-se a versatilidade na criação de conteúdos falsos, como sites, perfis, comprovantes, etc. Além desses conteúdos falsos serem extremamente convincentes, é possível criá-los de forma rápida e escalável. Muitos *malwares*, scripts maliciosos ou programas mais complexos são gerados com IA de maneira fácil.

O *deepfake* é uma técnica que está avançando muito rapidamente. Conforme o tempo passa, fica mais fácil criar vídeos, fotos e áudios passando-se por alguém, o que potencializa muito os ataques de engenharia social.

Figura 6 – Fluxograma sequência de ataque



Fonte: Elaboração própria

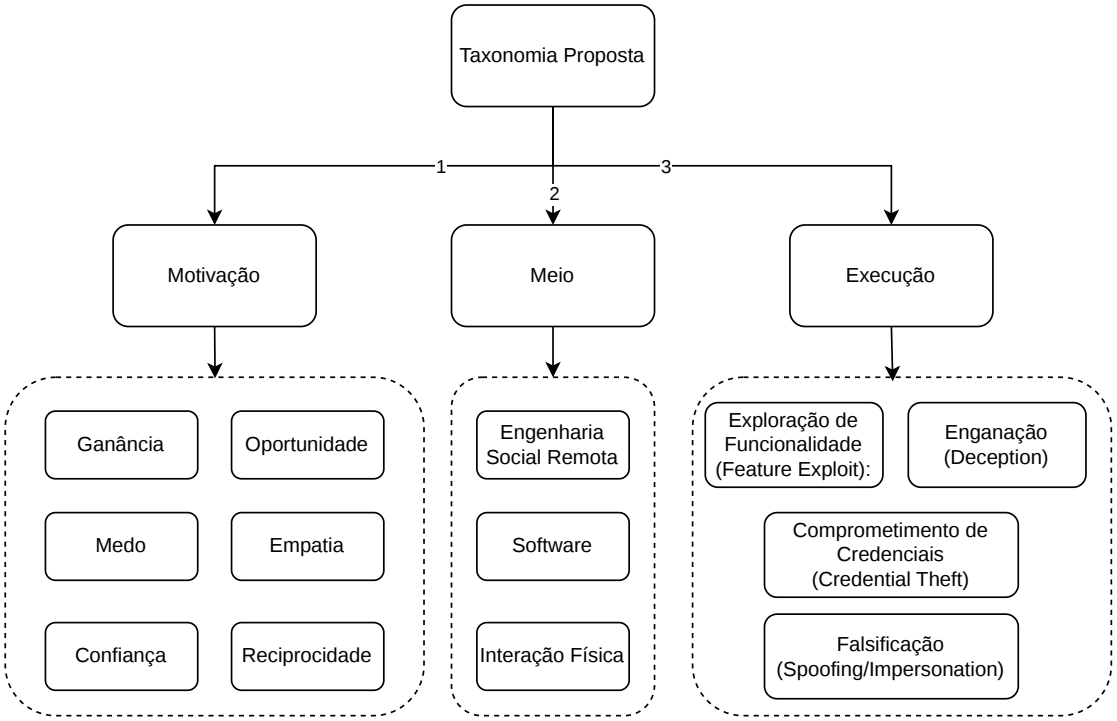
5.2 Resultados da taxonomia de fraudes no Pix

Com base no mapeamento das metodologias de golpe, propõe-se uma taxonomia estruturada, entendida como uma abordagem sistemática para organização e análise das ameaças de forma consistente e bem definida.

Os pilares da taxonomia são definidos a partir da ótica do fluxo de execução de um ataque. Ressalta-se que uma mesma metodologia pode estar associada a múltiplos elementos em cada pilar, caracterizando uma abordagem de categorização por atribuição de múltiplos rótulos. O fluxograma desse processo pode ser visualizado na Figura 6. Inicialmente, o atacante estabelece contato com a vítima por meio de um canal específico, com o objetivo de induzir uma determinada motivação associada à metodologia de golpe. A partir da reação da vítima, o atacante pode optar por descartar a tentativa ou prosseguir com a execução do ataque.

A taxonomia foi elaborada manualmente pelo autor e submetida a um processo de revisão pelos coautores. Adicionalmente, sua estrutura foi analisada por meio de uma

Figura 7 – Taxonomia de golpes no Pix



Fonte: Elaboração própria

avaliação comparativa com o suporte de três modelos de *LLM* de provedores distintos: *GPT-4o* (OPENAI, 2026), *Gemini 2.5 Pro* (GOOGLE, 2026a) e *DeepSeek-V3* (DEEPSEEK, 2026).

A proposta está organizada em três pilares principais: (a) Motivação, (b) Meio e (c) Execução. A Figura 7 apresenta, de forma detalhada, a estrutura definida.

A motivação é o gatilho (interesse ou curiosidade) despertado na vítima para iniciar o ataque. Pode-se destacar os seguintes gatilhos:

- **Ganância**: O desejo intenso e egoísta de obter vantagens financeiras rápidas e fáceis, superando a cautela.

  Exemplo de golpe: "Parabéns! Você foi sorteado para receber um retorno de 10 vezes o valor investido. Envie um PIX de R$ 200 para esta chave e receba R$ 2.000 em cinco minutos!"

- **Medo**: A emoção aflitiva que força uma ação impulsiva para evitar uma consequência negativa diante de uma ameaça iminente.

  Exemplo de golpe: "ALERTA: Uma compra suspeita de R$ 1.850 foi feita com seu cartão; para cancelar AGORA, transfira R$ 50 via PIX para a chave de segurança do nosso sistema."

- **Confiança**: A crença na credibilidade de uma suposta autoridade ou pessoa conhecida, que leva a vítima a baixar a guarda e seguir determinadas instruções.

  Exemplo de golpe: "Olá, aqui é o [nome de um amigo com WhatsApp clonado]. Estou em uma emergência e meu aplicativo do banco não está funcionando. Pode-me emprestar R$ 300 nesse PIX? Te devolvo amanhã, sem falta."

- **Oportunidade**: A percepção de uma circunstância única e imperdível que exige uma ação imediata para não se perder um grande benefício.

  Exemplo de golpe: "ÚLTIMA CHANCE: O produto que você queria está com 90% de desconto pelas próximas 2 horas. Pague agora com esta chave PIX e garanta o seu antes que o estoque acabe!"

- **Reciprocidade**: O impulso de retribuir um favor ou vantagem que você acredita ter recebido, mesmo que de forma não solicitada.

  Exemplo de golpe: "Creditamos por engano um bônus de R$ 75,00 em sua linha telefônica; como gesto de boa-fé, pedimos que devolva o valor para a chave PIX da nossa central de faturamento."

- **Empatia**: A compaixão pelo sofrimento de outra pessoa que desperta um forte desejo de ajudar imediatamente.

  Exemplo de golpe: "Mãe, meu celular quebrou e estou usando o de um amigo. Preciso pagar um conserto urgente. Transfira R$ 450 para este PIX, por favor!"

O segundo pilar é o meio, ou seja, como o atacante exerce o contato com a vítima. Nesse pilar, os ataques podem ser categorizados como:

- **Engenharia Social Remota**: Ataques usando um dos tipos de engenharia social foram detalhados no Capítulo 2.

- ***Software***: O ataque é realizado por meio de software, como, por exemplo, uma exploração de funcionalidades, *malware*, falhas sistemáticas, etc.

- **Interação Física**: Quando o ataque é realizado de forma física, como em um sequestro relâmpago.

Por último, temos a execução, que pode ter quatro subtipos. "Enganação", "Falsificação", "Exploração de Funcionalidade" e "Comprometimento de Credenciais":

- **Exploração de Funcionalidade (*Feature Exploit*)**: A exploração de funcionalidade, ou *feature exploit*, ocorre quando um atacante tira proveito de uma funcionalidade legítima, mas mal implementada ou configurada, de um sistema, software ou aplicação para realizar um ataque. Diferente de explorar uma vulnerabilidade

(um erro de programação), aqui o atacante abusa de um recurso que foi projetado para ser utilizado de uma certa forma, mas que, devido a falhas na sua concepção ou na maneira como é utilizado, pode ser manipulado para fins maliciosos.

Exemplo: O atacante utiliza a funcionalidade de agendamento e, através de engenharia social, envia uma mensagem a vítima dizendo que foi por engano e pedindo para que ela envie o valor de volta. Após a transferência da vítima, o atacante cancela o agendamento.

- **Falsificação (*Spoofing/Impersonation*)**: A falsificação, conhecida como spoofing ou impersonation, é a arte de disfarçar a identidade de um atacante para parecer uma entidade confiável, como uma pessoa, um sistema, um site ou uma organização. O objetivo principal é enganar a vítima para que ela confie no atacante e, assim, divulgue informações confidenciais, realize ações indesejadas ou permita o acesso a sistemas restritos.

  Exemplo: O golpista passa-se por um funcionário de banco, um técnico de segurança ou até mesmo um parente ou amigo em apuros. Isso pode ser feito por meio de chamadas telefônicas, mensagens de WhatsApp, SMS ou e-mails. Eles podem usar números de telefone falsificados (spoofing de número) ou perfis falsos nas redes sociais para aumentar a credibilidade.

- **Enganação (*Deception*)**: A enganação, ou *deception*, é uma tática ampla que envolve manipular a percepção de uma pessoa ou sistema para levá-los a tomar decisões que beneficiem o atacante. Diferente da falsificação, que se concentra em mudar a identidade, a enganação foca em criar uma situação ou cenário falso para influenciar o comportamento da vítima. Muitas vezes, a falsificação é uma ferramenta usada dentro de uma estratégia maior de engano.

  Exemplo: Um atacante alega que a conta da vítima foi invadida, que há uma transação suspeita ou que o aplicativo bancário precisa de uma "atualização de segurança urgente".

- **Comprometimento de Credenciais (*Credential Theft*))**: O comprometimento de credenciais, ou *credential theft*, é o ato de roubar nomes de usuário, senhas ou outras formas de autenticação que dão acesso a sistemas, contas ou redes. Este é frequentemente o objetivo final de muitos ataques de falsificação e enganação, pois as credenciais são a chave para acessar informações valiosas e realizar ações maliciosas em nome da vítima.

  Exemplo: Em alguns casos, o golpista pode tentar direcionar a vítima para um site falso (*phishing*) que imita o banco, pedindo que ela insira suas credenciais. Com as credenciais em mãos, o golpista pode, então, realizar transações.

A Tabela 5 descreve a taxonomia obtida para os golpes mapeados de acordo com os 3 pilares propostos.

