

UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB  
Centro de Ciências Sociais Aplicadas – CCSA  
Graduação em Administração – GADM

**IMPACTOS DAS FRAUDES BANCÁRIAS NA  
RELAÇÃO CLIENTE-BANCO: Percepção sobre a  
confiança, continuidade, segurança e recomendação**

MAYRA MARINHO DA SILVA

João Pessoa  
Setembro 2025

MAYRA MARINHO DA SILVA

**IMPACTOS DAS FRAUDES BANCÁRIAS NA  
RELAÇÃO CLIENTE-BANCO: Percepção sobre a  
confiança, continuidade, segurança e recomendação**

Trabalho de Curso apresentado como parte dos requisitos necessários à obtenção do título de Bacharel em Administração, pelo Centro de Ciências Sociais Aplicadas, da Universidade Federal da Paraíba / UFPB.

**Professora Orientadora:** Dra. Diana Lúcia Teixeira de Carvalho

João Pessoa  
Setembro 2025

**Catálogo na publicação**  
**Seção de Catalogação e Classificação**

S586i Silva, Mayra Marinho da.

Impactos das fraudes bancárias na relação  
cliente-banco: percepção sobre a confiança,  
continuidade, segurança e recomendação / Mayra Marinho  
da Silva. - João Pessoa, 2025.  
41 f. : il.

Orientação: Diana Lucia Teixeira de Carvalho.  
TCC (Graduação) - UFPB/CCSA.

1. Fraudes bancárias. 2. Instituições financeiras.  
3. Experiência do cliente. I. Carvalho, Diana Lucia  
Teixeira de. II. Título.

UFPB/CCSA

CDU 005(043)

## Folha de aprovação

Trabalho apresentado à banca examinadora como requisito parcial para a Conclusão de Curso do Bacharelado em Administração.

**Aluno(a):** Mayra Marinho da Silva

**Trabalho:** IMPACTOS DAS FRAUDES BANCÁRIAS NA RELAÇÃO CLIENTE-BANCO: Percepção sobre a confiança, continuidade, segurança e recomendação

**Área da pesquisa:** Marketing

**Data de aprovação:**

23/09/2025

### Banca Examinadora



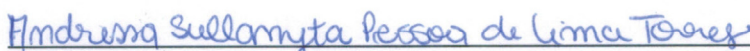
---

Prof<sup>ª</sup>. Dra. Diana Lucia Teixeira de Carvalho  
Orientadora



---

Prof<sup>ª</sup>. Dra. Fabiana Gama de Medeiros  
Avaliadora 1



---

Prof<sup>ª</sup>. Ma. Andressa Sullamyta Pessoa de Lima Torres  
Avaliadora 2

## **DEDICATÓRIA**

Dedico este trabalho aos meus queridos pais e a minha irmã mais velha, por todo o esforço, dedicação e apoio em todos os momentos de minha vida.

## **AGRADECIMENTOS**

Quero expressar minha gratidão à Deus, por ter me permitido chegar até aqui e finalizar mais um ciclo de estudos com honra e virtude;

A minha família, por sempre terem me incentivado a estudar e buscar aprimorar o meu conhecimento e habilidades pessoais em todas as fases da minha vida;

A minha orientadora, a professora Dra. Diana Lucia Teixeira de Carvalho, que acreditou no potencial do projeto desde o nosso primeiro encontro, apontando os direcionamentos necessários para que a pesquisa avançasse até o fim, além de demonstrar paciência e apoio a todos os meus questionamentos e dúvidas ao longo das etapas deste trabalho;

Aos meus amigos, que me acompanharam desde o início e no decorrer desta trajetória no curso de Administração, por me apoiarem e tornarem os momentos difíceis em boas lembranças que guardarei para sempre em minha memória;

Quero agradecer à Universidade Federal da Paraíba - UFPB e a todos os professores do Departamento de Administração que demonstraram comprometimento com a qualidade e excelência do ensino;

Agradeço a todas as pessoas que de alguma forma me ajudaram a concluir este trabalho, pelos ensinamentos valiosos adquiridos ao longo do processo de pesquisa e espero que os resultados deste trabalho possam contribuir para a comunidade acadêmica e para a sociedade como um todo.

## RESUMO

Nos últimos anos, o aumento das fraudes bancárias no Brasil tem afetado significativamente a relação entre clientes e instituições bancárias. Este estudo investigou o impacto dessas fraudes sobre aspectos de segurança e confiança no banco, assim como na intenção de continuidade do vínculo e na recomendação dos usuários. Adotou-se uma abordagem quantitativa, com aplicação de um questionário estruturado com consumidores de bancos maiores de 18 anos, com ou sem histórico de fraude, e foram realizadas perguntas baseadas nas principais fraudes bancárias no Brasil. Os resultados demonstraram que a percepção de segurança influencia fortemente a confiança na instituição, enquanto a confiança afeta moderadamente a disposição de recomendar o banco e a intenção de manter o relacionamento. Com relação às variáveis, locus de controle e motivação para se proteger, foi revelado que os clientes reconhecem a sua própria responsabilidade na segurança. Entretanto, é importante que os bancos evidenciem as suas iniciativas antifraudes por meio de estratégias de comunicação de marketing para aumentar o nível de confiança na instituição. Com isso, aumentam a intenção dos consumidores em relação à continuidade do vínculo e recomendação para terceiros, mesmo em um contexto de fraude. O estudo contribui teoricamente para a discussão sobre os impactos das fraudes financeiras e, na prática, oferece subsídios para estratégias futuras de proteção e relacionamento bancário. As limitações do estudo incluem a baixa participação de idosos e a concentração geográfica da amostra.

**Palavras-chave:** Fraudes Bancárias, Instituições Financeiras e Experiência do Cliente.

## **LISTA DE FIGURAS**

|                                                                |    |
|----------------------------------------------------------------|----|
| Figura 1 – Modelo conceitual do estudo.....                    | 16 |
| Figura 2 – Resultado da Modelagem de Equações Estruturais..... | 23 |

## **LISTA DE TABELAS**

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Tabela 1 – Análise psicométrica.....                            | 18 |
| Tabela 2 – Medidas descritivas.....                             | 19 |
| Tabela 3 – Medidas de correlação.....                           | 20 |
| Tabela 4 – Resultados da Modelagem de Equações Estruturais..... | 21 |



## SUMÁRIO

|          |                                                                                  |           |
|----------|----------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>INTRODUÇÃO</b>                                                                | <b>8</b>  |
| <b>2</b> | <b>REVISÃO DA LITERATURA</b>                                                     | <b>9</b>  |
| 2.1      | Principais Tipos de Fraudes Bancárias no Brasil                                  | 9         |
| 2.2      | Percepção de Segurança em Serviços Bancários                                     | 11        |
| 2.3      | Confiança nas Instituições Financeiras                                           | 12        |
| 2.4      | Continuidade da Relação com a Instituição Bancária                               | 13        |
| 2.5      | Recomendação dos Serviços Bancários                                              | 13        |
| 2.6      | Hipóteses e Desenho do Modelo de Pesquisa                                        | 14        |
| <b>3</b> | <b>PROCEDIMENTOS METODOLÓGICOS</b>                                               | <b>16</b> |
| <b>4</b> | <b>RESULTADOS</b>                                                                | <b>17</b> |
| 4.1      | Descrição da Amostra                                                             | 17        |
| 4.2      | Análise psicométrica                                                             | 18        |
| 4.3      | Análise das medidas descritivas                                                  | 19        |
| 4.4      | Análise de associação                                                            | 20        |
| 4.5      | Análise das hipóteses                                                            | 21        |
| <b>5</b> | <b>DISCUSSÃO DOS RESULTADOS</b>                                                  | <b>23</b> |
| <b>6</b> | <b>CONSIDERAÇÕES FINAIS</b>                                                      | <b>24</b> |
|          | <b>REFERÊNCIAS</b>                                                               | <b>26</b> |
|          | <b>APÊNDICE A – Quadro dos construtos utilizados, itens e respectivas fontes</b> | <b>32</b> |
|          | <b>APÊNDICE B – Termo de Consentimento Livre e Esclarecido</b>                   | <b>34</b> |
|          | <b>APÊNDICE C – Instrumento de coleta de dados</b>                               | <b>35</b> |
|          | <b>APÊNDICE D – Itens finais das escalas e medidas descritivas</b>               | <b>39</b> |
|          | <b>APÊNDICE E – Convites para participação da pesquisa</b>                       | <b>41</b> |

## 1 INTRODUÇÃO

Nos últimos anos, as instituições financeiras passaram por um intenso processo de digitalização, impulsionado principalmente pela pandemia da Covid-19. A necessidade de isolamento social e a migração acelerada de serviços para o ambiente online favoreceram o fortalecimento dos bancos digitais no mercado brasileiro, que se destacaram pela isenção de tarifas em seus serviços e pela ausência de agências físicas. Ademais, a ampliação do portfólio de serviços representou outro diferencial competitivo dos bancos digitais, na tentativa de aumentar a base de clientes e alcançar, inclusive, o público idoso, ao se posicionarem como uma melhor alternativa frente aos bancos tradicionais (Gerbelli, 2021).

Nesse cenário, os serviços bancários digitais se tornaram amplamente acessíveis à população brasileira, visto que as pessoas de baixa renda anteriormente sofriam discriminação por parte dos sistemas bancários tradicionais, devido à burocracia envolvida na criação de contas e na realização de depósitos. Contudo, a chegada das *fintechs* permitiu que essa parcela da sociedade passasse a ter o acesso facilitado à abertura de contas, transferências, pagamentos e compras online (Gandra, 2022).

Como resultado, iniciou-se uma competitividade no setor bancário que fez com que os bancos tradicionais também adaptassem os seus sistemas digitalmente. Diante disso, houve um crescimento no uso de canais digitais, como o *Internet Banking* e o *Mobile Banking*, que modernizaram os serviços, tornando-os mais ágeis, personalizados e eficientes. Entretanto, esse avanço tecnológico também trouxe desafios quanto à necessidade de investimentos contínuos em segurança cibernética e educação financeira para a proteção dos usuários, uma vez que os métodos utilizados para a aplicação de fraudes também evoluíram ao longo dos anos (Paula, 2024).

Conforme observado por Lopes (2023), o principal objetivo das fraudes está na obtenção de dados pessoais ou comerciais sensíveis. Para alcançar esse fim, os criminosos criam perfis falsos de indivíduos ou instituições legítimas, visando explorar a credibilidade atribuída pelas pessoas às empresas. Nesse contexto, os golpistas se valem de técnicas sofisticadas para a realização dos mais diversos tipos de ataques, afetando inúmeras vítimas em todo o território nacional.

O Relatório de Identidade Digital e Fraude de 2024, realizado pela Serasa *Experian* (2024), destaca que 42% dos 1.135 entrevistados já foram vítimas de fraude. Além disso, o valor médio desses prejuízos em decorrência dos golpes foi de R\$ 2.288,00. Em relação aos golpes mais comuns listados pela pesquisa, temos o uso indevido de cartões de crédito (39%) e as falsificações de boletos/PIX (32%). Os dados ressaltam a necessidade de medidas administrativas de segurança robustas por parte das instituições financeiras, para proteger os seus clientes e manter a confiança no sistema bancário (SERASA EXPERIAN, 2024).

Quanto à responsabilidade pelas fraudes bancárias, o que os consumidores esperam é que as instituições bancárias assumam a sua parte das obrigações pela administração das contas e operações financeiras, dado que o serviço contratado por eles deve apresentar medidas de segurança contra o risco de fraudes (Pithagoras, 2025). Nesse sentido, é necessário que tais instituições reconheçam o seu papel dentro dessa realidade e se comprometam a oferecer um suporte eficaz aos seus clientes, conquistando a sua confiança e fidelidade ao evitar que se tornem as próximas vítimas.

Considerando esse cenário, torna-se pertinente investigar de que maneira a ocorrência de situações de fraude pode afetar a percepção dos clientes sobre as instituições financeiras. Diante disso, surge a seguinte problemática: *Como o contexto de fraude impacta na percepção da confiança, continuidade, segurança e recomendação dos clientes sobre as instituições financeiras?*

Assim, o objetivo geral deste estudo é analisar o impacto do contexto de fraude na confiança, continuidade, segurança e recomendação dos clientes sobre as instituições financeiras.

Diante do exposto, a pesquisa justifica-se pela necessidade de compreender como essas experiências negativas impactam na relação dos consumidores com as instituições financeiras. Isso porque, em um cenário em que os clientes buscam proteção e apoio em situações de insegurança, torna-se crucial investigar os principais fatores que influenciam de forma positiva a experiência do cliente com as instituições bancárias.

Destaca-se ainda a contribuição prática deste trabalho, que envolve a análise das consequências das fraudes financeiras sob a ótica do consumidor, além de oferecer resultados que podem servir no desenvolvimento de estratégias de atendimento antifraude e pós-fraude por parte das instituições financeiras. No campo acadêmico, a pesquisa amplia o debate sobre os impactos das experiências fraudulentas ao explorar elementos do marketing de relacionamento que influenciam a manutenção do vínculo dos clientes com as organizações bancárias. Ademais, os resultados obtidos poderão servir de base para investigações futuras na área de marketing, especialmente aquelas voltadas à compreensão do comportamento do consumidor diante de situações de fraude.

## 2 REVISÃO DA LITERATURA

As fraudes bancárias, conforme apontado por Oliveira (2012), podem ser classificadas em três categorias distintas: interna, quando os golpes são praticados por indivíduos que possuem vínculo direto ou que estejam na instituição que sofreu a fraude; externa, quando não existe vínculo entre o agente fraudador e a instituição onde será realizada uma fraude; e mista, quando envolve a colaboração entre, pelo menos, um agente da instituição e um externo.

Sobre as fraudes externas, Gonçalves (2021) também revela que a pandemia da Covid-19 impulsionou os crimes cibernéticos, tendo em vista a maior adesão a canais digitais, como *Mobile* e *Internet Banking*, por pessoas com pouca familiaridade com o ambiente virtual. O cenário facilitou a atuação de golpistas, que se aproveitaram da engenharia social para explorar a vulnerabilidade das pessoas e de práticas como *phishing* e *pharming*, as quais dispensam a invasão de sistemas bancários, baseando-se exclusivamente no engano direto às vítimas.

Além disso, Santos (2023) destaca que, entre as fraudes mais recorrentes no *Internet Banking*, estão as transferências indevidas por meio de transações eletrônicas e o pagamento de boletos fraudulentos gerados por sistemas de autoatendimento. Os exemplos mencionados ilustram como o ambiente bancário digital, embora prático, apresenta riscos significativos aos consumidores. Dessa forma, empresas bancárias devem adotar medidas de segurança robustas e assumir a responsabilidade diante de eventuais falhas que resultem em prejuízo aos seus clientes (Diniz, 2021).

Nessa perspectiva, para esta revisão, serão abordados quatro tipos de fraudes bancárias externas que mais ocorrem no Brasil: *Phishing*, Golpe do PIX, Golpe do *WhatsApp* e Golpe da Falsa Central de Atendimento (FEBRABAN, 2025). Além disso, também será realizada uma revisão da literatura sobre os construtos que compõem a base analítica deste estudo, os quais serão aprofundados nas seções seguintes.

### 2.1 Principais Tipos de Fraudes Bancárias no Brasil

A Federação Brasileira de Bancos listou alguns dos principais golpes que mais tem impactado as instituições financeiras e os seus consumidores, entre eles temos: (1) *Phishing*, (2) Golpe do PIX, (3) Golpe do *WhatsApp* e (4) Golpe da Falsa Central de Atendimento (FEBRABAN, 2025). Cada uma dessas ameaças apresenta técnicas prejudiciais que buscam

explorar as vulnerabilidades dos usuários, diante da sua falta de conhecimento ou de possíveis falhas que os clientes venham a cometer.

### (1) *Phishing*

O phishing, ou pescaria digital, representa uma fraude eletrônica que consiste no envio de mensagens fraudulentas, realizadas por fraudadores ou engenheiros sociais, que buscam obter informações sensíveis, como senhas e dados pessoais de indivíduos. Os tipos de ataques mais comuns de *phishing* ocorrem geralmente por e-mail, SMS ou redes sociais (Moura Wust; Sordi, 2024).

Essa técnica se baseia na engenharia social, que explora erros humanos por meio da manipulação. Nesse caso, os golpistas utilizam o nome e a identidade visual de instituições renomadas para enganar o receptor da mensagem e fazê-lo expor os seus dados pessoais (Gonçalves, 2021; Kaspersky, 2025). Utilizando-se da identidade visual e de outras características reconhecíveis das instituições bancárias, os fraudadores conseguem induzir os consumidores a fornecer voluntariamente os seus dados, motivados pela confiança que depositam na suposta legitimidade da comunicação recebida.

Dessa forma, não há necessidade de invasão ou quebra dos sistemas bancários, pois os próprios usuários, enganados, fornecem as informações necessárias para que os criminosos acessem suas contas (Silva; Cerewuta, 2022). Essas informações que foram pescadas virtualmente pelos criminosos, posteriormente, passam a circular em um mercado ilícito, no qual outros fraudadores as comprem e utilizam para ocultar as suas verdadeiras identidades (Nascimento; Santos; Edler, 2022).

### (2) Golpe do PIX

Outro formato de golpe é por meio do Pix, um meio de pagamento brasileiro, criado para ser usado pelo aparelho celular. As transferências realizadas via Pix podem ser realizadas sem a necessidade de saber onde a outra pessoa tem conta bancária, pois somente com a informação da Chave Pix, os valores da transação são repassados para outra conta em poucos segundos. Não existem impedimentos em questão de horários, dias ou de qual instituição de pagamento, seja banco tradicional ou *fintech*, as transações financeiras serão executadas (Banco Central do Brasil, 2025).

De acordo com Koch (2022), desde a origem do Pix, em novembro de 2020, esse formato de pagamento vem sendo alvo de ações fraudulentas para movimentar o dinheiro das vítimas nas contas dos criminosos. Sob outra perspectiva, Branco (2021) aponta que os golpes podem ser feitos de diversas maneiras, e que uma das formas é o “capturador de sessões”, em que o criminoso faz o envio de arquivos infectados que monitoram a abertura do aplicativo bancário, permitindo a captura de credenciais de acesso da conta bancária da vítima.

Existem outras práticas de engenharia social que também são utilizadas, como o envio de comprovantes de Pix falsos, o envio de Pix errado e anúncios falsos nas redes sociais que solicitam pagamento em Pix (SPC Brasil, 2024). Ademais, como o Pix opera dentro do ambiente do autoatendimento digital, os bancos também podem assumir a responsabilidade por prejuízos decorrentes de fraudes cometidas nesse meio virtual (Santos, 2023).

### (3) Golpe do WhatsApp

Nesse tipo de fraude, existe um método muito usado que envolve a exploração da confiança da vítima e dos seus contatos próximos, chamado de Clonagem do WhatsApp. Os golpistas clonam a conta do aplicativo da vítima, obtendo acesso ao seu histórico de conversas

e contatos. Para isso, eles fingem ser de uma instituição ou de uma empresa conhecida e solicitam o código de verificação enviado por SMS, alegando se tratar de uma atualização, manutenção ou confirmação de cadastro (Moura Wust; Sordi, 2024).

Com o acesso ao código, os criminosos conseguem visualizar o histórico completo de conversas e a lista de contatos da vítima dentro dos seus próprios dispositivos. A partir disso, eles enviam mensagens falsas aos contatos próximos da vítima, passando-se por ela, e solicitam empréstimos. Com isso, eles enganam os contatos, fazendo-os acreditar que estão conversando com a pessoa verdadeira (Polido, 2023).

#### (4) Golpe da Falsa Central de Atendimento

Por fim, vale destacar o golpe da falsa central de atendimento, no qual o criminoso se passa por um funcionário do banco ou empresa conhecida com os quais a vítima possui algum vínculo, alegando que a sua conta foi comprometida. O fraudador solicita informações pessoais e financeiras, como por exemplo: senhas, número do cartão e dados da conta (Moura Wust; Sordi, 2024). Segundo Polido (2023), em determinadas situações, o fraudador induz a vítima a ligar para o número da central do banco, uma tática que serve para dissipar desconfianças sobre a ação fraudulenta. No entanto, o golpista permanece na linha e continua a simular o atendimento, conduzindo a conversa para conseguir obter os dados desejados.

Tendo em vista o panorama das quatro principais fraudes que afetam a integridade financeira dos clientes bancários, torna-se fundamental compreender os fatores que influenciam a decisão dos consumidores manterem ou não esse relacionamento com o banco. Nessa perspectiva, os próximos tópicos vão abordar a literatura dos construtos, segurança, confiança continuidade e recomendação.

## 2.2 Percepção de Segurança em Serviços Bancários

No cenário atual, a percepção de segurança constitui uma das principais preocupações dos consumidores na hora de contratar serviços bancários digitais, especialmente diante do aumento expressivo de fraudes. Em 2024, mais de 500 mil brasileiros foram vítimas de golpes bancários, sendo a maioria desses crimes cometidos por meio de dispositivos móveis, conforme indicado no levantamento da Federação Brasileira de Bancos (Jornal Nacional, 2025). Esse contexto evidencia não apenas a vulnerabilidade técnica do sistema, mas, sobretudo, o sentimento de insegurança que afeta o comportamento dos usuários.

A insegurança percebida, impulsionada pelo aumento de fraudes e pela exposição a vulnerabilidades nos canais digitais, faz com que os consumidores encarem a segurança como um fator de resistência ao utilizarem operações online, sobretudo entre os usuários mais tradicionais (Reis, 2018). No entanto, mesmo com a modernização dos sistemas bancários, tornam-se necessárias estratégias de segurança como os sistemas de inteligência artificial e *machine learning*, e outras soluções tecnológicas como o uso de biometria, autenticação multifatorial, criptografia e o *blockchain* (Pegoraro, 2024).

A adoção desses sistemas avançados de monitoramento e detecção contribui na identificação de possíveis fraudes financeiras. Essas abordagens protegem os recursos financeiros e informações confidenciais, garantindo que as comunicações entre os clientes e as empresas financeiras ocorram em um ambiente seguro (Souza, 2023). No entanto, a percepção de segurança não pode ser apenas voltada ao fortalecimento da segurança dos sistemas.

Existe o aspecto do risco percebido, que se refere à incerteza sentida pelos consumidores diante de possíveis perdas ao usarem serviços bancários online, especialmente quando não conseguem prever totalmente suas consequências (Bashir e Madhavaiah, 2015). Sendo assim, a adesão ao *internet banking* pode ser impactada pela confiança do usuário ao utilizar a

plataforma e pela segurança percebida, visto que a ausência desses fatores pode tornar a sua experiência frustrante e gerar resistência (Aribake e Mat Aji, 2020).

Além do risco percebido, autores como Jansen e Van Schaik (2017) apontam ainda os fatores psicológicos provenientes das fraudes. Os autores destacam que a resistência à utilização de serviços bancários digitais também pode estar associada ao *locus* de controle, um conceito que descreve se os indivíduos acreditam ter controle sobre os resultados de uma situação (*locus* interno) ou se esses resultados dependem de fatores externos (*locus* externo), como a instituição financeira.

Dependendo da situação, os clientes podem transferir a responsabilidade pela sua segurança ao banco ou podem assumir práticas preventivas, desde que estejam devidamente conscientizados sobre elas. Conforme apontado por Zohora *et al.* (2024) em seu estudo, os consumidores que possuem um nível maior de conhecimento sobre segurança tendem a utilizar mais recursos de proteção, como a alteração frequente de senhas, apresentando menor vulnerabilidade a fraudes. Enquanto outra parte dos entrevistados demonstrou uma baixa conscientização sobre práticas de segurança, o que evidencia a necessidade de campanhas educativas sobre riscos e medidas de proteção.