Tabela 5 – Categorização individual dos golpes mapeados

Trab.	**Motivação**	**Meio**	**Execução**
[01]	Confiança, empatia	Engenharia Social Remota	Enganação (Deception), Falsificação (Spoofing/ Impersonation)
[02]	Medo	Interação Física, Engenharia Social	Comprometimento de Credenciais (Credential Theft), Falsificação (Spoofing/ Impersonation)
[03]	Confiança, empatia	Engenharia Social Remota	Falsificação (Spoofing/ Impersonation), Enganação (Deception)
[04]	Confiança	Engenharia Social Remota	Enganação (Deception), Falsificação (Spoofing/ Impersonation)
[05]	Reciprocidade, empatia, confiança	Engenharia Social Remota	Enganação (Deception), Exploração de Funcionalidade (Feature Exploit), Falsificação (Spoofing/ Impersonation)
[06]	Confiança, medo, oportunidade	Engenharia Social Remota, Software	Comprometimento de Credenciais (Credential Theft), Falsificação (Spoofing/ Impersonation), Enganação (Deception)
[07]	Ganância, oportunidade	Engenharia Social Remota	Falsificação (Spoofing/ Impersonation), Enganação (Deception)
[08]	Confiança, medo	Engenharia Social Remota	Enganação (Deception), Comprometimento de Credenciais (Credential Theft), Falsificação (Spoofing/Impersonation)
[09]	Medo, confiança, empatia	Engenharia Social Remota	Falsificação (Spoofing/Impersonation), Enganação (Deception)
[10]	Confiança, empatia	Engenharia Social Remota	Falsificação (Spoofing/Impersonation), Enganação (Deception)
[11]	Medo, confiança, oportunidade	Engenharia Social Remota	Falsificação (Spoofing/Impersonation), Exploração de Funcionalidade (Feature Exploit), Comprometimento de Credenciais (Credential Theft)
[12]	Confiança, medo, empatia	Engenharia Social Remota	Falsificação (Spoofing/Impersonation), Enganação (Deception), Comprometimento de Credenciais (Credential Theft)
[13]	Reciprocidade, confiança, empatia	Engenharia Social Remota	Enganação (Deception), Exploração de Funcionalidade (Feature Exploit), Falsificação (Spoofing/Impersonation)

[14]	Oportunidade, ganância	Engenharia Social Remota	Enganação (Deception), Falsificação (Spoofing/Impersonation)
[15]	Oportunidade, ganância	Engenharia Social Remota	Comprometimento de Credenciais (Credential Theft), Enganação (Deception), Falsificação (Spoofing/Impersonation)

Fonte: Elaboração própria

Conforme a Tabela 5[1]. No que tange ao pilar Motivação, a Confiança demonstrou ser o gatilho mais explorado pelos fraudadores, presente na maioria dos golpes mapeados. Os criminosos buscam estabelecer uma relação de credibilidade, seja passando-se por uma instituição oficial ou por um conhecido, para baixar a guarda da vítima. Em segundo plano, destacam-se o Medo, utilizado para coagir vítimas em assaltos ou falsas centrais de segurança, e a Empatia, explorada em golpes que simulam emergências familiares ou campanhas de doação. A Ganância e a Oportunidade aparecem frequentemente atreladas, focadas em promessas de vantagens financeiras irreais.

Quanto ao Meio de propagação, a predominância é absoluta da Engenharia Social Remota, que foi identificada como vetor em quase a totalidade dos incidentes analisados. Isso corrobora a tese de que o fator humano é o elo mais visado no ecossistema Pix. As exceções ficam por conta de vetores técnicos específicos, como o uso de Software (*malware*) no golpe da "Mão Fantasma" e a Interação Física, restrita a crimes de violência direta, como sequestros-relâmpago.

Por fim, a análise da Execução revela que a Falsificação e a Enganação são as técnicas transversais mais recorrentes, fundamentais para sustentar a narrativa do golpe em quase todos os cenários. Técnicas como o Comprometimento de Credenciais aparecem como consequência em golpes específicos, enquanto a Exploração de Funcionalidade é utilizada de forma pontual para abusar de recursos legítimos do sistema.

[1] A Taxonomia dos golpes no Pix está disponível no *Kaggle* em <https://www.kaggle.com/datasets/glenerpizzolato/classificaotaxonomia-de-golpes-no-pix/data> (PIZZOLATO, 2025)

6 *DATASET* DE COMPROVANTES DE PAGAMENTO PIX

Antes de criar o *dataset* de comprovantes de pagamento Pix, foi realizada uma busca para identificar se já existia algum *dataset* com esse objetivo ou semelhante. A busca foi realizada no Kaggle (KAGGLE, 2026) e no Google *dataset* search (GOOGLE, 2026b), usando como palavras-chave: "Pix", "*Brazilian Instant Payment*", "*payment receipts*" e "*banking transaction*". Os resultados desta etapa estão sintetizados na Tabela 6.

Tabela 6 – *Datasets* resultantes da busca na literatura

Nome	Mês/Ano	Amostras	Características	Referência
pix-banking-transaction	08/2025	10.000	15	(BUENO, 2025)
brazilian-payment-methods	10/2024	102	13	(VIEIRA, 2024)

Fonte: Elaboração própria

A base *brazilian-payment-methods* foca na dinâmica macroeconômica dos métodos de pagamento no Brasil, apresentando dados quantitativos e comparativos entre Pix, TED e boletos. Contudo, tais dados são de natureza estatística e não atendem à necessidade de análise individual de transações.

O *dataset pix-banking-transaction* (BUENO, 2025) apresentou-se como o mais próximo do escopo desta pesquisa. Entretanto, observaram-se duas limitações críticas para os objetivos deste trabalho: a ausência de elementos visuais (composição estritamente textual e estruturada) e a origem sintética dos dados, o que pode não refletir integralmente as nuances e anomalias de casos reais. Outras fontes, como o portal *ceicdata.com*, foram consultadas, mas descartadas por se concentrarem apenas em métricas de volume e proporção de uso do sistema.

Diante da inexistência de uma base que contemplasse imagens de documentos reais, procedeu-se à coleta primária de dados. Para tanto, elaborou-se um formulário estruturado na plataforma *Google Forms*, o qual foi compartilhado via *e-mail* para todo o grupo de alunos da Universidade Federal do Pampa e no Linkedin[1]. A coleta baseou-se no fornecimento voluntário e anônimo de comprovantes autênticos por parte dos colaboradores.

O formulário era sucinto e claro, trazendo informações sobre o objetivo da coleta; TCLE (Termo de Consentimento Livre e Esclarecido); Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), reforçando que todos os dados coletados seriam utilizados exclusivamente para fins acadêmicos e de pesquisa; os dados sensíveis foram anonimizados; quem teria acesso, como seria o armazenamento; o tempo que seriam mantidos e as instruções sobre a solicitação de exclusão dos mesmos; e sobre o sorteio. O formulário da coleta dos comprovantes pode ser conferido no Apêndice B.

Como estímulo para a participação, foi realizado um sorteio de R$ 100,00 entre os participantes. Cada comprovante contava como uma entrada no sorteio. Quanto mais

[1] *https://www.linkedin.com/in/glenerpizzolato/*

comprovantes fossem enviados, maior era a chance de vitória.

6.1 Implementação da pipeline de anonimização de dados sensíveis

Todo o processo e a referência ao arquivo citado nesta seção estão disponíveis em <https://github.com/glener10/job-llm-PII-anonymization-by-templates> (PIZZOLATO, 2026).

Após a etapa de coleta via formulário, os arquivos são centralizados em um diretório no *Google Drive*. Inicialmente, os comprovantes são armazenados de forma não estruturada, seguindo a nomenclatura padrão:

```
NOME_ARQUIVO - NOME_PARTICIPANTE.EXTENSÃO
```

Para viabilizar a análise, foi executado um processo de organização automatizado através do arquivo *scripts/file_organizer.py*. Este procedimento reestruturou os arquivos em uma hierarquia de diretórios categorizada por usuário.

```
payment-receipts/
├── Glener/
│   └── comprovante_pix_01 - Glener.png
└── Claudio/
    └── comprovante_pix_02 - Claudio.png
```

Após essa separação do envio foi utilizado o caso de uso *src/usecases/get_bank_of_payment_receipt.py* para identificar de forma automatizada a qual banco pertence aquele comprovante de pagamento. Foi utilizado o modelo *Gemini 2.5 Flash* (GOOGLE, 2026a), a instrução está descrita abaixo no *Prompt* 6.1.

Prompt 6.1 – Prompt de identificação da instituição bancária.

```
1 Você é um especialista em bancos e comprovantes de pagamentos
  Pix, sua função é receber um comprovante (imagem ou PDF), e
  identificar de qual banco é aquele comprovante de pagamento Pix.
2 Responda apenas com o nome do banco, sem nenhuma outra
  informação adicional.
```

Resultando na estrutura organizada abaixo:

```
payment-receipts/
├── Glener/
│   └── nu/
│       └── comprovante_pix_01 - Glener.png
└── Claudio/
    └── xp/
        └── comprovante_pix_02 - Claudio.png
```

A sistematização apresentada permite a segregação dos dados em múltiplos níveis de granularidade. Como exemplo, um comprovante enviado pelo usuário "Glener", referente a uma transação na instituição "Nu", é automaticamente movido para o subdiretório correspondente sob a raiz do projeto. Da mesma forma, registros de outros colaboradores, como o usuário "Claudio" com transações da "XP", são alocados em pastas distintas.

O processo de anonimização é feito a partir de uma lista de *templates*. Cada *template* é composto por um par de arquivos: um json com as coordenadas dos locais dos dados sensíveis; e um comprovante de pagamento anonimizado, o qual será utilizado para a comparação com o comprovante de entrada usando LLM.

Um novo *template* é criado através do script *scripts/create_coordinates.py*. Basta preencher os locais de dados sensíveis, e será gerado um par com a imagem ou pdf anonimizado e um json das coordenadas.

Para mitigar a execução da comparação do *template* com o comprovante de entrada, limitou-se a executar as comparações somente dos *templates* de um determinado banco e de uma determinada extensão. Por exemplo, para o comprovante de pagamento abaixo, serão carregados todos os *templates* disponíveis do banco "Nu" que sejam imagens:

```
payment-receipts/
├── Glener/
│   └── nu/
│       └── comprovante_pix_01 - Glener.png
```

Com todos *templates* carregados é executado o caso de uso *src/usecases/matcher.py*, que tem como objetivo identificar se o comprovante de entrada corresponde a algum dos *templates* carregados. Nessa etapa é utilizado o modelo *Gemini 2.5 Flash* (GOOGLE, 2026a) com a configuração descrita na Tabela 7.

A utilização de *Top-K* $= 1$ e *Temperature* $= 0.0$ visa eliminar a estocasticidade do modelo, garantindo que a classificação dos comprovantes seja determinística e baseada exclusivamente na maior probabilidade estatística de acerto. A instrução utilizada nessa etapa está evidenciada no *Prompt* 6.2.

Prompt 6.2 – Prompt de identificação da template correspondente.