A percepção de segurança também depende da capacidade dos bancos de equilibrar a usabilidade e a proteção, promovendo ferramentas e práticas eficazes e de segurança. Segundo Jansen e Van Schaik (2017), a adoção de comportamentos preventivos tende a crescer quando os usuários percebem que os benefícios superam os custos envolvidos e reconhecem que outras pessoas também estão se protegendo. Desse modo, os bancos devem buscar um equilíbrio entre usabilidade e segurança, investindo em estratégias que estimulem a adoção coletiva de práticas seguras.

### 2.3 Confiança nas Instituições Financeiras

As fraudes bancárias afetam diretamente a relação entre os consumidores e as instituições financeiras. No contexto dos serviços bancários digitais, a confiança dos clientes representa um dos elementos mais sensíveis e decisivos para a continuidade do vínculo entre cliente e banco após a experiência de fraude, especialmente quando precisam confiar na segurança das operações, na proteção dos dados e na qualidade dos serviços prestados pela instituição (Teixeira, 2020; Fidelis, 2023).

No ambiente do *Internet Banking*, a confiança pode ser compreendida como a disposição do cliente em realizar transações financeiras online acreditando que o banco vai cumprir com as suas obrigações, mesmo que não se possa monitorar diretamente as suas ações (Yousafzai; Pallister; Foxall, 2009). Embora o ambiente digital ofereça praticidade, ele também expõe os clientes aos riscos, exigindo que os bancos adotem medidas técnicas de segurança mais eficazes e que promovam transparência e responsabilidade. Assim, medidas como criptografia robusta, autenticação em múltiplos fatores e sistemas antifraude tornam-se indispensáveis para preservar essa relação de confiança (Bashir; Madhavaiah, 2015).

Diante das transformações digitais e tecnológicas que ocorrem nos sistemas bancários, a confiança passa a depender de uma estrutura regulatória. Tendo em vista que, à medida que as instituições financeiras acessam grandes volumes de dados pessoais, torna-se fundamental assegurar a transparência das operações e a responsabilidade pelo tratamento dessas informações (Teixeira, 2020).

Conforme Madureira (2024), o banco se torna responsável pela confiança depositada pelos clientes de proteger o seu patrimônio pessoal. Essa relação assimétrica, em que o consumidor se configura como a parte mais vulnerável da relação de consumo, suscetível ao risco de atos fraudulentos de terceiros, exige um dever de qualidade no fornecimento de

serviços. Assim, os serviços vão além de expectativas funcionais, envolvendo a segurança e a responsabilidade diante de falhas nos sistemas.

Além disso, os bancos devem se atentar para as suas estratégias de construção de confiança, pois esse fator é essencial para a aceitação dos serviços bancários digitais e influencia diretamente a percepção de risco dos consumidores. Uma estratégia eficaz é manter os clientes informados, o que contribui para a redução de possíveis desentendimentos e fortalece a relação banco-cliente (Bashir e Madhavaiah, 2015).

## **2.4 Continuidade da Relação com a Instituição Bancária**

A relação entre cliente e instituição bancária pode ser seriamente abalada por episódios de fraude, independentemente da responsabilidade direta da instituição ou da posterior compensação dos prejuízos. Estudos como o de Somanchi e Telang (2016) mostram que clientes impactados por transações fraudulentas, mesmo quando ressarcidos, tendem a encerrar sua relação com a organização financeira. Esse efeito foi ainda maior entre aqueles que não receberam compensação, gerando impactos severos no relacionamento entre clientes com maior tempo de serviço.

Diante disso, a adoção de práticas voltadas à segurança e à comunicação transparente representa um aspecto central no esforço de manutenção dessa relação. Conforme destaca Hoffmann e Birnbrich (2012), a familiaridade dos clientes com os protocolos de segurança e a clareza na comunicação das medidas antifraude são essenciais para sustentar o vínculo, sobretudo com públicos mais experientes.

A continuidade do relacionamento bancário está, portanto, associada à decisão do cliente de manter e, eventualmente, expandir a sua conexão com a instituição. Essa decisão é influenciada pela qualidade do atendimento e pelo fornecimento de soluções rápidas e personalizadas. Tais exigências representam as principais demandas dos clientes no cenário digital (Ferreira, 2021). Nessa perspectiva, Cabral e Torres (2019) destacam que a satisfação e a fidelização dos clientes devem ser contínuas, e que a qualidade do atendimento precisa ser priorizada pelos bancos, visto que a opção de migrar de banco é considerada quando o cliente está insatisfeito com os serviços prestados.

Nesse sentido, o marketing de relacionamento surge como uma abordagem eficaz para compreender o comportamento do consumidor antes e após a contratação de serviços. Ele se propõe a converter interações pontuais em relações contínuas e significativas, agregando valor à experiência do cliente e promovendo vantagem competitiva para o banco (Unes; Camioto; Guerreiro, 2019). Complementarmente, o marketing de relacionamento indica que as empresas realizem um atendimento eficiente, com foco na personalização, no uso inteligente da tecnologia e com atenção às demandas dos clientes. Esses aspectos podem promover o valor e a imagem da empresa, além de fortalecer a relação com os clientes (Leite; Ceo, 2024).

Em vista disso, torna-se crucial que os bancos estejam atentos tanto à prestação de serviços de qualidade em situações críticas, como fraudes, quanto à capacidade de compreender e atender às necessidades de seus usuários. A eficiência dos canais de atendimento, aliada a uma comunicação transparente e a orientações claras sobre segurança digital, configuram-se como fatores determinantes para a satisfação e fidelização dos usuários no ambiente bancário digital (Rezende *et al.*, 2019; Amin, 2016).

## **2.5 Recomendação dos Serviços Bancários**

A recomendação de serviços bancários é um importante indicador da percepção de utilidade, à satisfação com os serviços e à influência do círculo social durante o relacionamento com as instituições financeiras. Além disso, clientes mais engajados com os serviços do banco

tendem a recomendar a marca a outros possíveis clientes, uma vez que sentem uma forte conexão com o seu banco digital (Alves *et al.*, 2023).

De acordo com Bashir e Madhavaiah (2015), a influência social exerce um forte impacto na decisão dos consumidores ao escolherem serviços bancários, devido à importância atribuída à opinião de pessoas próximas, como amigos, familiares e outros grupos sociais ao qual pertencem. Conforme mostra a pesquisa realizada pela Fintech Mambu, 90% dos entrevistados entre os 18 aos 35 anos buscaram recomendações antes de escolher um banco. Deste percentual, 24% procuraram informações na internet para escolher um banco e 66% recorreram a pessoas próximas, como amigos e familiares (Souza, 2022).

Embora a recomendação seja fortalecida por experiências positivas e influências sociais, é válido considerar o impacto de eventos negativos, como fraudes bancárias, na percepção dos clientes. A ocorrência de golpes não só gera custos financeiros, mas também emocionais, afetando a percepção de segurança das iniciativas oferecidas pela instituição, mesmo com a compensação das perdas financeiras. (Somanchi; Telang, 2016). Nesse contexto, a forma como o banco responde a essas ocorrências se torna decisiva. Ao intervir na qualidade do serviço bancário e resolver os problemas, a instituição pode assegurar a satisfação do cliente e até reforçar a confiança dos usuários no ambiente digital (Amin, 2016).

Assim, altos níveis de satisfação, quando combinados a serviços de valor, influenciam positivamente na intenção de recomendar, sobretudo nos canais digitais. A oferta de garantias incondicionais em caso de perdas, aliada a sistemas bancários online funcionais e agradáveis, pode incentivar os usuários a compartilhar essas experiências (Bashir e Madhavaiah, 2015). Ademais, é essencial que os bancos financiem medidas de segurança robustas e tenham agilidade na restauração da confiança sempre que ameaças de fraude forem identificadas (Moura Wust; Sordi, 2024).

Dessa forma, clientes que percebem as instituições financeiras como seguras e responsáveis diante de situações negativas, como fraudes, tendem não apenas a manter sua fidelidade, mas também a recomendar a marca a outras pessoas. A recomendação, portanto, reflete a confiança restaurada e a segurança percebida no ambiente digital. Rahi, Alghizzawi e Ngah (2022) sustentam essa visão ao apontar que, ao desenvolver ou aprimorar a plataforma de *Internet Banking*, as instituições devem considerar as características intrínsecas dos usuários, dado que a imagem positiva dos serviços online fortalece a confiança, estimula o uso contínuo e a recomendação do serviço a familiares e amigos.

## 2.6 Hipóteses e Desenho do Modelo de Pesquisa

As definições das hipóteses deste estudo foram estabelecidas pelas relações estruturais entre os construtos: segurança, confiança, continuidade e recomendação, os quais representam as dimensões centrais da experiência do cliente com o banco, dentro do contexto de fraudes bancárias. A partir da literatura analisada anteriormente, foram propostas três hipóteses.

A relação entre segurança e confiança é essencial no ambiente bancário digital, sobretudo diante do aumento de tentativas de fraudes. A percepção de segurança antifraude constitui um dos principais fatores de decisão do consumidor ao contratar serviços online, pois a vulnerabilidade técnica e psicológica gerada por golpes, como por exemplo, *Phishing*, Golpe do Pix, Golpe do WhatsApp e Golpe da Falsa Central de Atendimento, acaba comprometendo a credibilidade nos bancos (Bashir; Madhavaiah, 2015; Reis, 2018; FEBRABAN, 2025; Jansen; Aribake e Mat Aji, 2020).

Estudos indicam que medidas antifraude, como autenticação multifatorial e sistemas de inteligência artificial, podem fortalecer a confiança na operação de serviços devido ao aumento da proteção dos dados pessoais dos clientes (Pegoraro, 2024; Madureira 2024; Souza, 2023). Por outro ângulo, existem estudos que ressaltam a resistência de consumidores ao adotarem



serviços digitais, por conta da teoria do Locus de Controle. Nessa concepção, a responsabilidade pela segurança pode ser atribuída ao banco (locus externo) ou assumida pelo próprio cliente de forma proativa (locus interno), podendo variar com base no nível de conhecimento em segurança digital (Jansen e Van Schaik, 2017; Zohora et al., 2024). Perante o exposto, são formuladas as seguintes hipóteses para o estudo:

H1a: A percepção de segurança antifraude influencia positivamente a confiança do cliente

H1b: O locus de controle influencia positivamente a confiança do cliente

H1c: A motivação para se proteger influencia positivamente a confiança do cliente

A literatura aponta que a recomendação é influenciada tanto por experiências positivas quanto pela forma como o banco responde a situações críticas. Clientes que percebem as suas instituições como seguras e confiáveis após fraudes demonstram maior disposição em recomendar os serviços, pois a confiança aumenta a satisfação do cliente e reforça a qualidade do ambiente bancário digital (Somanchi; Telang, 2016; Amin, 2016). Nesse cenário, a habilidade dos bancos em restaurar a confiança após eventos fraudulentos é fundamental para o fortalecimento da conexão com o cliente e na criação de uma imagem positiva (Alves et al., 2023; Rahi; Alghizzawi; Ngah, 2022). Alguns autores apontam que altos níveis de satisfação combinados à segurança percebida ampliam a intenção de recomendar, inclusive em canais digitais (Bashir; Madhavaiah, 2015). Esse contexto justifica a hipótese abaixo:

H2: A confiança na instituição influencia a disposição do cliente recomendar o banco