Tabela 7 – Configurações de chamada do *Gemini 2.5 Flash* para identificação de template correspondente e *guardrails*

Parâmetro	**Valor**	**Descrição**
Temperature	0.0	Garante respostas determinísticas.
Top_p	1.0	Considera todo o espectro de probabilidade acumulada.
Top_k	1	Seleciona apenas o *token* mais provável.
Max Output Tokens	2048	Limite máximo de *tokens* na resposta.

```
<PERSONA>
Você é um Analista Forense de Documentos Bancários especializado em detecção de fraude e verificação de templates.
</PERSONA>

<CONTEXTO>
O objetivo é verificar se dois comprovantes de Pix pertencem ao mesmo "Layout Mestre" (mesmo banco, mesma versão de app).
Você receberá duas imagens. Uma delas pode conter tarjas pretas (censura de dados sensíveis).
</CONTEXTO>

<INSTRUCOES_DE_VISAO>
1. **Ignore as Tarjas:** Trate tarjas pretas/coloridas cobrindo valores como "ruído irrelevante". O layout existe *através* delas.
2. **Foco nas Chaves (Keys):** Identifique os rótulos dos campos (ex: "Destinatário", "Valor", "Data", "ID da transação").
3. **Foco na Identidade Visual:** Logotipo do banco, cor de fundo do cabeçalho, fontes utilizadas.
</INSTRUCOES_DE_VISAO>

<ALGORITMO_DE_COMPARACAO>
Execute mentalmente estes passos:
1. Identifique a instituição financeira de ambas as imagens. Se forem diferentes -> `is_match: false`.
2. Extraia a lista ordenada de CHAVES (Labels) da Imagem A (de cima para baixo).
3. Extraia a lista ordenada de CHAVES (Labels) da Imagem B (de cima para baixo).
4. Compare as duas listas. Elas devem ser idênticas em conteúdo e ordem.
    * *Permissão:* Aceite pequenas variações de OCR ou corte de imagem (ex: rodapé cortado), desde que o "corpo" do comprovante
```

```
seja igual.
    * *Proibição:* Se a Imagem A tem os campos alinhados À esquerda e a Imagem B centralizados, isso é uma quebra de estrutura.
</ALGORITMO_DE_COMPARACAO>

<CRITERIOS_DE_CONFIANCA>
- 1.0: Mesmo banco, logos idênticos, mesma lista de chaves na exata mesma ordem visual.
- 0.8: Mesmo banco e estrutura, mas uma imagem tem qualidade inferior ou corte leve que dificulta leitura de 1 ou 2 chaves.
- 0.2: Mesmo banco, mas layout diferente (ex: comprovante web vs comprovante mobile).
- 0.0: Bancos diferentes ou documentos não relacionados.
</CRITERIOS_DE_CONFIANCA>

<FORMATO_DE_RESPOSTA>
Responda APENAS com o JSON. Não inclua markdown (```json).
Certifique-se de preencher o campo "reason" com a evidência: liste as chaves encontradas em ambos para justificar.
```

Caso o comprovante de entrada não tenha nenhum *template* correspondente, é necessário criar um novo *template*, resultando assim em uma pipeline de integração contínua. Caso seja encontrado algum *template* correspondente, realiza-se a anonimização com as coordenadas através do caso de uso *src/usecases/masking.py* e na sequência, é executado o *guardrails* (*src/usecases/guardrails.py*) para validar se nenhum dado sensível, mesmo após a anonimização, passou despercebido. A configuração utilizada está na Tabela 7. A instrução utilizada no processo de *guardrails* pode ser conferida abaixo no *Prompt* 6.3. O fluxo completo está descrito na imagem 8.

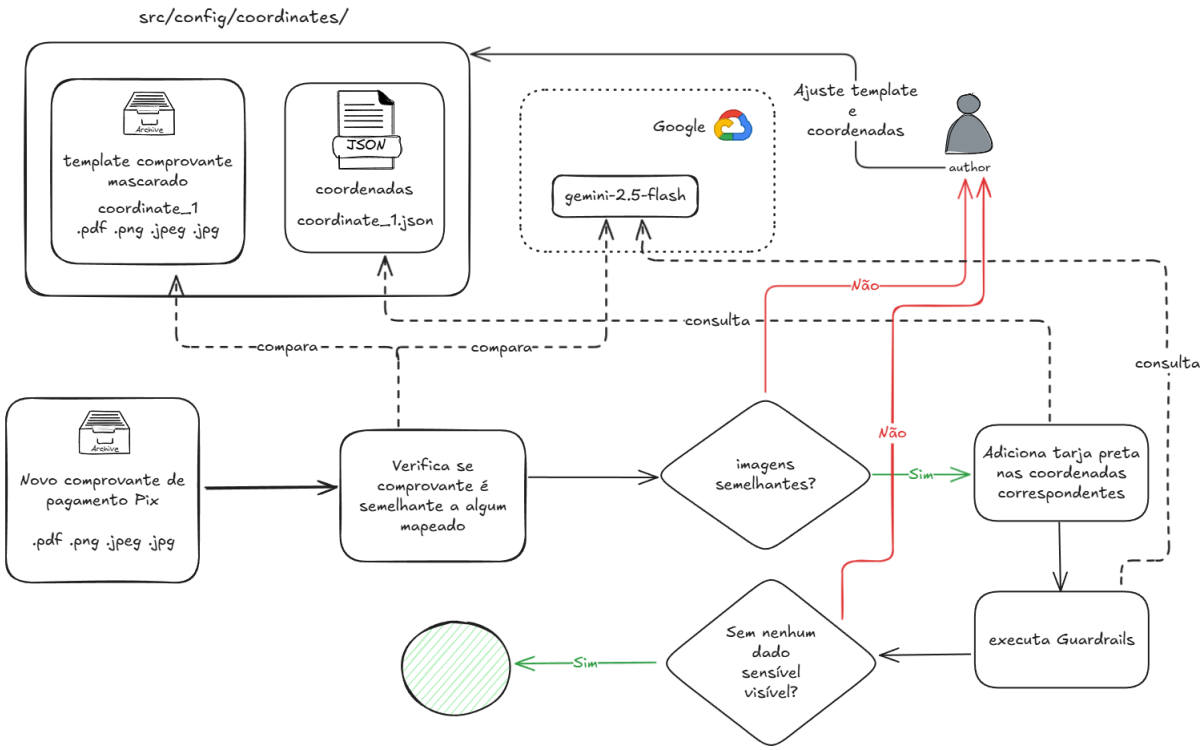
Prompt 6.3 – Prompt para validação de dado sensível após anonimização.

```
<PERSONA>
Você é um Auditor de Segurança da Informação (DLP) altamente cético. Sua única função é bloquear o vazamento de PII (Personally Identifiable Information).
</PERSONA>

<CONTEXTO_VISUAL>
Você está analisando comprovantes bancários Pix.
- Estrutura típica: Um RÓTULO (ex: "Destinatário") seguido de um VALOR (ex: "João da Silva").
- O usuário tentou anonimizar os VALORES aplicando tarjas pretas
```

```
(retângulos sólidos).
</CONTEXTO_VISUAL>

<DEFINICAO_DE_DADO_SENSIVEL>
Considere como SENSÍVEL (Vazamento) se qualquer um destes estiver visível:
1. Nomes de Pessoas (Pessoa Física). Nota: Nomes de Bancos ou Instituições de Pagamento NÃO são sensíveis.
2. CPF ou CNPJ (parcial ou total, observe que se o CNPJ for da instituição que está enviando ou recebendo o Pix não é um dado sensível, apenas se for chave Pix).
3. Agência e Conta.
4. Chaves Pix (E-mail, Telefone, CPF).
</DEFINICAO_DE_DADO_SENSIVEL>

<REGRAS_DE_OURO>
1. **Rótulo != Valor:** O texto "CPF" ou "Nome" impresso no layout é apenas um rótulo. Isso é SEGURO. O vazamento só ocorre se o NÚMERO do CPF ou o NOME da pessoa estiver legível.
2. **A Regra da Tarja:** - Se um valor está coberto por uma tarja preta sólida: SEGURO (Ignore).
   - Se a tarja é translúcida e permite leitura: VAZAMENTO.
   - Se a tarja cobre apenas metade do nome/número: VAZAMENTO.
3. **Ignore (Safe List):**
   - Valores monetários (R$ 50,00).
   - Datas e Horários.
   - IDs de Transação (sequências longas de letras e números aleatórios).
   - Nomes de Bancos (ex: "Nubank", "Itaú", "Banco Central").
   - Mensagens de rodapé.
</REGRAS_DE_OURO>

<PROCEDIMENTO_DE_ANALISE>
Analise cada campo visualmente:
Passo 1: Identifique um campo (ex: Nome do Favorecido).
Passo 2: Olhe para o valor deste campo.
Passo 3: O valor é legível?
    - NÃO (tem tarja preta) -> OK.
    - SIM -> É um nome de banco ou dado da Safe List?
        - SIM -> OK.
        - NÃO -> ALERTA DE VAZAMENTO.
</PROCEDIMENTO_DE_ANALISE>
```

```
42
43 <FORMATO_RESPOSTA>
44 Retorne apenas o JSON. Se encontrar vazamento, adicione o nome
   do campo em 'leaked_fields'.
```

Figura 8 – Fluxo anonimização com *templates* e coordenadas



Como esta se trabalhando com dados sensíveis, é preciso utilizar modelos de IA de forma controlada para não vazar informações. Inicialmente, utilizou-se o *ollama* para executar modelos localmente, mas estes não obtiveram bons resultados. Dentre eles, foram testados os seguintes modelos com possíveis causas dos resultados negativos:

1. *minicpm-v*: Modelo extremamente compacto que realiza redimensionamentos consideráveis, prejudicando a assertividade.

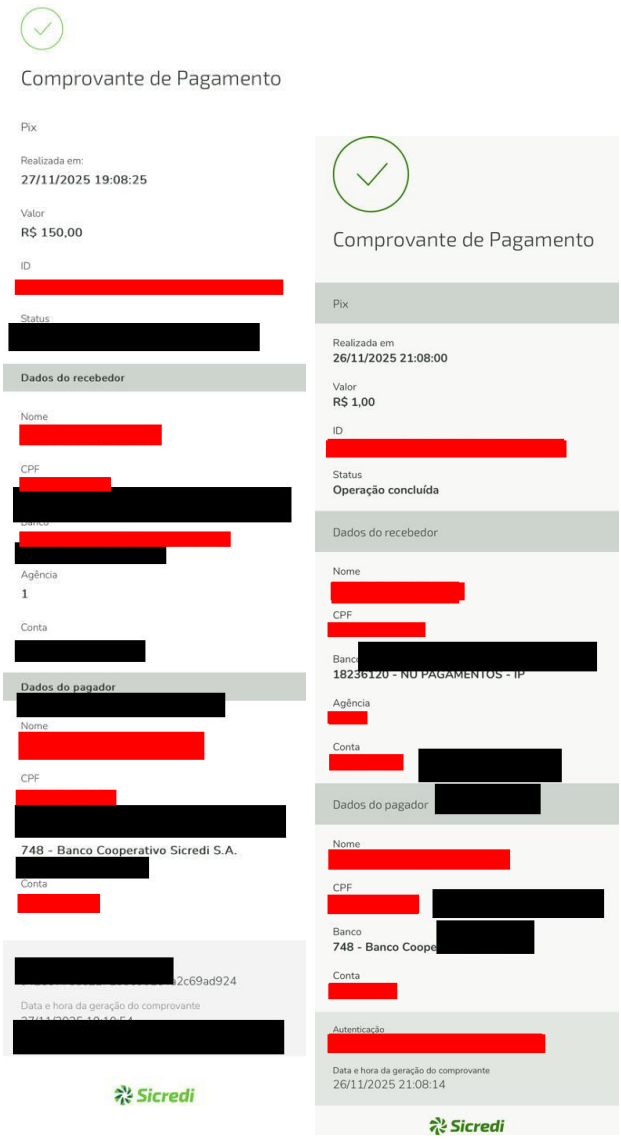
2. *qwen3-vl:8b*: Utiliza um processador visual leve que simplifica a estrutura dos dados da imagem e reduz sua resolução original.

3. *gemma3:4b* e *gemma3:12b*: São modelos otimizados para a identificação e localização de objetos em cenas, em vez da análise detalhada de textos. Eles possuem um módulo de captura de imagem com menor capacidade de percepção de detalhes finos.

4. *qwen2.5vl:7b*: É um modelo mais robusto que os anteriores, mas que ainda assim realiza redimensionamentos que prejudicam a assertividade.

Percebeu-se que a IA alucinava, citando *templates* erroneamente, conforme pode-se ver na imagem da Figura 9. As tarjas em preto foram onde a IA anonimizou de acordo com as coordenadas. As tarjas em vermelho são onde estariam, de fato, os dados sensíveis. Nessa etapa, o *guardrails* foi extremamente importante para identificar as anonimizações problemáticas, automatizando a execução e acelerando o processo.

Figura 9 – Anonimização incorreta com modelo qwen2.5vl:7b



Como alternativa, foi necessário usar um modelo mais robusto, como *qwen2.5vl:32b*. No entanto, este não foi suportado pelo computador usado para o processamento (*workspace*[2]). Uma alternativa possível seria utilizar o Google Colab ou contratar um computador dedicado para rodar o modelo. Por fim, foi decidido executar o modelo *gemini-2.5-flash* com a API paga. Nesse modo, o Google não usa os dados utilizados para treinar o modelo (GOOGLE, 2025).

[2] Especificação da Máquina: Processador 13th Gen Intel(R) Core(TM) i5-13450HX 2.40 GHz; 16 GB de RAM; Placa de vídeo NVIDIA GeForce RTX 3050 6 GB.

A pipeline mostrou-se muito eficaz, rápida e com baixo custo em casos com poucos *templates*, visto que é necessário criar manualmente cada conjunto de uma entrada anonimizada e o mapa das coordenadas onde estão os dados sensíveis. Por mais que o processo de criação seja rápido e fácil, caso haja muitos formatos de entrada, o tempo da pipeline pode escalar consideravelmente. Além disso, na pipeline são executadas muitas comparações entre uma entrada e um dado *template*. Consequentemente, se houver muitos *templates*, será necessário executar muitas comparações.

6.2 Análise dos resultados do *dataset*

Para a validação da metodologia proposta, consolidou-se um dataset contendo 142 comprovantes de pagamento Pix[3], obtidos por meio da colaboração voluntária de 16 participantes. A amostragem abrange um total de 13 instituições financeiras distintas, garantindo a heterogeneidade necessária.

A distribuição das amostras detalhada na Tabela 8 revela uma concentração predominante no banco Nu, que representa individualmente 49,3% do volume total (70 comprovantes), seguido pelas instituições XP (16,9%) e Sicredi (9,2%). No que tange aos formatos de arquivo, o dataset apresenta uma prevalência de arquivos de imagem comprimida (JPEG), correspondendo a 62% das entradas, seguidos por documentos portáteis (PDF), que compõem 35,2% da base. Essa diversidade de formatos exigiu que a pipeline de processamento fosse capaz de manipular tanto extração visual quanto textual com a mesma eficácia.

Para processar essa variedade, foi necessário o mapeamento de 54 templates de anonimização distintos, conforme explicado na pipeline de anonimização na seção 4.2. Conforme apresentado na Tabela 9, observa-se uma correlação direta entre a quantidade de amostras e a diversidade de templates: o banco Nu, devido à sua maior representatividade e atualizações frequentes de layout, demandou a criação de 23 templates (42,6% do total), enquanto a maioria das outras instituições exigiu entre um e dois modelos de referência para cobrir suas variações.

Pode-se acompanhar alguns resultados da anonimização correta na Figura 10, com comprovantes de pagamento Pix das instituições Sicredi e Nu. Na Figura 11 evidenciam-se os resultados da anonimização dos bancos Nu e Banrisul.

O *dataset* possui limitações quanto à sua abrangência, uma vez que o volume de amostras é condicionado à adesão voluntária na pesquisa aplicada. Adicionalmente, observa-se uma concentração de dados provenientes de instituições específicas, o que pode restringir a representatividade do conjunto frente à totalidade do ecossistema bancário nacional.

[3] Por questões de segurança, o *dataset* está disponível mediante solicitação ao autor, pelo e-mail *glenerpizzolato@gmail.com*. O acesso está sujeito à avaliação do solicitante e restrito às amostras cujos participantes autorizaram o compartilhamento do conjunto de dados anonimizado com terceiros.

Tabela 8 – Distribuição de amostras por instituição e tipo

Instituição	**Total geral**		**Extensão das amostras**							
	Qtd	**%**	**jpeg**		**jpg**		**png**		**pdf**	
			Qtd	%	Qtd	%	Qtd	%	Qtd	%
Itaú	11	7,7%	7	63,6%	0	0,0%	0	0,0%	4	36,4%
99Pay	2	1,4%	2	100,0%	0	0,0%	0	0,0%	0	0,0%
Banrisul	4	2,8%	1	25,0%	0	0,0%	0	0,0%	3	75,0%
BB	7	4,9%	3	42,9%	0	0,0%	0	0,0%	4	57,1%
Caixa	2	1,4%	0	0,0%	0	0,0%	0	0,0%	2	100,0%
Inter	5	3,5%	5	100,0%	0	0,0%	0	0,0%	0	0,0%
MercadoPago	1	0,7%	0	0,0%	0	0,0%	1	100,0%	0	0,0%
Next	1	0,7%	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Nu	70	49,3%	41	58,6%	1	1,4%	1	1,4%	27	38,6%
PicPay	1	0,7%	0	0,0%	0	0,0%	0	0,0%	1	100,0%
Santander	1	0,7%	0	0,0%	0	0,0%	0	0,0%	1	100,0%
Sicredi	13	9,2%	5	38,5%	0	0,0%	0	0,0%	8	61,5%
XP	24	16,9%	24	100,0%	0	0,0%	0	0,0%	0	0,0%
Total	**142**	**100,0%**	**88**	**61,97%**	**2**	**1,41%**	**2**	**1,41%**	**50**	**35,21%**

Tabela 9 – Distribuição de *templates* por instituição e tipo

Instituição	**Total geral**		**Extensão dos *templates***			
	Qtd	**%**	**png**		**pdf**	
			Qtd	%	Qtd	%
Itaú	4	7,4%	3	75,00%	1	25,00%
99Pay	2	3,7%	2	100,00%	0	0,00%
Banrisul	2	3,7%	1	50,00%	1	50,00%
BB	7	13,0%	3	42,86%	4	57,14%
Caixa	1	1,9%	0	0,00%	1	100,00%
Inter	1	1,9%	1	100,00%	0	0,00%
MercadoPago	1	1,9%	1	100,00%	0	0,00%
Next	1	1,9%	1	100,00%	0	0,00%
Nu	23	42,6%	14	60,87%	9	39,13%
PicPay	1	1,9%	0	0,00%	1	100,00%
Santander	1	1,9%	0	0,00%	1	100,00%
Sicredi	6	11,1%	3	50,00%	3	50,00%
XP	4	7,4%	4	100,00%	0	0,00%
Total	**54**	**100,00%**	**33**	**61,11%**	**21**	**38,89%**

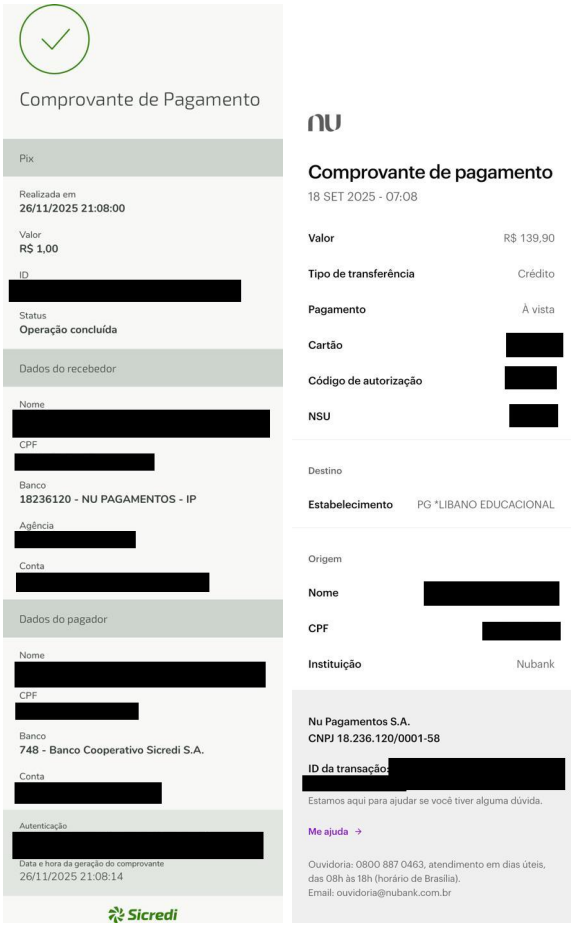


Figura 10 – Exemplos de anonimização correta: Bancos Sicredi e Nu

Figura 11 – Exemplos de anonimização correta: Bancos Nu e Banrisul

7 CONCLUSÃO

Este capítulo apresenta as contribuições advindas dos resultados obtidos, uma discussão a respeito dos mecanismos de defesa, impacto do uso da inteligência artificial e a segurança dos métodos de pagamento do brasil, bem como trabalhos futuros.

7.1 Contribuições

O presente trabalho apresenta duas principais contribuições: (a) um repositório das principais metodologias de ataques no Pix e uma categorização/agrupamento (taxonomia) dos mesmos;[1] e (b) um *dataset* de comprovantes de pagamento Pix e uma pipeline para anonimizar dados sensíveis em imagens e PDFs. Uma revisão abrangente das metodologias de ataques envolvendo o sistema Pix foi desenvolvida, mapeando quinze golpes distintos e propondo uma taxonomia dessas fraudes de forma estruturada, que organiza esses incidentes segundo motivação, meio e execução. Os resultados mostram uma evolução clara das estratégias criminosas, que migraram de métodos simples para abordagens híbridas cada vez mais sofisticadas, combinando manipulação psicológica, exploração técnica e uso intensivo de mecanismos automatizados.