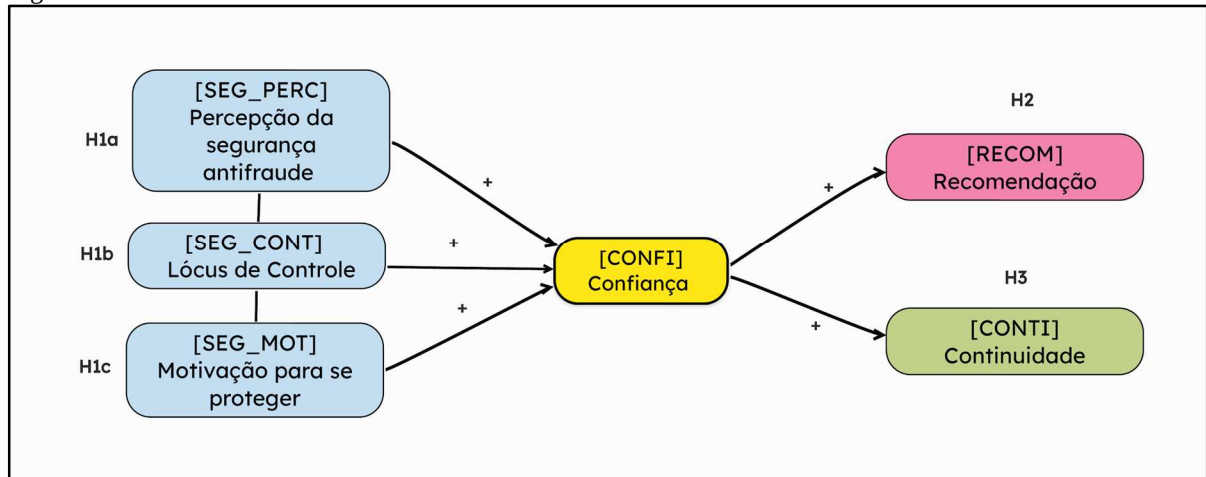
A continuidade da relação bancária depende, principalmente, da confiança que o cliente deposita na instituição, especialmente após episódios de fraude. Estudos revelam que consumidores afetados por transações fraudulentas tendem a encerrar vínculos bancários, mesmo quando há ressarcimento, reforçando que a confiança é uma dimensão determinante para a permanência (Somanchi; Telang, 2016). No entanto, práticas de comunicação transparente, agilidade no atendimento e protocolos de segurança contribuem para preservar a lealdade do cliente e expandir o relacionamento com o banco (Hoffmann; Birnbrich, 2012; Ferreira, 2021). No contexto das fraudes bancárias, em que a insatisfação do cliente é acentuada, a confiança adquirida ou restaurada pela instituição bancária é o fator que sustenta a decisão de continuidade, o que justifica a hipótese proposta a seguir:

H3: A confiança na instituição influencia a disposição do cliente continuar a se relacionar com o banco

Após a apresentação e justificativa das hipóteses da pesquisa a serem testadas, a Figura 1 demonstra o modelo conceitual do estudo, considerando as relações entre os construtos, confiança, segurança, continuidade e recomendação. O construto “Segurança” foi dividido em três dimensões, percepção da segurança antifraude, locus de controle e motivação para se proteger, conforme proposto por Jansen (2018) e Aribake e Mat Aji (2020).

No modelo, as hipóteses H1a, H1b e H1c são antecedentes da confiança do cliente no banco. Por sua vez, o construto confiança se conecta às hipóteses H2 e H3, indicando a sua relação direta com a recomendação e a continuidade do relacionamento com o banco. A Figura 1 expõe as relações hipotéticas:

Figura 1: Modelo conceitual do estudo



Fonte: Elaborado pelo autor (2025)

Depois de apresentar o modelo e as hipóteses, o próximo tópico aborda os processos e as decisões metodológicas adotadas e o desenvolvimento do instrumento de pesquisa.

### 3 PROCEDIMENTOS METODOLÓGICOS

Nesta seção, detalha-se os procedimentos metodológicos escolhidos para a pesquisa. Com o objetivo de analisar a relação dos consumidores com as instituições financeiras após experiências de fraudes bancárias, a pesquisa utiliza uma abordagem quantitativa, pois esse enfoque parte da formulação de hipóteses e da definição de variáveis mensuráveis, permitindo a medição numérica e a análise estatística dos dados coletados (Perovano, 2016).

O estudo se classifica como descritivo, visto que tem como objetivo principal analisar características específicas de uma população ou fenômeno, assim como identificar e compreender a natureza das relações entre variáveis. Esse tipo de pesquisa usa técnicas padronizadas de coleta de dados e faz levantamento de atitudes, opiniões e comportamentos de um grupo dentro de um determinado contexto (Gil, 2019).

A fase inicial da pesquisa contou com a revisão da literatura nas seguintes bases de dados nacionais e internacionais: Google Acadêmico, SciELO e *Emerald Insight*. Nesse sentido, a fundamentação teórica foi construída a partir da verificação de artigos publicados em periódicos científicos, monografias e livros especializados. Além disso, foi conduzida uma busca por escalas validadas anteriormente na literatura, com vistas à adaptação para os objetivos do presente estudo.

Os construtos escolhidos para integrar no instrumento de pesquisa foram os seguintes: “Confiança”, adaptado dos trabalhos de Hoffmann e Birnbrich (2012) e Valentin Ngobo (2004); “Continuidade”, adaptado de Hoffmann e Birnbrich (2012); “Recomendação”, adaptado dos estudos de Bashir e Madhavaiah (2015), Rahi, Ghani e Ngah (2018) e Rahi, Alghizzawi e Ngah (2022); e, por último, “Segurança”, que foi adaptado dos estudos de Jansen (2018) e Aribake e Mat Aji (2020). No Apêndice 1 encontram-se as referências das escalas originais que foram adaptadas e usadas para o estudo, assim como os itens de mensuração de cada construto que compõem o instrumento de pesquisa.

Antes da coleta de dados, foi executado um processo de validação dos itens dos construtos e as questões sociodemográficas, buscando avaliar a sua clareza, relevância e correspondência com os construtos analisados no instrumento de pesquisa. Para isso, o questionário foi avaliado por dois professores de Marketing, especialistas em métodos quantitativos, e depois foi realizado um pré-teste com 15 respondentes, que forneceram opiniões e sugestões sobre o instrumento.

Entre as modificações realizadas no questionário, destacam-se a reordenação das perguntas e a substituição de alguns termos nos itens dos construtos, com o objetivo de reduzir o efeito de similaridade entre eles. Enquanto isso, no construto "recomendação", três perguntas foram excluídas e duas novas foram incluídas, resultando em um total de três questões, a fim de aumentar a sua consistência interna. A partir dos resultados obtidos com o pré-teste e das recomendações dos especialistas, a ferramenta de pesquisa foi ajustada e, em seguida, foi divulgada em sua versão final.

O questionário final, contendo 32 perguntas, foi disponibilizado online por meio da plataforma *Google Forms*. Esse instrumento foi dividido em questões de caracterização sociodemográfica (gênero, renda, idade, nível de formação, e cidade/estado em que residem). Assim como houve perguntas sobre o vínculo com instituições financeiras e bancos, tempo de relacionamento com essas organizações, ocorrência de fraudes sofridas, tipos de fraudes bancárias vivenciadas e frequência de fraudes envolvendo pessoas próximas.

Ademais, acrescentam-se as questões sobre os construtos mencionados anteriormente, sendo contextualizados com um texto introdutório sobre os quatro tipos de cenário de fraudes bancárias que mais ocorrem no Brasil, conforme a Federação Brasileira de Bancos (FEBRABAN, 2025). Os itens dos construtos foram dispostos em escalas do tipo *Likert* de 7 pontos, no qual o respondente indica o seu nível de concordância, sendo 1 (Discordo totalmente) e 7 (Concordo totalmente).

O procedimento de coleta de dados ocorreu no período de 28 de julho a 18 de agosto de 2025. A divulgação do questionário foi realizada pelas redes sociais da pesquisadora, especificamente, o WhatsApp, o Instagram e o Gmail. No Instagram, o questionário foi compartilhado pelo perfil da pesquisadora e pelo grupo de pesquisa, Lemic, por meio dos *Stories* e do *Feed*. A pesquisa também foi compartilhada pelo perfil da coordenação do curso de Administração, e as imagens divulgadas no Instagram estão disponíveis no Apêndice 5. No WhatsApp e Gmail, o questionário foi compartilhado com amigos, familiares e pessoas próximas.

Quanto à análise de dados, os resultados do questionário passaram pela aplicação de diferentes técnicas estatísticas, com o apoio do software SPSS e do software R. Entre as etapas de testagem das hipóteses, inicialmente, realizou-se uma análise psicométrica, considerando o *alpha de Cronbach* e as cargas fatoriais de cada construto. Posteriormente, os dados foram submetidos às análises descritivas e teste de correlação de Pearson. Por fim, a verificação das hipóteses foi feita por meio da modelagem de equações estruturais. Esses procedimentos foram desenvolvidos com fundamento na literatura especializada (Cohen, 1988; Dancey e Reidy, 2019; Hair et al., 2009).

## 4 RESULTADOS

No presente item, são apresentados os resultados obtidos a partir do estudo empírico. Inicialmente, será exposta a análise descritiva dos dados, considerando medidas como média, desvio-padrão e quartis. Na sequência, foi realizada a análise psicométrica, com as respectivas cargas fatoriais dos itens dos construtos e o nível de confiabilidade do instrumento, medido pelo coeficiente *alpha de Cronbach*. Posteriormente, verificou-se as associações entre as variáveis por meio do teste de correlação de Pearson e, por último, foi realizada uma análise conjunta das hipóteses por meio de equações estruturais, com o objetivo de esclarecer as relações de influência entre os construtos.

### 4.1 Descrição da amostra

Sobre a caracterização da amostra, houve um total de 160 respostas, no qual 62,5% foram respondentes do gênero feminino e 37,5% do gênero masculino. Sobre a idade dos participantes, houve uma maior representação 57,5% da faixa etária entre 18 e 29 anos, seguida de 23,1% da faixa etária entre 30 e 39 anos. Sobre o grau de escolaridade, 32,5% dos participantes indicaram possuir o Ensino Superior Incompleto, em seguida, 22,5% indicaram ter o Ensino Médio Completo. Quanto à renda pessoal, a maioria dos respondentes 26,3% apontaram ter uma renda de até R\$1.518,00, um salário mínimo. Adicionalmente, 21,9% indicaram ter uma renda acima de R\$ 2.000,00 até R\$ 3.000,00, enquanto outros 21,9% relataram ter uma renda acima de R\$ 5.000,00.

Quanto à localização geográfica, os participantes foram agrupados por região, sendo que a maioria dos respondentes (96,25%) residia na região Nordeste, seguida das regiões Sudeste (3,13%) e Sul (1%). Em relação às instituições financeiras utilizadas, os bancos tradicionais mais citados foram: Caixa Econômica Federal (46,88%), Banco do Brasil (38,13%), Bradesco (33,75%) e Itaú (23,75%). Também foram mencionados bancos digitais, os mais citados foram Nubank (69,38%), Inter (26,88%) e Mercado Pago (24,38%). Sobre o tempo de relacionamento com os bancos ou instituições financeiras, 20,6% relataram ser clientes há mais de 10 anos, 26,2% possuem vínculo entre 6 a 10 anos, 30,6% possuem vínculo entre 5 a 4 anos e 17,5% entre 2 a 3 anos.

A respeito do percentual de participantes que foram ou não foram vítimas de alguma fraude bancária, 26,3% dos respondentes foram vítimas de fraude e 73,8% não foram vítimas de fraude. No questionário, foram investigados quatro tipos de fraudes, com base nas principais fraudes bancárias apresentadas pelo site da FEBRABAN. Dentre os participantes que relataram ter sido vítimas, 9,4% relataram ter sofrido *Phishing* por e-mail e 8,1% indicaram ter sofrido o Golpe da Falsa Central de Atendimento. Enquanto 7,5% sofreram o Golpe do PIX e 14,4% apontaram ter sofrido o Golpe do WhatsApp.

As alternativas dos quatro tipos de fraudes, encontram-se no Apêndice C, questão doze, e seguem essa ordem: *Phishing* (Letra A), Falsa Central de Atendimento (Letra B), Golpe do PIX (Letras C, E, F) e Golpe do WhatsApp (Letras D, G). Ademais, entre os respondentes, 24,4% conseguiram identificar o golpe antes de sofrer prejuízo financeiro, enquanto 60,6% não sofreram nenhuma das fraudes listadas ou sofreram um tipo diferente de fraude.

## 4.2 Análise psicométrica

A análise psicométrica foi conduzida por meio do software SPSS, com o objetivo de identificar a consistência interna dos itens e confiabilidade dos construtos. Para tanto, foram considerados os valores de cargas fatoriais acima de 0,50 e do *alpha de Cronbach* acima de 0,70, como valores de referência, a fim de confirmar que as variáveis mensuram de forma adequada os construtos propostos. Os dados estão expostos na Tabela 2.