O mapeamento das metodologias de ataque, em conjunto com a categorização, facilita novos estudos sobre segurança no Pix. A taxonomia compartilhada em (PIZZOLATO, 2025)[2] pode agir como um guia nacional de golpes relacionados ao Pix, servindo como base para pesquisa em segurança digital, aprendizado de máquina e criação de simuladores de fraude para testes controlados. Essas iniciativas têm potencial para fortalecer a resiliência do ecossistema Pix, além de acompanhar a crescente sofisticação das ameaças observadas. Organizar os incidentes facilita a extensão do estudo e ajuda no desenvolvimento de novos mecanismos de defesa para evitar os golpes. Além disso, a organização pode servir para criar e direcionar campanhas de conscientização com o intuito de educar os usuários e mitigar as vítimas dos golpes.

Para a criação do *dataset* foi desenvolvida uma pipeline para fazer a anonimização dos dados sensíveis em imagens de PDFs. *Datasets* são fundamentais para servir de alicerces na criação de novos modelos cada vez mais eficazes na percepção visual de falsificações. Estes conjuntos de dados permitem transitar de uma postura defensiva reativa para uma estratégia de inteligência antecipatória, essencial para o enfrentamento de ameaças emergentes, viabilizando testes comparativos rigorosos e o estudo aprofundado de padrões ilícitos. Assim, a consolidação dessas bases de referência é crítica para capacitar pesquisadores e sistemas a identificar, com maior precisão, tanto as vulnerabilidades em documentos visuais quanto as novas estratégias adotadas por fraudadores.

---

[1] Alguns resultados preliminares desta dissertação foram apresentados no trabalho "Mapeamento e Análise de Metodologias de Fraude Aplicadas ao Pix no Brasil" na XXII Escola Regional de Redes de Computadores (PIZZOLATO et al., 2025).

[2] <https://www.kaggle.com/datasets/glenerpizzolato/classificaotaxonomia-de-golpes-no-pix/data>

7.2 Melhoria continua nos mecanismos de defesa

A análise evidencia que a maior parte das fraudes ocorre por engenharia social, destacando a centralidade do fator humano na superfície de ataque. As entrevistas com representantes do Banco do Brasil, Sicredi e Banrisul comprovaram essa afirmação, uma vez que a rapidez das transações do Pix e a pulverização imediata dos valores dificultam a recuperação. As instituições utilizam autenticação multifatorial, sistemas de detecção baseados em IA e campanhas de conscientização, mas há consenso de que a velocidade dos criminosos e a vulnerabilidade emocional dos usuários ainda constituem gargalos críticos.

Com o aumento dos incidentes de segurança e vazamentos cadastrais, é um fato que o Banco Central continua a adotar medidas preventivas contra ataques. Em 28 de setembro de 2021, foi implantado o Bloqueio Cautelar (Banco Central do Brasil, 2021b), que ocorre quando há suspeita de fraude no momento do recebimento do Pix. Os recursos podem ficar bloqueados por até 72 horas e, em caso de confirmação da fraude, o valor é devolvido ao pagador. Além disso, foram impostos novos requisitos de segurança para as instituições parceiras, a exemplo das normas listadas a seguir, cujo prazo limite para adequação encerrou-se em 01 de março de 2026 (UOL, 2025).

- Autenticação: Exigência de autenticação multifatorial (MFA) na comunicação de dados.
- Controles Técnicos: Uso de certificados digitais, proteção de rede e instrumentos de rastreabilidade.
- Prevenção: Aumento da frequência e rigor nos testes de intrusão (*pentests*) e controles de acesso.

Desde 02 de fevereiro de 2026, tornou-se obrigatório o rastreamento do fluxo de recursos através de múltiplas camadas de contas, transcendendo a primeira conta receptora. Essa medida viabiliza o bloqueio e a recuperação de valores mesmo em cenários de dispersão rápida para "contas laranjas" (Banco Central do Brasil, 2026a). Tal funcionalidade apresenta-se como uma solução robusta para o principal gargalo identificado nas entrevistas com representantes das instituições parceiras, detalhadas na Seção 3.2.

Após o incidente do dia 29 de agosto de 2025 (G1, 2025), o Banco Central emitiu uma nova restrição: transferências acima de 15 mil reais só serão permitidas a instituições e prestadores de serviços intermediários que cumprirem todos os requisitos de segurança do órgão. Nenhuma companhia de pagamentos poderá operar sem autorização prévia, e o prazo para regularização é até maio de 2026 (Banco Central do Brasil, 2025).

Em setembro de 2023 foi publicada a responsabilidade das instituições financeiras de comunicar a seus usuários que tiveram seus dados vazados em incidentes de Pix (Banco Central do Brasil, 2023). Além disso, existem consequências para as instituições participantes ou em processo de adesão ao Pix que descumprirem seus deveres, o que pode levar

à multa, suspensão ou exclusão (Banco Central do Brasil, 2021a). A suspensão de 30 dias ocorre quando o participante inadimplir no pagamento de multa entre 15 e 30 dias após o prazo estabelecido. Já a suspensão de 60 dias ocorre quando o participante descumpre, total ou parcialmente, disposições do Regulamento do Pix ou dos demais documentos que compõem esse Regulamento de forma a: (a) acarretar grave risco ao funcionamento regular do Pix; (b) gerar lesão relevante aos usuários finais do Pix; (c) contribuir para a criação de um ambiente de indisciplina no Pix.

Uma penalidade de exclusão é imposta à instituição que não corrigir, no prazo de 60 (sessenta) dias, a irregularidade que originou a aplicação da penalidade de suspensão. Descumprir total ou parcialmente disposições do Regulamento do Pix ou dos demais documentos que compõem esse Regulamento, de forma a acarretar grave prejuízo ao regular funcionamento do Pix ou grave lesão aos usuários finais do Pix; ou não pagar multas após o prazo final estabelecido.

Os ataques de engenharia social são os mais predominantes em número para o Pix. Conforme a Seção 3.2, as instituições financeiras priorizam a educação dos usuários como prevenção a esse tipo de ataque. É fato que conscientizar a população mitiga, em parte, os ataques. Mas sabe-se que se torna inviável treinar e/ou educar toda a população brasileira, visto que os ataques de engenharia social estão cada vez mais sofisticados; os atacantes estão sempre um passo à frente, adaptando-se às novas técnicas de segurança. Defende-se que o uso da tecnologia para evitar os ataques deve ser o foco da segurança para mitigar esses ataques.

Os ataques realizados por meio das empresas Sinqia (G1, 2025) e C&M Software (EXAME, 2025) foram os mais expressivos e recentes. Os ataques ocorreram por meio da exploração de credenciais, utilizando desenvolvedores internos dessas empresas para obtê-las. No caso da C&M, os atacantes contataram um desenvolvedor júnior da empresa que, conforme seu próprio relato, disponibilizou seu acesso aos atacantes por R$ 5.000,00 e mais R$ 10.000,00 para continuar executando comandos. Dessa forma, viabilizou-se o acesso indevido dos atacantes, ocasionando o maior ataque digital do Brasil.

Mas deveria um atacante, por meio da máquina de um desenvolvedor júnior, ter conseguido executar esse ataque? Aqui, é muito importante que as empresas, especialmente aquelas relacionadas ao mundo financeiro, tenham processos rigorosos para o permissionamento no nível de acesso de seus funcionários, adotem a política de *zero trust*, utilizem um cofre de senhas para guardar credenciais e monitorem atividades suspeitas, limitando o acesso a aplicações críticas, redes e variáveis de ambiente. No caso da Sinqia, não há nada confirmado. A suspeita, em nota da própria empresa, é a exploração de credenciais legítimas de fornecedores de TI.

O Banco Central realiza melhorias contínuas. Mas, muitas vezes, após uma fraude ocorrer, percebe-se que sempre estamos um passo atrás dos atacantes. Por exemplo, o rastreamento do caminho dos recursos em múltiplas contas (Banco Central do Brasil,

2026a) só foi implementado após os incidentes na *Sinqia* (G1, 2025) e na C&M Software (EXAME, 2025). Mesmo confirmando nas entrevistas que a dependência de agilidade, por parte do cliente, para notificar um golpe e recuperar os valores perdidos já era uma dor das instituições parceiras há muito tempo.

7.3 Dualidade da inteligência artificial

O mapeamento das principais metodologias mostra que, sem nenhuma exceção, todos os ataques podem ser potencializados com técnicas diversas de Inteligência Artificial. Hoje, o acesso a modelos via provedores e serviços na internet é muito fácil e barato. Dessa forma, mesmo o atacante mais leigo consegue potencializar seu ataque de forma rápida e fácil. Por exemplo, usar *deepfake* para gerar uma imagem, vídeo ou áudio falso é extremamente fácil e rápido de ser feito. Com uma pequena entrada da vítima (que é facilmente encontrada nas redes sociais), é possível gerar conteúdo falso extenso e realista.

O mapeamento das técnicas de segurança junto aos métodos de prevenção citados nas entrevistas mostra que a Inteligência Artificial está sendo utilizada cada vez mais para evitar fraudes, muitas vezes em mecanismos específicos de instituições (não obrigatórios). É importante escolher instituições com camadas de segurança robustas e credibilidade na área de segurança, ativando todos os mecanismos disponíveis a fim de evitar golpes.

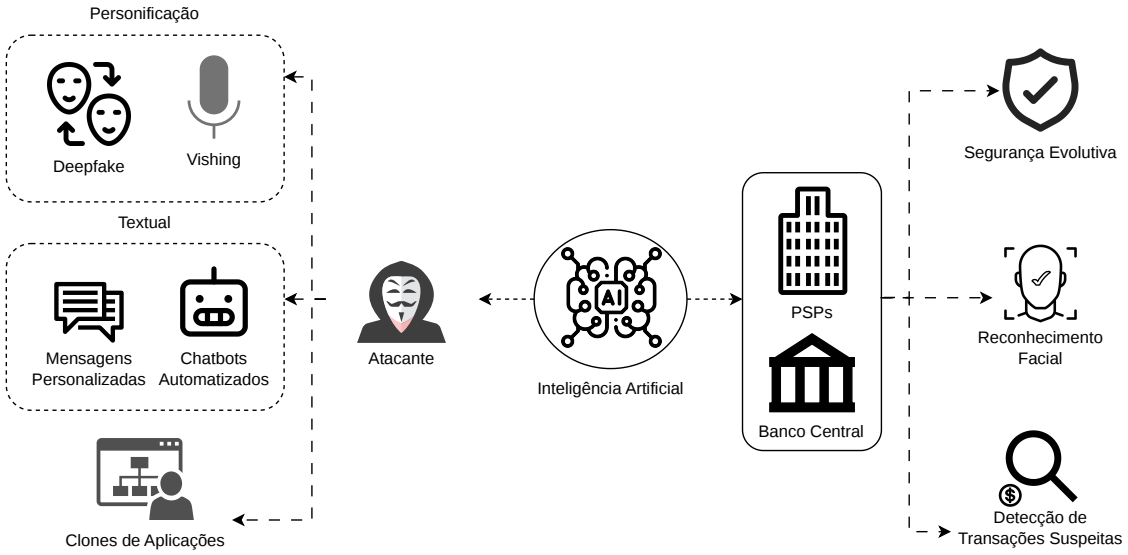
A investigação confirma que a inteligência artificial desempenha hoje um papel dual: amplifica significativamente a capacidade ofensiva dos criminosos, ao mesmo tempo em que fortalece as estratégias defensivas adotadas por instituições financeiras. É possível entender como os modelos batalham entre si. Por exemplo, no *deepfake*, pode-se imaginar um atacante usando modelos específicos para tentar burlar os modelos utilizados no reconhecimento facial das instituições financeiras. Isso gera, de forma indireta, um aprendizado de máquina no contexto de Redes Adversárias Generativas (GANs), onde duas redes neurais, a Geradora e a Discriminadora, competem entre si para melhorar o desempenho. O mesmo se aplica ao *phishing*, onde um atacante pode usar LLM para gerar textos e conversas cada vez mais sofisticados para induzir a vítima a cair no golpe, enquanto softwares de segurança podem usar outros modelos para tentar evitá-los.

7.4 Considerações sobre segurança dos métodos de pagamento do Brasil

Dentro da área de segurança em tecnologia, nenhum sistema é considerado 100% seguro. É fato que cada método de pagamento possui suas vulnerabilidades conhecidas e outras ainda desconhecidas. Diante disso, deve-se perguntar: optar pelo Pix em alguns casos e utilizar outros métodos de pagamento em outros cenários, levando em consideração o valor da transação, os horários e o número de recebedores, etc?

É difícil abrir mão da praticidade do Pix para usar outro método de pagamento mais burocrático e complexo. Ao optar pelo Pix, o usuário não abre mão da segurança

Figura 12 – Dualidade da inteligência artificial



Fonte: Elaboração própria

necessariamente, mas adota um sistema com características próprias que implicam diferentes tipos de riscos e benefícios em comparação com métodos mais tradicionais, como boletos bancários e cartões, ou tecnologias emergentes, como *blockchain*. A escolha do método de pagamento ideal depende do contexto da transação, do seu valor e do nível de confiança entre as partes envolvidas.

O Pix foi concebido com robustas camadas de segurança. As transações são protegidas por criptografia e autenticação, seguindo os padrões do Sistema Financeiro Nacional. A agilidade, no entanto, é sua principal característica e também um ponto de atenção, por mais que todas as transações sejam registradas e vinculadas a um CPF ou CNPJ (o que facilita investigações em casos de fraude). Cada método de pagamento possui suas vantagens e desvantagens.

Os números mostram que o Pix continuará sendo a forma de pagamento mais utilizada e que apresentará crescimento constante em relação aos demais métodos de pagamento, pois é muito rápido e prático de usar. Em suma, não há um método de pagamento universalmente "mais seguro" em todos os cenários. Cada método possui suas particularidades, vantagens e desvantagens, conforme a Tabela 10. A escolha de qual usar deve ser exclusivamente feita pelo usuário, ciente de que esse método pode apresentar brechas de segurança. É necessária uma constante evolução tecnológica nas técnicas de segurança para evitar incidentes com essas tecnologias.

Tabela 10 – Análise de segurança dos métodos de pagamento

Método	Vantagens (proteção)	Desvantagens (riscos)
PIX	• Transações criptografadas; • Rastreabilidade.	• Facilita crimes de coação física; • Alto risco de engenharia social.
TED DOC	• Janela de tempo para bloqueio; • Menor atratividade para crimes presenciais.	• Exposição excessiva de dados pessoais (CPF, Nome, Conta); • Comum em golpes de agendamento.
Boleto	• Preservação de credenciais; • Validação de emissor via DDA.	• Ataques que alteram a linha digitável; • Falsificação visual fácil.
Cartão	• Mecanismo de *Chargeback*; • Uso de cartão virtual em compras online.	• Clonagem física; • Fraudes em compras por aproximação em aglomerações.

Fonte: Elaboração própria

7.5 Trabalhos futuros

Novas metodologias de golpes são criadas diariamente. Continuar este estudo e aumentar a amostragem é essencial para o aperfeiçoamento da taxonomia e da categorização, a fim de facilitar pesquisas futuras.

Uma lacuna importante a ser preenchida é a transição de um estudo qualitativo para uma análise quantitativa. Propõe-se o mapeamento da frequência de cada metodologia de ataque para identificar quais tipologias apresentam maior volume e maior prejuízo financeiro. Através da integração de dados quantitativos, é possível correlacionar as metodologias de fraude com perfis demográficos específicos (idade, gênero e grau de literacia tecnológica). Investigar quais gatilhos de motivação, como Confiança, Medo ou Empatia são mais eficazes contra cada perfil de vítima permitiria o desenvolvimento de campanhas de conscientização personalizadas e mais assertivas.

Adicionalmente, observa-se a oportunidade de evoluir a taxonomia proposta para um nível maior de granularidade, migrando de uma categorização multi-label para uma categorização mais específica, idealmente com a atribuição de um único rótulo por pilar. No entanto, essa transição exige um refinamento prévio na definição das tipologias de golpes e não realizar o processo de deduplicação, uma vez que muitas delas apresentam variações significativas em sua execução. Por exemplo, o golpe do "falso funcionário de banco" pode se desdobrar em diferentes vetores de ataque, como o roubo de credenciais ou a indução à instalação de malware. Dessa forma, torna-se necessário decompor essas categorias amplas em subtipos mais bem definidos, permitindo uma categorização mais precisa e consistente, além de favorecer análises comparativas e automatizações futuras.

Destaca-se o potencial de generalização da taxonomia proposta para além do contexto específico do Pix, ampliando sua aplicabilidade para o domínio mais amplo de frau-

des e ataques digitais. Nesse sentido, o Pix pode ser compreendido como uma instância particular dentro de uma estrutura taxonômica mais abrangente, na qual os ataques são organizados a partir dos pilares propostos, passíveis de evolução ou extensão para novos eixos analíticos. Essa abordagem permite a reutilização do modelo em diferentes contextos, como fraudes envolvendo cartões, boletos e outros meios de pagamento, promovendo maior padronização analítica e facilitando a comparação entre diferentes modalidades de ataque. Além disso, uma taxonomia mais macro contribui para a identificação de padrões transversais, apoiando tanto a formulação de estratégias de mitigação mais robustas quanto o desenvolvimento de soluções automatizadas de detecção e resposta.

Para ampliar a escalabilidade do processo da pipeline de anonimização de dados sensíveis e mitigar a dependência de intervenção humana, é fundamental superar a limitação imposta pela criação manual de *templates* de coordenadas. Sugere-se o desenvolvimento ou a integração de modelos de visão computacional já validados e consolidados na literatura, que sejam capazes de identificar e localizar campos de PII de forma dinâmica. Tal evolução permitiria a automação integral da pipeline, dispensando a exigência de um repositório fixo de coordenadas para cada variação de layout das instituições financeiras, otimizando significativamente o processamento de grandes volumes de amostras heterogêneas e agilizando a expansão do *dataset*.

Outra frente relevante envolve a geração de dados sintéticos, com o objetivo de ampliar a diversidade e o volume das amostras disponíveis para treinamento de modelos de inteligência artificial. Técnicas de geração sintética, como *data augmentation* e modelos generativos, podem ser utilizadas para criar variações controladas de comprovantes, preservando características estatísticas relevantes sem expor dados sensíveis reais. Essa abordagem não apenas contribui para mitigar limitações relacionadas à privacidade e à escassez de dados, como também permite simular cenários de ataque ainda não observados, fortalecendo a capacidade preditiva dos sistemas desenvolvidos.

Modelos de inteligência artificial precisam de dados para seu treinamento, aperfeiçoar o *dataset* proposto e gerar novos conjuntos de dados confiáveis e de boa qualidade é essencial para criar mecanismos de segurança cada vez mais robustos.

O *dataset* de comprovantes de pagamentos reais apresenta potencial de utilização em cenários tanto defensivos quanto ofensivos, característica inerente a bases de dados realistas e ricas em contexto. Do ponto de vista defensivo, pode ser empregado no treinamento de modelos de detecção de fraudes documentais, permitindo identificar inconsistências estruturais, padrões atípicos e indícios de adulteração em comprovantes utilizados em golpes. Em contrapartida, sob a ótica ofensiva, o mesmo conjunto de dados pode subsidiar a geração de comprovantes falsos mais verossímeis, evidenciando a necessidade de controles rigorosos de acesso e uso responsável, bem como a adoção de técnicas de mitigação de riscos associadas ao seu compartilhamento.

Nesse contexto, uma aplicação promissora do *dataset* reside na área de análise fo-

rense digital, especialmente na validação de autenticidade de documentos financeiros. A partir das amostras coletadas, é possível extrair características visuais, textuais e estruturais que sirvam como base para algoritmos capazes de distinguir documentos legítimos de versões manipuladas. Elementos como tipografia, alinhamento, metadados implícitos e padrões de formatação podem ser explorados como indicadores de integridade, contribuindo para o desenvolvimento de ferramentas automatizadas de apoio à investigação de fraudes.

Considerando o avanço das *deepfakes* aplicadas a golpes financeiros, pesquisas futuras podem explorar técnicas de detecção automática de conteúdo sintético (texto, áudio e vídeo) gerados pela IA.

Sugere-se também investigar o impacto de políticas públicas e regulamentações específicas que possam reduzir a superfície de ataque em cenários de engenharia social e interação física, incluindo protocolos unificados de bloqueio de emergência no sistema financeiro.

Ressalta-se que a amplitude do escopo abordado neste trabalho ao explorar múltiplas dimensões do problema, desde a taxonomia de ataques até a construção do *dataset*, abriu diversas frentes de investigação e evolução. Essa abordagem mais abrangente não apenas evidencia a complexidade do tema, como também estabelece uma base inicial sólida e flexível, capaz de orientar pesquisas futuras em diferentes direções.

Por fim, este trabalho foi concebido com a preocupação de manter uma linguagem acessível e didática, permitindo sua compreensão por públicos além do meio acadêmico. Nesse sentido, abre-se a possibilidade de sua adaptação para iniciativas de educação e conscientização, como *workshops*, palestras e materiais educativos direcionados a diferentes perfis, incluindo crianças, adultos e idosos. A transformação do conteúdo em formatos mais interativos e práticos pode ampliar significativamente seu impacto social, contribuindo para a disseminação de conhecimento e para a prevenção de fraudes no cotidiano da população.