Tabela 1 – Análise psicométrica

| Construtos           | Itens (códigos) | Cargas Fatoriais | Alpha de Cronbach |
|----------------------|-----------------|------------------|-------------------|
| [CONFI] Confiança    | CONFI1          | 0,779            | 0,811             |
|                      | CONFI2          | 0,805            |                   |
|                      | CONFI3          | 0,819            |                   |
|                      | CONFI4          | 0,794            |                   |
| [CONTI] Continuidade | CONTI1          | 0,894            | 0,939             |
|                      | CONTI2          | 0,925            |                   |
|                      | CONTI3          | 0,939            |                   |

|                                              |           |       |       |
|----------------------------------------------|-----------|-------|-------|
|                                              | CONTI4    | 0,921 |       |
| [RECOM] Recomendação                         | RECOM1    | 0,893 | 0,917 |
|                                              | RECOM2    | 0,949 |       |
|                                              | RECOM3    | 0,937 |       |
|                                              |           |       |       |
| [SEG_CONT] Locus de Controle                 | SEG_CONT1 | 0,759 | 0,732 |
|                                              | SEG_CONT2 | 0,851 |       |
|                                              | SEG_CONT3 | 0,815 |       |
| [SEG_PERC] Percepção de Segurança Antifraude | SEG_PERC1 | 0,872 | 0,759 |
|                                              | SEG_PERC2 | 0,845 |       |
|                                              | SEG_PERC3 | 0,744 |       |
| [SEG_MOT] Motivação para se proteger         | SEG_MOT1  | 0,777 | 0,879 |
|                                              | SEG_MOT2  | 0,885 |       |
|                                              | SEG_MOT3  | 0,866 |       |
|                                              | SEG_MOT4  | 0,898 |       |

Fonte: Elaborado pelo autor (2025)

Considerando os resultados expostos na Tabela 1, no que diz respeito às cargas fatoriais, todos os itens apresentaram valores satisfatórios, acima de 0,70, superior ao limite mínimo recomendado de 0,50, expondo uma boa representatividade deles em relação aos construtos (Hair et al., 2009). Observa-se que os itens mais próximos de 1, e, portanto, mais representativos, foram aqueles pertencentes ao construto Continuidade (CONTI), com cargas variando entre 0,894 e 0,939, e ao construto Recomendação (RECOM), cujas cargas oscilaram entre 0,893 e 0,949.

Quanto à confiabilidade interna, avaliada pelo coeficiente *alpha de Cronbach*, todos os construtos alcançaram valores superiores ao patamar mínimo recomendado de 0,70, confirmando a adequação das escalas e dos itens do instrumento. Destacam-se os construtos Continuidade ( $\alpha = 0,939$ ) e Recomendação ( $\alpha = 0,917$ ), que apresentaram confiabilidade classificada como excelente, seguidos por Motivação para se proteger ( $\alpha = 0,879$ ), considerada muito boa, e por Confiança ( $\alpha = 0,811$ ), classificada como aceitável. Já os construtos Percepção de Segurança Antifraude ( $\alpha = 0,759$ ) e Locus de Controle ( $\alpha = 0,732$ ), embora tenham apresentado índices mais baixos em relação aos demais, ainda foram considerados aceitáveis de acordo com a literatura (Hair et al., 2009).

### 4.3 Análise das medidas descritivas

Com base nos resultados da análise psicométrica, os itens de cada construto foram agregados, por meio dos valores de cada respondente ponderados pelos valores das cargas fatoriais dos respectivos itens, o que gerou uma única medida por construto. A partir disso, foram extraídas as medidas estatísticas de posição (média e quartis) e de dispersão (desvio-padrão), conforme demonstrado na Tabela 2.

Tabela 2 - Medidas descritivas

| Variáveis         | Média | Desvio-padrão | Percentis |      |      |
|-------------------|-------|---------------|-----------|------|------|
|                   |       |               | 25        | 50   | 75   |
| [CONFI] Confiança | 4,92  | 1,406         | 4,01      | 5,00 | 5,94 |

|                                                          |      |       |      |      |      |
|----------------------------------------------------------|------|-------|------|------|------|
| [CONTI] Continuidade                                     | 3,21 | 1,900 | 1,31 | 2,76 | 4,52 |
| [RECOM] Recomendação                                     | 2,99 | 1,920 | 1,00 | 2,66 | 4,38 |
| [SEG_CONT] Segurança - Locus de Controle                 | 4,47 | 1,526 | 3,35 | 4,66 | 5,63 |
| [SEG_PERC] Segurança - Percepção de Segurança Antifraude | 4,26 | 1,607 | 3,00 | 4,34 | 5,55 |
| [SEG_MOT] Segurança - Motivação para se proteger         | 5,98 | 1,363 | 5,29 | 6,63 | 7,00 |

Fonte: Elaborado pelo autor (2025)

Tendo em vista os resultados apresentados na Tabela 2, o construto “Confiança” teve uma média igual a 4,92, indicando um nível geral de confiança relativamente favorável em relação ao banco, com isso se confirmando nas medidas dos quartis. O construto “Continuidade” teve uma média igual a 3,21, o que indica que, após sofrer uma fraude bancária, os respondentes concordam em manter o vínculo com o banco. Enquanto isso, o construto “Recomendação” teve a menor média dos construtos, com valor 2,99. Com isso, os respondentes revelaram pouca disposição em recomendar os serviços de *Internet Banking* do seu banco, o que foi evidenciado também nos valores dos quartis. O desvio-padrão foi o mais elevado em comparação com o dos outros construtos, o que indica que houve uma alta variação das respostas.

O construto “Locus de Controle” teve uma média de 4,47, ou seja, há uma moderada concordância, em média, acerca da responsabilidade dos respondentes pela manutenção da sua própria segurança durante o uso dos serviços de *Internet Banking*. O valor médio do construto (4,26) “Percepção de Segurança Antifraude” indica que, de modo geral, a percepção dos respondentes sobre as ações preventivas de fraude dos seus bancos é razoável. Por último, o construto “Motivação para se proteger” apresentou a maior média de todos os construtos analisados, sendo igual a 5,98. Isso demonstra que os respondentes revelam uma boa disposição para seguir as recomendações de proteção antifraudes do seu banco.

#### 4.4 Análise de associação

A análise de correlação de Pearson foi conduzida com o auxílio do software SPSS, com o objetivo de verificar a intensidade e a direção das relações lineares entre os construtos do modelo conceitual. O coeficiente de correlação ( $r$ ) pode variar de -1 a +1, sendo que valores próximos de 1 indicam forte correlação positiva, valores próximos de -1 apontam forte correlação negativa e valores próximos de 0 revelam ausência ou baixa associação. Para fins de interpretação, adotou-se a classificação de Dancey e Reidy (2019), em que correlações entre 0,10 e 0,30 são consideradas fracas, 0,40 e 0,60 são moderadas e acima de 0,70 são fortes. Os resultados são apresentados na Tabela 3.

Tabela 3 - Medidas de correlação

| Construtos (Variáveis) | CONFI   | CONTI   | RECOM   | SEG_CONT | SEG_PERC | SEG_MOT |
|------------------------|---------|---------|---------|----------|----------|---------|
| CONFI                  | 1       |         |         |          |          |         |
| CONTI                  | 0,400** | 1       |         |          |          |         |
| RECOM                  | 0,325** | 0,811** | 1       |          |          |         |
| SEG_CONT               | 0,633** | 0,285** | 0,307** | 1        |          |         |
| SEG_PERC               | 0,681** | 0,455** | 0,389** | 0,447**  | 1        |         |

|                |         |       |       |         |         |   |
|----------------|---------|-------|-------|---------|---------|---|
| <b>SEG_MOT</b> | 0,477** | 0,107 | 0,066 | 0,323** | 0,274** | 1 |
|----------------|---------|-------|-------|---------|---------|---|

Fonte: Elaborado pelo autor (2025)

Nota: N = 160. Nas células, \*\* indica significância a  $p < 0,01$  (2 extremidades).

Com base nos resultados, observa-se que o construto “Confiança” (CONFI) apresenta correlações fortes, próximos de +1, com o construto “Percepção de Segurança Antifraude” (SEG\_PERC;  $r = 0,681$ ) e com o construto “Lócus de controle” (SEG\_CONT;  $r = 0,633$ ). Essas informações indicam que tanto a forma como os clientes avaliam as ações da instituição quanto o sentimento de controle pessoal sobre a sua proteção se relacionam positivamente com a confiança no banco.

Ademais, a confiança também se correlaciona de maneira moderada com a motivação individual para se proteger (SEG\_MOT;  $r = 0,477$ ). Esse resultado evidencia que, embora a disposição individual de seguir as regras de proteção do banco contribua para o fortalecimento da confiança, o seu impacto é menos expressivo do que os aspectos relacionados à segurança antifraude desenvolvida pelos bancos (SEG\_PERC;  $r = 0,681$ ).

Por sua vez, o construto “Confiança” apresentou correlação moderada com o construto “Continuidade” (CONTI;  $r = 0,400$ ) e moderada, porém mais fraca, com o construto “Recomendação” (RECOM;  $r = 0,325$ ). Esses valores sugerem que, embora a confiança esteja relacionada tanto com a intenção de permanecer com o banco utilizando os serviços quanto com a disposição para recomendar o banco a pessoas próximas e terceiros, essa relação é mais intensa no caso da continuidade.

Entre os demais construtos, a associação mais forte foi observada entre Recomendação e Continuidade ( $r = 0,811$ ), evidenciando que os respondentes propensos a recomendar a instituição também tendem a manter o relacionamento com ela. Por outro lado, as menores correlações foram verificadas entre os construtos “Motivação para se proteger” e “Recomendação” ( $r = 0,066$ ) e entre “Motivação para se proteger” e “Continuidade” ( $r = 0,107$ ), os valores são baixos, bem próximos de zero. Isso mostra que, estatisticamente, não há associação linear entre os construtos.

Dessa forma, os valores observados permitem inferir que eventuais mudanças na motivação para seguir regras de segurança não se relacionam com alterações nos níveis de continuidade (intenção de permanecer no banco após uma fraude) ou de recomendação (indicar o banco a outras pessoas).

#### 4.5 Análise das hipóteses

Com o intuito de verificar as hipóteses do estudo, foi aplicada a modelagem de equações estruturais por meio do software RStudio, versão 4.5.1, com os pacotes *semPlot* e *lavaan*, utilizando a função *sem*., cujos resultados encontram-se dispostos na Tabela 4. No que diz respeito à interpretação dos indicadores da modelagem de equações estruturais (SEM), o valor de referência para o limiar significativo das hipóteses é o de 0,05, desse modo, quando o p-valor for  $< 0,05$  indica que um resultado é estatisticamente significativo. Enquanto isso, a análise dos valores de beta padronizados e de covariância são baseados na seguinte classificação de Cohen (1988): valores entre 0,10 e 0,29 representam uma baixa relação entre as variáveis; valores entre 0,30 e 0,49 indicam uma relação moderada entre as variáveis; e, em contraste, valores acima de 0,50 sugerem uma forte relação entre as variáveis.

Tabela 4 – Resultados da Modelagem de Equações Estruturais

| Hipóteses  | Relação                          | Beta ( $\beta$ ) | P-valor   | Resultado     |
|------------|----------------------------------|------------------|-----------|---------------|
| <b>H1a</b> | SEG_PERC $\rightarrow$ Confiança | 0,459            | $< 0,001$ | Não rejeitada |
| <b>H1b</b> | SEG_CONT $\rightarrow$ Confiança | 0,352            | $< 0,001$ | Não rejeitada |

|            |                          |       |        |               |
|------------|--------------------------|-------|--------|---------------|
| <b>H1c</b> | SEG_MOT → Confiança      | 0,237 | <0,001 | Não rejeitada |
| <b>H2</b>  | Confiança → Recomendação | 0,325 | <0,001 | Não rejeitada |
| <b>H3</b>  | Confiança → Continuidade | 0,401 | <0,001 | Não rejeitada |

Fonte: Elaborado pelo autor (2025)

Considerando os achados exibidos na Tabela 4, verifica-se que, das cinco hipóteses lançadas, todos os valores de  $\beta$  padronizados foram estatisticamente significativos. Na hipótese H1a, a percepção de segurança antifraude apresenta uma influência muito forte na confiabilidade da instituição, com o  $\beta$  padronizado = 0,459. Representando a variável que mais impacta o construto confiança; isso significa que quanto maior for a percepção das ações de segurança antifraude sobre um determinado banco, maior será a confiança sobre o banco. Esse resultado converge com o obtido na análise bivariada.

Acerca da hipótese H1b, o locus de controle obteve uma influência positiva moderada, com o  $\beta$  padronizado = 0,352. Esse achado demonstra que, quanto mais os clientes percebem estar no controle das medidas antifraude, maior é a tendência de confiarem no banco. A respeito da hipótese H1c, a motivação para se proteger teve o menor valor  $\beta$  padronizado, que foi igual a 0,237, indicando uma fraca influência. Esse resultado sugere que seguir as práticas de segurança do banco é menos expressivo em comparação às demais variáveis analisadas no estudo para que a confiança dos clientes seja fomentada.

Sobre a hipótese H2, a confiança influencia moderadamente na recomendação do banco, com o  $\beta$  padronizado = 0,325. Esse resultado evidencia que quanto maior for a confiança sobre um determinado banco, maior será a probabilidade dos clientes o recomendarem. Com relação à hipótese H3, o construto confiança também influencia moderadamente sobre a continuidade da relação com o banco, com o  $\beta$  padronizado = 0,401. Isso indica que quanto maior for a confiança, maior será a probabilidade de o cliente permanecer com o vínculo.

Assim, todos os resultados de p-valor das hipóteses foram menores que 0,05, sendo iguais a <0,001, um valor muito inferior ao limite de significância de 0,05, o que implica num resultado estatisticamente significativo. Ou seja, isso sugere que existem fortes evidências da hipótese nula ser rejeitada e que pode existir um efeito real entre as cinco hipóteses de pesquisa.

Ademais, foi realizada uma análise de covariância entre as variáveis Recomendação e Continuidade, que foi igual a 0,79. Esse resultado aponta que a relação entre elas é extremamente forte (acima de 0,50), indicando que quando as pessoas recomendam os serviços de um banco, elas também tendem a continuar usando-os. Esse efeito forte também foi observado na correlação entre os dois construtos.

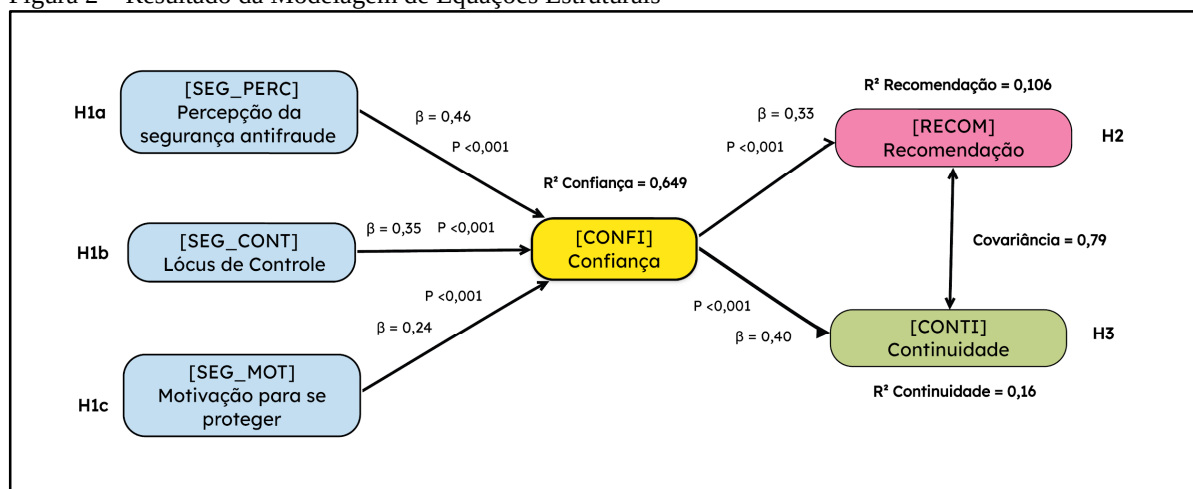
Nesse contexto, com o propósito de compreender a proporção da variabilidade explicada pelas relações entre os construtos do modelo de equações estruturais (SEM), utiliza-se o coeficiente de determinação ( $R^2$ ). Esse indicador revela o quanto dos valores previstos de uma variável dependente do modelo se aproximam das variáveis independentes do modelo. Conforme a classificação proposta por Cohen (1988), valores de  $R^2$  entre 0,02 e 0,12 indicam pouca variabilidade explicada; valores entre 0,13 e 0,25 sugerem uma variabilidade parcialmente explicada e valores superiores a 0,26 apontam uma elevada capacidade explicativa do modelo sobre a variabilidade dos dados.

Com base nessa métrica, os resultados evidenciaram que a variável Confiança apresentou  $R^2 = 0,464$ , o que representa um alto nível de variabilidade explicada pelo modelo, corroborando a relevância de seus efeitos sobre os demais construtos. Já a variável Continuidade obteve  $R^2 = 0,160$ , valor que indica uma explicação moderada, enquanto a variável Recomendação apresentou  $R^2 = 0,106$ , valor que caracteriza um baixo poder explicativo. Assim, observa-se que a Confiança se destacou como o construto mais influente do modelo, tendo um resultado consistente com os valores de beta encontrados, sobretudo em sua relação positiva com as variáveis segurança, recomendação e continuidade.



A Figura 2 exibe um novo modelo baseado nos resultados obtidos na modelagem de equações estruturais gerada pelo software RStudio.

Figura 2 – Resultado da Modelagem de Equações Estruturais



Fonte: Elaborado pelo autor (2025)

No tópico seguinte, serão expostos os resultados referentes aos impactos das fraudes bancárias sobre o relacionamento entre clientes e instituições financeiras, assim como a percepção dos respondentes acerca dos quatro construtos, estabelecendo conexões com os resultados já discutidos pelo campo acadêmico sobre o tema.

## 5 DISCUSSÃO DOS RESULTADOS

Com base nas análises realizadas, todas as hipóteses foram confirmadas, indicando relações significativas entre os construtos explorados. No que diz respeito à primeira hipótese (H1a), que trata da relação entre o construto segurança antifraude e confiança, os resultados apontaram que a percepção de segurança exerce forte influência sobre a confiança nas instituições bancárias.

Esse achado está em consonância com Yousafzai, Pallister e Foxall (2009), que afirmaram, em seu estudo, que a confiança é um construto multidimensional e apresenta três antecedentes, entre eles a segurança percebida, juntamente com a privacidade percebida e a confiabilidade no cenário de *Internet Banking*. Em sua análise, a relação segurança percebida e confiança também foi significativa, com uma influência moderada a forte.

O resultado da hipótese H1b sobre locus de controle evidenciou que a confiança dos clientes se fortalece quando eles percebem a sua maior participação no controle das medidas antifraude. Por outro lado, a hipótese H1c, relativa à motivação de proteção, apresentou o menor efeito entre as variáveis, sugerindo que a confiança decorrente do cumprimento das práticas de segurança pelos bancos exerce um impacto relativamente de menor expressão, apesar de na análise descritiva o construto motivação de proteção ter obtido a maior média dentre os construtos de segurança.

Com isso, pode-se entender que, embora motivados para se protegerem contra fraudes, os respondentes esperam iniciativas antifraudes dos seus bancos. Nesse contexto, é possível inferir que, como estratégia de comunicação de marketing para aumentar o nível de confiança dos clientes, os bancos devem evidenciar suas iniciativas de segurança antifraude, incentivando-os a serem proativos na adesão de tais ações, para aproveitar sua motivação em relação ao comportamento de consumo seguro.

Ainda sobre esses construtos, Jansen e van Schaik (2017) tenham investigado os conceitos de *locus de controle* e *motivação de proteção*, o estudo não utilizou modelagem de equações estruturais, o que impossibilita a comparação direta dos resultados. Entretanto, seus achados descritivos permitem certas aproximações, especialmente quanto às médias dos construtos. No presente estudo, a média de *locus de controle* foi 4,47 e a de *motivação para se proteger* de 5,98, ambas medidas consideradas de moderada a alta. Esses valores indicam que os usuários de *Internet Banking* reconhecem sua responsabilidade na própria segurança e apresentam *motivação elevada* para adotar medidas de proteção, mesmo entre aqueles menos engajados.

Com base nos dados dos percentis de *locus de controle*, é possível destacar que a maior parte dos respondentes se considera responsável por se proteger contra fraudes bancárias online, em vez de transferir essa responsabilidade para o banco (*locus externo*). Os resultados de Jansen e van Schaik (2017) corroboram com os achados, que também evidenciaram médias elevadas nos construtos *Locus de Controle* e *Motivação de proteção*, demonstrando que, entre os usuários de *Internet Banking*, aqueles que acreditam ter controle sobre a sua própria segurança (*locus interno*), apresentam uma maior *motivação* para adotar uma medida de proteção recomendada.

Quanto à hipótese H2, que examina a relação entre *confiança* e *recomendação*, os dados indicam efeito moderado da *confiança* sobre a disposição do cliente em recomendar o banco. Contudo, Bashir e Madhavaiah (2015), apontaram uma relação mais baixa, entre as variáveis *confiança* e *intenção comportamental*, possivelmente em consequência da multidimensionalidade desse construto, que abrange a *intenção de uso no futuro do Internet Banking*, a *adoção na rotina* e a *recomendação do serviço*. Assim, a influência da *confiança* pode variar em cada aspecto analisado, mas com um efeito maior no comportamento de *recomendação*.

Sobre o resultado da correlação dos construtos *confiança* e *recomendação*, apesar de significativa, apresentou um valor associativo fraco. Em contraste, no estudo de Rezende *et al.* (2019) a correlação entre os construtos *confiança* e *fidelização dos clientes* indicou uma associação forte e significativa. Esse achado sugere que os clientes com uma opinião positiva sobre o valor do banco tendem a ter uma relação próxima e fiel.

Com relação à hipótese H3, a *confiança* também influencia moderadamente na disposição do cliente em continuar se relacionando com o banco. De forma semelhante, Hoffmann e Birnbrich (2012) indicaram que a *confiança* tem uma influência positiva e significativa sobre a *intenção de continuidade dos clientes*, só que numa variação mais baixa. Dessa maneira, os achados convergem para o entendimento de que o construto *confiança* é um fator relevante para a continuidade do relacionamento bancário.

Em síntese, o resultado da análise de covariância entre as variáveis *Recomendação* e *Continuidade* apresentou convergência com o estudo de Rahi, Alghizzawi e Ngah (2021), que confirmou a hipótese de que a *intenção de continuidade do usuário de Internet Banking* impacta positivamente a *intenção de recomendar o serviço*, sobretudo quando o cliente considera que a imagem institucional do banco transmite *confiança* e *segurança*. Diante dos achados discutidos, o próximo tópico apresenta as considerações finais deste estudo, destacando suas principais contribuições e implicações.

## 6 CONSIDERAÇÕES FINAIS

O estudo realizado teve como objetivo analisar como o contexto de fraude impacta na *intenção de continuidade* e *recomendação*, com base em aspectos de *segurança* e de *confiança* dos clientes sobre instituições financeiras. Para a sua fundamentação, foram levantadas cinco hipóteses que tiveram base na literatura existente sobre o tema, e que buscaram abordar as relações entre os construtos investigados.

Com relação a avaliação conjunta das hipóteses, por meio da modelagem de equações estruturais, as cinco hipóteses propostas, apresentaram valores estatisticamente significativos e se mantiveram influentes. Esse conjunto de análises permitiu que fosse alcançado o objetivo geral desta pesquisa, de investigar como o contexto de fraude afeta as percepções e comportamentos dos clientes em relação às instituições financeiras.