REFERÊNCIAS

Banco Central do Brasil. **Resolução BCB n° 177 de 22 de dezembro de 2021**. 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=177>. Citado na página 67.

Banco Central do Brasil. **Resolução BCB nº 147, de 28 de setembro de 2021**. 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=resolu%C3%A7%C3%A3o%20bcb&numero=147>. Acesso em: 7 mar. 2026. Citado na página 66.

Banco Central do Brasil. **Resolução BCB no. 342 de 26 de setembro de 2023**. 2023. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=resoluÃğÃčo%20bcb&numero=342>. Citado na página 66.

Banco Central do Brasil. **BC aprova medidas para reforçar a segurança do Sistema Financeiro Nacional**. 2025. Acessado em: 17 de setembro de 2025. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20827/nota>. Citado na página 66.

Banco Central do Brasil. **BC aprimora o Mecanismo Especial de Devolução do Pix**. 2026. Acessado em: 19 de janeiro de 2026. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20817/nota>. Citado 2 vezes nas páginas 66 e 68.

Banco Central do Brasil. **Lista de participantes ativos do Pix. Publicado em 03 de março de 2026**. 2026. Acessado em: 07 de março de 2026. Disponível em: <https://www.bcb.gov.br/content/estabilidadefinanceira/participantes_pix_pdf/lista-participantes-instituicoes-em-adesao-pix-20260303.pdf>. Citado na página 21.

Banco Central do Brasil. **Pix em números**. 2026. [Online; acessado em 26 de fevereiro de 2026.]. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix-em-numeros-estatisticas>. Citado 2 vezes nas páginas 17 e 21.

Banco Central do Brasil. **Registro de incidentes com dados pessoais**. 2026. [Online; acessado em 23 de janeiro de 2026.]. Disponível em: <https://www.bcb.gov.br/acessoinformacao/lgpd?modalAberto=registro_de_incidentes_com_dados_pessoais>. Citado 2 vezes nas páginas 22 e 43.

Banco Central do Brasil. **Site do Banco Central do Brasil**. 2026. Acessado em: 16 de fevereiro de 2026. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix>. Citado 2 vezes nas páginas 21 e 27.

BELLI, L. et al. A consumer-centric approach for Inclusion in Digital Public Infrastructures. **Global Solutions Journal Issue 10**, 2024. Citado na página 34.

BRASIL, B. N. **Vítima de 'sequestro do Pix' relata cárcere de 8h na mata: 'R$ 160 mil em saques e empréstimos'**. 2022. Disponível em: <https://www.bbc.com/portuguese/brasil-62045088>. Citado na página 44.

BRASIL, S. **Golpe do Pix: veja quais são e saiba como se proteger**. 2024. Disponível em: <https://www.spcbrasil.org.br/blog/golpe-do-pix>. Citado na página 44.

BUENO, L. **PIX banking transaction**. [S.l.]: Kaggle, 2025. Https://www.kaggle.com/datasets/juniorbueno/pix-banking-transaction/code. Acessado em 10 de fevereiro de 2026. Citado na página 53.

CBN. **Extorsão usando o PIX fez o número de sequestros-relâmpagos disparar 40% em SP**. 2021. Acessado em: 30 de janeiro de 2026. Disponível em: <https://cbn.globoradio.globo.com/media/audio/351182/extorsao-usando-o-pix-fez-o-numero-de-sequestros-r.htm>. Citado na página 23.

COSTA, K. da et al. Central bank digital currencies: a high-level overview. **Available at SSRN 4271644**, 2022. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4271644>. Citado na página 34.

DEEPSEEK. **DeepSeek Chat: AI Language Model**. [S.l.]: DeepSeek, 2026. <https://www.deepseek.com>. Acessado em: 17 de fevereiro de 2026. Citado na página 47.

DELLABARBA, P. L. B. **Tecnologia de pagamento instantâneo: pix e criminalidade patrimonial: uma análise econométrica**. 113 f., il. p. Dissertação (Dissertação (Mestrado Profissional em Economia)) — Universidade de Brasília, Brasília, 2023. Disponível em: <https://repositorio.unb.br/handle/10482/49899>. Citado na página 34.

DINHEIRO, S. **Novo golpe do Pix: bandidos abusam de mecanismo que serve para prevenir fraudes; veja como se proteger**. 2024. https://www.seudinheiro.com/2024/financas-pessoais/novo-golpe-do-pix-bandidos-abusam-de-mecanismo-que-serve-para-prevenir-fraudes-veja-como-se-proteger-jesc/. Citado na página 44.

D'OLIVEIRA, I. C.; FERNANDES, P. H. D. Negação plausível em sequestros relâmpagos: implementação do modo pânico em aplicativos bancários. 2024. Citado na página 36.

EXAME. **Dinheiro que some em segundos: o roubo de R$ 1 bilhão e as lições para o futuro da cibersegurança**. 2025. Disponível em: <https://exame.com/tecnologia/dinheiro-que-some-em-segundos-o-roubo-de-r-1-bilhao-e-as-licoes-para-o-futuro-da-ciberseguranca/>. Citado 3 vezes nas páginas 23, 67 e 68.

FCDL/SC. **Conheça os golpes com Pix e saiba como evitá-los**. 2023. Disponível em: <https://www.fcdl-sc.org.br/fcdl-blog/conheca-os-golpes-com-pix-e-saiba-como-evita-los/>. Citado na página 44.

G1. **Em novo golpe do Pix, criminosos invadem contas em rede social e simulam vendas com mega descontos; saiba como se proteger**. 2022. https://g1.globo.com/sp/vale-do-paraiba-regiao/noticia/2022/03/15/em-novo-golpe-do-pix-criminosos-invadem-contas-em-rede-social-e-simulam-vendas-com-mega-descontos-saiba-como-se-proteger.ghtml. Citado na página 44.

G1. **Ataque hacker desviou R$ 710 milhões, diz empresa que opera sistema PIX**. 2025. Acessado em: 08 de setembro de 2025. Disponível em: <https://g1.globo.com/economia/noticia/2025/09/02/ataque-hacker-sinqia.ghtml>. Citado 4 vezes nas páginas 23, 66, 67 e 68.

GLOBO. **Pix cresce, circulação de notas cai: e o que vem depois? Veja qual o futuro do dinheiro**. 2024. [Online; acessado em 23 de janeiro de 2026.]. Disponível em: <https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2024/06/03/pix-cresce-circulacao-de-notas-cai-e-o-que-vem-depois-veja-qual-o-futuro-do-dinheiro.ghtml>. Citado na página 22.

GOOGLE. **Termos de Serviço Adicionais da API Gemini**. 2025. Disponível em: <https://ai.google.dev/gemini-api/terms?hl=pt-br#paid-services>. Citado na página 60.

GOOGLE. **Gemini - Large Language Model**. 2026. <https://gemini.google.com>. Citado 8 vezes nas páginas 34, 38, 41, 43, 45, 47, 54 e 55.

GOOGLE. **Google Dataset Search**. 2026. Acessado em 03 de março de 2026. Disponível em: <https://datasetsearch.research.google.com/>. Citado na página 53.

GOV-BR. **Pix se consolida como meio de pagamento mais usado pelos brasileiros**. 2022. [Online; acessado em 22 de janeiro de 2026. https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/11/pix-se-consolida-como-meio-de-pagamento-mais-usado-pelos-brasileiros]. Disponível em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/11/pix-se-consolida-como-meio-de-pagamento-mais-usado-pelos-brasileiros>. Citado na página 21.

KAGGLE. Kaggle, 2026. Acessado em 03 de março de 2026. Disponível em: <https://www.kaggle.com/>. Citado na página 53.

MAX, M. **Pix: Conheça os golpes mais frequentes e como evitar fraudes na transferência de dinheiro**. 2021. Disponível em: <https://midiamax.uol.com.br/cotidiano/economia/2021/pix-conheca-os-golpes-mais-frequentes-e-como-evitar-fraudes-na-transferencia-de-dinheiro/>. Citado na página 44.

MENDES, M. L. I. B. E. A responsabilidade civil das instituições bancárias diante do cenário de fraudes digitais envolvendo vítimas idosas por meio do Sistema de Pagamentos Instantâneos (PIX) no Brasil. **Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro**, 2023. Disponível em: <https://pantheon.ufrj.br/handle/11422/25307>. Citado na página 34.

NETO, A. A. C. **Post-Quantum Cryptography methods applied to the Brazilian instant payment system (Pix): A feasibility study**. 2022. Disponível em: <https://cryptoid.com.br/wp-content/uploads/2022/04/quantum-cryptography-pix-en.pdf>. Citado na página 34.

NU. **Nubank lança "Modo Rua", função inovadora de segurança que limita transações no app ao sair de casa**. 2022. https://international.nubank.com.br/pt-br/consumidores/nubank-lanca-modo-rua-funcao-inovadora-de-seguranca-que-limita-transacoes-no-app-ao-sair-de-casa/. Citado na página 39.

NU. **Golpe da mão fantasma: o que é e como se proteger do acesso remoto?** 2024. Disponível em: <https://blog.nubank.com.br/golpe-mao-fantasma-acesso-remoto/>. Citado na página 44.

NU. **Três Maneiras: como o Nubank usa IA para deixar seus clientes mais tranquilos**. 2024. Acessado em: 3 de fevereiro de 2026. Disponível em: <https://www.youtube.com/watch?v=-vNDEXhtby8>. Citado na página 39.

OLLAMA. **Start building with open models**. 2026. Acessado em 03 de março de 2026. Disponível em: <https://ollama.com/>. Citado na página 31.

OPENAI. **ChatGPT: Modelo de Linguagem da OpenAI**. 2026. Acessado em: 17 de fevereiro de 2026. Disponível em: <https://openai.com/chatgpt>. Citado 6 vezes nas páginas 34, 38, 41, 43, 45 e 47.

PERNAMBUCO, D. de. **O avanço do Pix e o tempo de vida do papel moeda**. 2024. [Online; acessado em 23 de janeiro de 2026.]. Disponível em: <https://www.diariodepernambuco.com.br/noticia/economia/2024/07/o-avanco-do-pix-e-o-tempo-de-vida-do-papel-moeda.html>. Citado na página 22.

PIZZOLATO, G. **Taxonomia de fraudes no Pix**. Kaggle, 2025. Acessado em 17 de março de 2026. Disponível em: <https://www.kaggle.com/datasets/glenerpizzolato/classificaotaxonomia-de-golpes-no-pix/data>. Citado 2 vezes nas páginas 51 e 65.

PIZZOLATO, G. **GitHub: job-llm-PII-anonymization-by-templates**. GitHub, 2026. Acessado em 07 de março de 2026. Disponível em: <https://github.com/glener10/job-llm-PII-anonymization-by-templates>. Citado na página 54.