Assim, este artigo buscou contribuir teoricamente para a ampliação do debate acadêmico sobre os impactos das fraudes financeiras, pois evidencia que, dentre os três diferentes antecedentes da confiança, a percepção de segurança antifraude tem uma grande influência sobre a confiança dos clientes. Além de demonstrar que fatores psicológicos do consumidor, como o *locus* de controle e a motivação de proteção, também podem influenciar na confiança. Ademais, o estudo amplia a compreensão do efeito da confiança na recomendação e na continuidade para dentro do contexto de fraudes bancárias. Dessa forma, os resultados podem apoiar pesquisas futuras em marketing, principalmente aquelas voltadas à análise do comportamento do consumidor em situações de fraude.

No campo prático, os resultados podem auxiliar os bancos e instituições financeiras no desenvolvimento de estratégias eficazes de proteção e atendimento ao cliente, uma vez que os achados demonstraram a importância de que os clientes tenham conhecimento sobre as estratégias de proteção contra fraudes dos seus bancos. Nesse contexto, é importante que essas organizações invistam em sistemas de monitoramento, alertas de transações, autenticação em dois fatores e ofereçam orientações claras em seus canais de atendimento.

Essas iniciativas podem ter efeitos positivos na visão dos seus consumidores, uma vez que possibilitam aos usuários que participem ativamente do processo de proteção e se sintam amparados diante de qualquer tentativa de fraude que, infelizmente, possa acabar acontecendo com eles. À vista disso, recomenda-se que os bancos também direcionem a atenção às campanhas preventivas voltadas para os diferentes perfis de clientes, considerando que o conhecimento sobre segurança antifraude deve ser adaptado às necessidades de cada público e transmitido de forma objetiva pelos diversos canais de comunicação das instituições bancárias.

Sobre as limitações encontradas ao longo desta pesquisa, destaca-se a baixa participação de respondentes idosos (a partir dos 50 anos), que representaram apenas 10,6% da amostra. Além disso, observa-se a falta de diversificação do público quanto à localização geográfica, já que a maioria dos participantes (96,25%) era residente da região Nordeste. Com relação a possíveis sugestões de pesquisas futuras, elas podem abordar outros tipos de fraudes bancárias que estejam em evidência no país ou que estejam em destaque no site da Federação Brasileira de Bancos (FEBRABAN), bem como sugere-se que sejam realizadas pesquisas qualitativas para analisar quais são os sentimentos e consequências das fraudes no comportamento dos consumidores lesados.

Ademais, sugere-se que estudos futuros explorem a qualidade do suporte e do atendimento oferecidos pelas instituições financeiras em situações de fraude, considerando que esses aspectos podem exercer uma influência significativa sobre a confiança, a recomendação e a continuidade do relacionamento com os clientes. No campo das pesquisas quantitativas, recomenda-se o aprofundamento desse estudo por meio do cruzamento dos construtos analisados neste estudo com as variáveis sociodemográficas da amostra, com a finalidade de ampliar a compreensão dos resultados encontrados com as experiências de fraudes dos consumidores.

## REFERÊNCIAS

ALVES, Lara Elisa Justino *et al.* Engajamento de usuários brasileiros de bancos digitais. In: **ENCONTRO DA ANPAD – EnANPAD**. São Paulo, SP: Escola Superior de Agricultura Luiz de Queiroz, Universidade de São Paulo, 2023. DOI: <https://doi.org/10.21714/2177-2576EnANPAD2023>. Disponível em: <https://spers.pro.br/site/wp-content/uploads/2023/10/2023-ENANPAD-Engajamento-de-usuarios-brasileiros-de-bancos-digitais.pdf>. Acesso em: 15 abr. 2025.

AMIN, Muslim. Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. **International Journal of Bank Marketing**, [s. l.], v. 34, n. 3, p. 280-306, 16 maio 2016. DOI: <https://doi.org/10.1108/ijbm-10-2014-0139>. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/ijbm-10-2014-0139/full/html#abstract>. Acesso em: 16 abr. 2025.

ARIBAKE, Fadare Olusolade; MAT AJI, Zahurin. The mediating role of perceived security on the relationship between Internet Banking users and their determinants. **International Journal of Advanced Research in Engineering and Technology**, [s. l.], v. 11, n. 2, p. 296-318, 2020. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3553853](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3553853). Acesso em: 21 mar. 2025.

BANCO CENTRAL DO BRASIL. **Sistema de Pagamentos Brasileiro: Pix**. Gov.br. 2025. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix>. Acesso em: 7 abr. 2025.

BASHIR, Irfan; MADHAVAIAH, Chendragiri. Consumer attitude and behavioural intention towards Internet banking adoption in India. **Journal of Indian Business Research**, [s. l.], v. 7, n. 1, p. 67-102, 16 mar. 2015. DOI: <https://doi.org/10.1108/jibr-02-2014-0013>. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/jibr-02-2014-0013/full/html>. Acesso em: 11 mar. 2025.

BRANCO, D. C. Golpes no Pix: veja como funcionam as duas principais abordagens dos criminosos. **Canaltech**, [s. l.], 17 nov. 2021. Disponível em: <https://canaltech.com.br/seguranca/golpes-no-pix-veja-como-funciona-as-duas-principais-abordagens-dos-criminosos-201998/>. Acesso em: 7 abr. 2025

CABRAL, Daniel Barbosa; TORRES, Nancy Maria Correa. Satisfação e fidelização de clientes do setor bancário brasileiro. **Navus - Revista de Gestão e Tecnologia**, v. 9, n. 4, p. 195-205, 1 out. 2019. Disponível em: <https://doi.org/10.22279/navus.2019.v9n4.p195-205.929>. Acesso em: 27 jul. 2025.

COHEN, Jacob. Statistical Power Analysis for the Behavioral Sciences. 2. ed. Hillsdale, N.J: L. Erlbaum Associates, 1988. 567 p. *E-book*.

DANCEY, Cristina; REIDY, John. **Estatística sem matemática para psicologia**. (Métodos de pesquisa). 7. ed. Porto Alegre: Penso, 2019. E-book. pág.177. ISBN 9788584291434. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584291434/>. Acesso em: 08 set. 2025.

DINIZ, Rafael Elias. **Responsabilidades das instituições bancárias perante os danos causados por ataques cibernéticos**. 2021. Monografia (Graduação em Direito) — Fundação Educacional do Município de Assis (FEMA), Assis, São Paulo. 2021.

FERREIRA, Fernanda Alves. Os Serviços Internet Banking E A Sua Utilidade No Relacionamento Entre Cliente E Instituição Financeira. 2021. 61 p. **Dissertação de mestrado** — Universidade Estadual do Centro-Oeste – Unicentro, Guarapuava, 2021.

FIDELIS, Lucinele de Jesus. Avanços tecnológicos e os novos determinantes do uso expandido de assistentes virtuais em Mobile Banking. 2023. 49 f. Monografia (Graduação em Administração) — Universidade Federal de Ouro Preto, Mariana, 2023. Disponível em: <https://monografias.ufop.br/handle/35400000/6048>. Acesso em: 5 abr. 2025.

GANDRA, Alana. Pandemia aumenta acesso da população a serviços bancários. 19 jan. 2022. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2022-01/pandemia-aumenta-acesso-da-populacao-servicos-bancarios>. Acesso em: 15 jul. 2025.

GERBELLI, Luiz Guilherme. Pandemia acelera digitalização e bancos acirram briga por clientes. 10 jul. 2021. Disponível em: <https://www.google.com/amp/s/g1.globo.com/google/amp/economia/noticia/2021/07/10/pandemia-acelera-digitalizacao-e-bancos-acirram-briga-por-clientes.ghtml>. Acesso em: 14 jul. 2025.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 7. ed. Rio de Janeiro: Atlas, 2019. E-book. p.ii. ISBN 9788597020991. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788597020991/>.

GOLPE do Pix: veja quais são e saiba como se proteger. SPC Brasil, [s. l.], 03 set. 2024. Disponível em: <https://www.spcbrasil.com.br/blog/golpe-do-pix>. Acesso em: 03 mar. 2025.

GOLPES mais Comuns/ Antifraude. **FEBRABAN**, [s. l.], 2025. Disponível em: <https://portal.febraban.org.br/AntiFraude/>. Acesso em: 11 abr. 2025.

GONÇALVES, Lucca Merhy Arruda. **Responsabilidade civil em casos de fraudes digitais no setor bancário**. 2021. 80 f. Trabalho de Conclusão de Curso (Graduação em Direito) — Faculdade de Direito de Curitiba, Centro Universitário Curitiba, Curitiba, 2021. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/17830>. Acesso em: 5 abr. 2025.

HOFFMANN, Arvid O. I.; BIRNBRICH, Cornelia. The impact of fraud prevention on bank customer relationships. **International Journal of Bank Marketing**, [s. l.], v. 30, n. 5, p. 390-407, 20 jul. 2012. DOI: <https://doi.org/10.1108/02652321211247435>. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/02652321211247435/full/html#abstract>. Acesso em: 21 fev. 2025.

JANSEN, Jurjen; VAN SCHAIK, Paul. Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, [s. l.], v. 25, n. 2, p. 165-180, 12 jun. 2017. DOI: <https://doi.org/10.1108/ics-03-2017-0018>. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/ics-03-2017-0018/full/html>. Acesso em: 6 abr. 2025.

JANSEN, Jurjen. **Do you bend or break?** Preventing online banking fraud victimization through online resilience. 2018. 296 f. Doctoral thesis — Open Universiteit, Heerlen, 2018.

JR., Joseph FH.; PRETO, William C.; BABIN, Barry J.; e outros. *Análise multivariada de dados*. 6. ed. Porto Alegre: Bookman, 2009. E-book.

KOCH, Gustavo Duarte Waltereith. **Perfil de vítimas de golpes em uma instituição financeira**. 2022. 33 f. Monografia (Graduação em Administração) — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022.

LEITE, Maevy Andrade; CEO, Márcio. Gestão de Relacionamento com o Cliente: Uma Análise sobre Fidelização e Satisfação. RCMOS - **Revista Científica Multidisciplinar O Saber**, v. 1, n. 2, 25 nov. 2024. Disponível em: <https://doi.org/10.51473/rcmos.v1i2.2024.763>. Acesso em: 05 abr. 2025.

LOPES, Victor Ferreira. **Investigação e prevenção de crimes virtuais**: um estudo sobre phishing como ameaça digital. 2023. 61 f. Monografia (Graduação em Direito) - Centro Universitário Brasileiro (UNIBRA), Recife, 2023.

MADUREIRA, João Pedro Brandão. A era do pix: a responsabilidade objetiva das instituições financeiras sobre fraudes bancárias, uma análise à luz do código de defesa do consumidor. **Revista Direito UNIFACS – Debate Virtual**, n. 288, p. 1-11, 2024. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/8904>. Acesso em: 04 abr. 2025.

MAIS DE 500 mil brasileiros são vítimas de golpes bancários aplicados por celular em 2024. **Jornal Nacional**, [s. l.], 12 abr. 2025. Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2025/04/12/mais-de-500-mil-brasileiros-sao-vitimas-de-golpes-bancarios-aplicados-por-celular-em-2024.ghtml>. Acesso em: 15 abr. 2025.

MOURA WUST, E. F.; SORDI, V. F. Fraudes e golpes bancários no Brasil. Encontro internacional de gestão, desenvolvimento e inovação, 7., 2024, [s. l.]. **Anais [...]**. [s. l.]. Disponível em: <https://periodicos.ufms.br/index.php/EIGEDIN/article/view/20807>. Acesso em: 23. mar. 2025.

NASCIMENTO, Guilherme Afonso de Melo; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. A Importância do Combate à Desinformação e a Atualização do Código Penal para Crimes Virtuais de Engenharia Social/Phishing. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 11, p. 2225-2233, 30 nov. 2022. Disponível em: <https://doi.org/10.51891/rease.v8i11.7809>. Acesso em: 05 abr. 2025

NUNES, Danilo Arthur de Oliva. A responsabilidade eletrônica das instituições bancárias. **Revista Unifacs**, 2014. Disponível em: <http://www.revistas.unifacs.br/index.php/redu/article/download/3129/2252>. Acesso em: 05 abr. 2025

O QUE é engenharia social? Kaspersky, [s. l.], 25 fev. 2025. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering>. Acesso em: 14 abr. 2025.