PIZZOLATO, G. et al. Mapeamento e Análise de Metodologias de Fraude Aplicadas ao Pix no Brasil. In: **Anais da XXII Escola Regional de Redes de Computadores**. Porto Alegre, RS, Brasil: SBC, 2025. p. 172–178. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/errc/article/view/39199>. Citado na página 65.

PRIDEMORE, W. A.; ROCHE, S. P.; ROGERS, M. L. Cashlessness and street crime: A cross-national study of direct deposit payment and robbery rates. ***Justice Quarterly***, Taylor & Francis, v. 35, n. 5, p. 919–939, 2018. Citado na página 22.

RIBEIRO, A. S. **A responsabilidade das instituições financeiras nas fraudes em transações via Pix**. Dissertação (Mestrado) — Universidade Federal de Uberlândia, 2023. Disponível em: <https://repositorio.ufu.br/handle/123456789/40959>. Citado na página 34.

RUDDER, D. **Como funcionam as táticas de engenharia social no Pix?** 2023. Disponível em: <https://datarudder.com/como-funcionam-as-taticas-de-engenharia-social-no-pix/>. Citado na página 44.

SERASA. **Golpes do Pix: como se proteger?** 2024. Disponível em: <https://www.serasa.com.br/premium/blog/golpes-do-pix-como-se-proteger/>. Citado na página 44.

SINDICONET. **Criminoso invade prédio e obriga morador a fazer Pix em SP**. 2025. Disponível em: <https://www.sindiconet.com.br/informese/criminoso-invade-predio-obriga-morador-fazer-pix-sp-noticias-seguranca>. Citado na página 44.

STONE. **Como se prevenir contra o golpe do falso leilão?** 2024. Disponível em: <https://blog.stone.com.br/como-se-prevenir-contra-o-golpe-do-falso-leilao/>. Citado na página 44.

STONE. **Golpe do WhatsApp clonado: veja como funciona e o que fazer**. 2024. Disponível em: <https://blog.stone.com.br/golpe-do-whatsapp-clonado/>. Citado na página 44.

TECH, F. **Brasil tem alta de 200% nos ataques de engenharia social em 2020**. 2021. [Online; acessado em 23 de janeiro de 2026.]. Disponível em: <https://febrabantech.febraban.org.br/temas/seguranca/brasil-tem-alta-de-200-nos-ataques-de-engenharia-social-em-2020>. Citado na página 23.

TEMPO, O. **Golpe da Madonna finge que ela foi assaltada e pede Pix: 'Hello, friend'**. 2024. Disponível em: <https://www.otempo.com.br/brasil/golpe-da-madonna-finge-que-ela-foi-assaltada-e-pede-pix-hello-friend-1.3524426>. Citado na página 44.

UFRJ. **Pix: 6 golpes mais frequentes**. 2021. Disponível em: <https://seguranca.tic.ufrj.br/noticias/pix-6-golpes/>. Citado 2 vezes nas páginas 43 e 44.

UOL. **BC reforça regras de segurança cibernética para proteger Pix contra hackers**. 2025. Acessado em: 19 de janeiro de 2026. Disponível em: <https://economia.uol.com.br/noticias/redacao/2025/12/19/para-proteger-pix-de-hackers-bc-reforca-regras-de-seguranca-cibernetica.htm?cmpid=copiaecola>. Citado na página 66.

VALLE, G. H. del et al. CEMLA's survey on central bank digital currencies in Latin America and the Caribbean. **Latin American Journal of Central Banking**, Elsevier, v. 5, n. 4, p. 100135, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2666143824000176>. Citado na página 34.

VIEIRA, C. **Brazilian Payment Methods**. [S.l.]: Kaggle, 2024. Https://www.kaggle.com/datasets/clovisdalmolinvieira/brazilian-payment-methods. Acessado em 22 de março de 2026. Citado na página 53.

ANEXO A – QUESTIONÁRIO ENTREVISTAS

Figura 13 – Questionário entrevistas com representantes do Banco do Brasil, Sicredi e Banrisul - parte 1

Introdução ao questionário

"Olá, agradecemos por participar deste questionário. Ele faz parte de uma pesquisa acadêmica que investiga fraudes no Pix e as medidas de segurança adotadas pelas instituições financeiras. Suas respostas serão utilizadas exclusivamente para fins acadêmicos e tratadas de forma anônima. O preenchimento leva cerca de 5 a 7 minutos."

Seção 1: Informações gerais

1. Qual é o seu papel no setor financeiro ou em relação ao uso do Pix?
   - ( ) Funcionário de banco
   - ( ) Consultor de segurança
   - ( ) Cliente ou usuário do Pix
   - ( ) Outro (especificar): _____

2. Qual é o nível de familiaridade com o funcionamento do Pix?
   - ( ) Nenhuma
   - ( ) Baixa
   - ( ) Média
   - ( ) Alta

Seção 2: Tipos de fraudes no Pix

3. Quais tipos de fraudes no Pix você já presenciou ou conhece? *(Marque todas as opções que se aplicam)*
   - ( ) Golpes de phishing (falsos links ou mensagens fraudulentas)
   - ( ) Engenharia social (manipulação para obter dados pessoais)
   - ( ) Clonagem de WhatsApp
   - ( ) Uso de contas falsas ou laranjas
   - ( ) Outros (especificar): _____

4. Com que frequência você acredita que ocorrem fraudes no Pix no Brasil?
   - ( ) Raramente
   - ( ) Ocasionalmente
   - ( ) Frequentemente
   - ( ) Muito frequentemente

Figura 14 – Questionário entrevistas com representantes do Banco do Brasil, Sicredi e Banrisul - parte 2

5. Na sua opinião, quais grupos são mais afetados por fraudes no Pix? *(Marque todas que se aplicam)*
    - ( ) Idosos
    - ( ) Pequenos empresários
    - ( ) Pessoas com baixa familiaridade tecnológica
    - ( ) Todos os grupos igualmente

Seção 3: Medidas de segurança

6. Quais medidas de segurança você conhece que são utilizadas para prevenir fraudes no Pix? *(Marque todas que se aplicam)*
    - ( ) Autenticação em duas etapas (2FA)
    - ( ) Monitoramento de transações suspeitas
    - ( ) Bloqueio de contas suspeitas
    - ( ) Uso de inteligência artificial para análise de comportamento
    - ( ) Outros (especificar): _____

7. Na sua percepção, essas medidas de segurança são eficazes?
    - ( ) Sim, totalmente eficazes
    - ( ) Parcialmente eficazes
    - ( ) Pouco eficazes
    - ( ) Ineficazes

8. Quais melhorias você acredita que poderiam ser implementadas para aumentar a segurança no Pix?
    - Resposta aberta: _____

Seção 4: Uso de inteligência artificial (IA)

9. Você acredita que a IA desempenha um papel importante na prevenção de fraudes no Pix?
    - ( ) Sim
    - ( ) Não
    - ( ) Não sei

Figura 15 – Questionário entrevistas com representantes do Banco do Brasil, Sicredi e Banrisul - parte 3

10. Quais aplicações de IA você conhece ou acredita que poderiam ser úteis no combate às fraudes no Pix?
- Resposta aberta: _____

Seção 5: Desafios e perspectivas

11. Quais são os maiores desafios que você enxerga no combate às fraudes no Pix?

Resposta aberta: _____

- Em sua opinião, o que poderia ser feito para conscientizar mais os usuários sobre as fraudes no Pix?

Resposta aberta: _____

- Você gostaria de adicionar algum comentário ou sugestão sobre segurança no Pix?

Resposta aberta: _____

ANEXO B – FORMULÁRIO DE COLETA DOS COMPROVANTES

Figura 16 – Formulário coleta dos comprovantes de pagamento - parte 1

Envie um comprovante Pix e concorra a R$ 100 💰

Olá, pessoal!

Estou realizando uma pesquisa na disciplina Laboratório de Inteligência Artificial Aplicada no Programa de Pós-Graduação em Engenharia de Software da Universidade Federal do Pampa (UNIPAMPA).

Objetivo é coletar comprovantes de pagamentos Pix para treinar modelos de inteligência artificial a identificar formatos/templates de diversas instituições. Com isso podemos:

- Treinar modelos de Inteligência Artificial para identificar comprovantes falsos.

- Permite a pesquisadores estudar as táticas, ferramentas e padrões utilizados por fraudadores, ajudando a antecipar novas ameaças.

* Indicates required question

1. Email *

Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) 🔑
Este estudo segue rigorosamente a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Todos os dados coletados serão utilizados exclusivamente para fins acadêmicos e de pesquisa.

Informações pessoais ou sensíveis (como CPF, nome, número de conta, identificador da transação, etc.), serão anonimizados por dados sintéticos e todos arquivos serão removidos após o processamento.

Quem terá acesso: Os dados ficarão sob responsabilidade exclusiva do autor da pesquisa, com acesso restrito somente a ele.
Como serão armazenados: Os arquivos serão armazenados de forma segura no Google Drive vinculado ao e-mail institucional glenerpizzolato.aluno@unipampa.edu.br
Por quanto tempo serão guardados: Os dados serão mantidos apenas durante o período da pesquisa, sendo apagados após o término da coleta e análise, previsto para 08/12/2025.

Atenção! O participante pode solicitar a exclusão de seus dados a qualquer momento entrando em contato com o email glenerpizzolato.aluno@unipampa.edu.br

Figura 17 – Formulário coleta dos comprovantes de pagamento - parte 2

2. **TCLE (Termo de Consentimento Livre e Esclarecido)** *

Check all that apply.

☐ Aceito compartilhar meus comprovantes de pagamento Pix para fins de pesquisa e estou ciente que os dados serão anonimizados e excluídos após o processamento.

Envio dos Comprovantes de Pagamento Pix

Quanto mais instituições bancárias e amostras alcançarmos na pesquisa, mais abrangente e relevante será o trabalho.

Cada comprovante enviado contará como uma entrada no sorteio, então quanto mais comprovantes enviar, maiores as chances de ganhar!

Formas de Participar

1. **Envio de comprovante de qualquer destinatário**: Evite compartilhar dados de terceiros.
   Fique a vontade para adicionar elementos visuais para anonimizar ou ocultar os dados sensíveis antes do envio.
   Reforçamos o nosso comprometimente com os dados sensíveis utilizados na pesquisa.
2. **Envie o comprovante realizado a partir de um Pix de R$ 0,01 para a chave 55996981032**: Essa chave é do autor, nesse cenário não precisamos se preocupar com os dados de terceiros.

3. Anexar Comprovantes *

Files submitted:

Sorteio

Muito obrigado pela colaboração!

O sorteio será realizado no dia 09/12/2025 e transmitido via Google Meet, horário será compartilhado no linkedin www.linkedin.com/in/glenerpizzolato.

Sua contribuição ajuda diretamente no avanço da pesquisa em inteligência artificial aplicada à segurança digital.