OLIVEIRA, Rossimar Laura. Gestão de fraudes financeiras externas em bancos. 2012. **Universidade de São Paulo**, [s. l.], 2012. Disponível em: <http://www.teses.usp.br/teses/disponiveis/96/96132/tde-21122012-111004/>. Acesso em: 05 abr. 2025

PAULA, Gabriel Ferraz de. Digitalização financeira e o sistema financeiro brasileiro: impactos e evoluções nos meios e instrumentos de pagamento - 2019-2023. 2024. 63 p. Monografia — Pontifícia Universidade Católica de Goiás, Goiânia, 2024.

PEGORARO, Alexandre. **Qual a importância da tecnologia no combate às fraudes nas transações financeiras?** 14 nov. 2024. Disponível em: <https://kronoos.com/blog/qual-a-importancia-da-tecnologia-no-combate-às-fraudes-nas-transações-financeiras>. Acesso em: 15 abr. 2025.

PEROVANO, Dalton Gean. **Manual de metodologia da pesquisa científica**. 1. ed. Curitiba: Intersaberes, 2016. *E-book*.

PITHAGORAS, Fernando. Exclusão da responsabilidade dos entes bancários por supostas fraudes - Migalhas. 6 mai. 2025. Disponível em: <https://www.migalhas.com.br/depeso/429601/exclusao-da-responsabilidade-dos-entes-bancarios-por-supostas-fraudes>. Acesso em: 24 jul. 2025.

POLIDO, Gabriel Carvalho. **Estudo sobre fraudes digitais e o desenvolvimento de aplicativo para smartphones android e IOS para uso em palestras de sensibilização e esclarecimento**. 2023. 41 f. Monografia (Graduação em Ciência da Computação) - Universidade Estadual Paulista “Júlio de Mesquita Filho”, Bauru.

RAHI, Samar; ALGHIZZAWI, Mahmoud; NGAH, Abdul Hafaz. Factors influence user's intention to continue use of e-banking during COVID-19 pandemic: the nexus between self-determination and expectation confirmation model. **EuroMed Journal of Business**, 25 mar. 2022. Disponível em: <https://doi.org/10.1108/emjb-12-2021-0194>. Acesso em: 25 jul. 2025.

RAHI, Samar; GHANI, Mazuri Abd; NGAH, Abdul Hafaz. A structural equation model for evaluating user's intention to adopt internet banking and intention to recommend technology. *Accounting*, p. 139-152, 2018. Disponível em: <https://doi.org/10.5267/j.ac.2018.3.002>. Acesso em: 25 jul. 2025.

REIS, Victor Souza. **Inovação Bancária: um estudo cientrométrico sobre os avanços do Mobile banking**. 2018. 82 f. Monografia (Bacharelado em Engenharia de Produção) — Universidade de Brasília, Brasília, 2018. Disponível em: [https://bdm.unb.br/bitstream/10483/22963/1/2018\\_VictorSouzaReis\\_tcc.pdf](https://bdm.unb.br/bitstream/10483/22963/1/2018_VictorSouzaReis_tcc.pdf). Acesso em: 19 mar. 2024

RELATÓRIO de Fraude 2024: consumidores estão dispostos a pagar mais caro por segurança. 24 jun. 2024. Disponível em: <https://www.serasaexperian.com.br/conteudos/prevencao-a-fraude/relatorio-de-fraude-2024-consumidores-estao-dispostos-a-pagar-mais-caro-por-seguranca/>. Acesso em: 22 jan. 2025.

REZENDE, Gracielle Antunes Cangussú *et al.* Relação entre o Marketing de Relacionamento e a Fidelização de Clientes: um estudo no setor bancário. **Revista Eletrônica Gestão e Serviços**, [s. l.], v. 10, n. 1, p. 2648, 24 set. 2019. DOI: <https://doi.org/10.15603/2177-7284/regs.v10n1p2651-2675>. Disponível em:

<https://www.researchgate.net/publication/336164359>. Acesso em: 17 abr. 2025.

SANTOS, Katarine Oliveira Domiciano dos. As fraudes bancárias e a responsabilidade civil das instituições financeiras. 2023. 61 f. **Monografia** (Graduação em Direito) — Pontifícia Universidade Católica de São Paulo, São Paulo, 2023.

SILVA, Ana Jasmim Barbosa da; CEREWUTA, Pollyanna Marinho Medeiros. A responsabilidade civil das instituições bancárias por danos sofridos no golpe pix. **JNT- Facit Business and Technology Journal**, [s. l.], v. 3, n. 39, p. 71-90, 2022. Disponível em: <https://revistas.faculdefacit.edu.br/index.php/JNT/article/view/1942>. Acesso em: 2 mar. 2025.

SOMANCHI, Sriram; TELANG, Rahul. Security, Fraudulent transactions and Customer Loyalty: A Field Study. **International Conference on Interaction Sciences**, [s. l.], 2016. Disponível em: <https://aisel.aisnet.org/icis2016/ISSecurity/Presentations/10/>. Acesso em: 10 abr. 2025.

SOUZA, Leandro Miguel. Boca a boca é o principal fator de decisão dos jovens ao escolher um banco. **Startups**, [s. l.], 19 mai. 2022. Disponível em: <https://startups.com.br/negocios/boca-a-boca-e-principal-fator-de-decisao-dos-jovens-ao-escolher-banco/>. Acesso em: 16 abr. 2025.

SOUZA, Ronaldo. Prevenção de Fraudes Financeiras: Estratégias e Medidas de Proteção. **gov.br**, [s. l.], 28 ago. 2023. Disponível em: <https://www.gov.br/investidor/pt-br/penso-logo-invisto/prevencao-de-fraudes-financeiras-estrategias-e-medidas-de-protecao>. Acesso em: 15 abr. 2025.

TEIXEIRA, Raphaela Dias. **Tecnologias disruptivas no sistema bancário: fintechs e blockchain sob à ótica da inclusão financeira na era digital**. 2020. 66 f. Monografia (Bacharelado em Ciências Econômicas) — Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020. Disponível em: <https://pantheon.ufrj.br/bitstream/11422/15089/1/RDTeixeira.pdf>. Acesso em: 5 de abr. 2025.

UNES, Bárbara Vieira Junqueira; CAMIOTO, Flávia de Castro; GUERREIRO, Érico Daniel Ricardi. Fatores relevantes para a fidelização de clientes no setor bancário. **Gestão & Produção**, [s. l.], v. 26, n. 2, 2019. DOI: <https://doi.org/10.1590/0104-530x2828-19>. Disponível em: <https://www.scielo.br/j/gp/a/9WJCFswV4TfMv43tD3JTqjP/>. Acesso em: 16 abr. 2025.

VALENTIN NGOBO, Paul. Drivers of customers' cross-buying intentions. *European Journal of Marketing*, v. 38, n. 9/10, p. 1129-1157, set. 2004. DOI: <https://doi.org/10.1108/03090560410548906>. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/03090560410548906/full/html?skipTracking=true>. Acesso em: 20 abr. 2025.

YOUSAFZAI, Shumaila; PALLISTER, John; FOXALL, Gordon. Multi-dimensional role of trust in Internet banking adoption. **The Service Industries Journal**, [s. l.], v. 29, n. 5, p. 591-



605, maio 2009. DOI: <https://doi.org/10.1080/02642060902719958>. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/02642060902719958>. Acesso em: 6 abr. 2025.

ZOHORA, Fatema Tuz *et al.* Optimizing credit card security using consumer behavior data: Big Data and machine learning approach to fraud detection. **Frontline Marketing, Management and Economics Journal**, [s. l.], v. 04, n. 12, p. 26-60, 9 dez. 2024. DOI: <https://doi.org/10.37547/marketing-fmmej-04-12-04>. Disponível em: <https://www.researchgate.net/publication/386595242>. Acesso em: 16 abr. 2025.

**APÊNDICE A – Quadro dos construtos utilizados, itens e respectivas fontes**

| <b>Construtos</b>                             | <b>Autores</b>              | <b>Itens da escala</b>                                                                                                                                               |
|-----------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confiança                                     | Hoffmann e Birnbrich (2012) | Eu acredito que o meu banco é confiável.                                                                                                                             |
|                                               |                             | Eu acredito que o meu banco cumpre as promessas que me faz.                                                                                                          |
|                                               |                             | Eu acredito que eu posso confiar no meu banco o tempo todo.                                                                                                          |
|                                               |                             | Eu acredito que o meu banco está genuinamente preocupado com minhas necessidades.                                                                                    |
|                                               | Valentin Ngobo (2004)       | Eu acredito que o meu banco é confiável.                                                                                                                             |
|                                               |                             | Eu acredito que o meu banco cumpre as promessas que me faz.                                                                                                          |
|                                               |                             | Eu acredito que eu posso confiar no meu banco o tempo todo.                                                                                                          |
|                                               |                             | Eu acredito que o meu banco está genuinamente preocupado com minhas necessidades.                                                                                    |
| Segurança - Percepção da segurança antifraude | Aribake e Mat Aji (2020)    | Eu sei quais são as iniciativas de prevenção de fraudes desenvolvidas pelo meu banco.                                                                                |
|                                               |                             | Eu me considero bem-informado(a) sobre as ações antifraude do meu banco.                                                                                             |
|                                               |                             | Eu me sinto seguro(a) com as iniciativas de prevenção de fraudes do meu banco.                                                                                       |
| Segurança - Motivação para se proteger        | Jansen (2018)               | Eu sigo as regras de segurança do meu banco (por exemplo, “não compartilhe as suas senhas bancárias com ninguém”) para me proteger contra fraudes bancárias on-line. |
|                                               |                             | Eu estou disposto(a) a cumprir as orientações de segurança online do meu banco.                                                                                      |
|                                               |                             | Eu tenho certeza de que seguirei as regras de segurança sugeridas pelo meu banco.                                                                                    |
|                                               |                             | Eu tenho intenção de seguir as regras de proteção do meu banco contra fraudes online.                                                                                |
| Segurança - Locus de Controle                 | Jansen (2018)               | Eu considero que manter a segurança dos serviços de Internet Banking do meu banco está sob meu controle.                                                             |
|                                               |                             | Eu acredito que me proteger contra fraudes bancárias online está sob meu controle.                                                                                   |
|                                               |                             | Acredito que eu sou o principal responsável por me proteger contra fraudes bancárias online.                                                                         |
| Continuidade                                  | Hoffmann e Birnbrich (2012) | Mesmo se eu sofresse uma fraude bancária, eu ainda teria uma forte intenção de continuar um relacionamento com o meu banco.                                          |
|                                               |                             | Se eu enfrentasse uma fraude financeira, eu ainda teria uma forte intenção de permanecer com meu banco por um longo tempo.                                           |

|              |                                 |                                                                                                                                                              |
|--------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |                                 | Mesmo se eu fosse vítima de uma fraude bancária, eu ainda teria uma forte intenção de manter meus produtos atuais no meu banco.                              |
|              | Rahi, Ghani e Ngah (2018)       | Caso eu sofresse uma fraude bancária, eu ainda manteria meu vínculo com o meu banco.                                                                         |
| Recomendação | Rahi, Ghani e Ngah (2018)       | Eu teria a intenção de recomendar o uso dos serviços de internet banking aos meus amigos e familiares, independentemente de ter sofrido uma fraude bancária. |
|              |                                 | Eu definitivamente pediria aos meus amigos e familiares para usarem o serviço de internet banking, mesmo se eu tivesse sofrido uma fraude bancária.          |
|              | Rahi, Alghizzawi e Ngah (2022); | Eu teria a intenção de recomendar o uso dos serviços de internet banking aos meus amigos e familiares, independentemente de ter sofrido uma fraude bancária. |
|              |                                 | Eu definitivamente pediria aos meus amigos e familiares para usarem o serviço de internet banking, mesmo se eu tivesse sofrido uma fraude bancária.          |
|              | Bashir e Madhavaiah (2015)      | Eu recomendaria fortemente que outras pessoas usassem os serviços do Internet Banking oferecidos pelo meu banco, mesmo que eu sofresse uma fraude bancária.  |

## **APÊNDICE B – Termo de Consentimento Livre e Esclarecido**

Olá! Meu nome é Mayra Marinho, sou estudante de Administração na Universidade Federal da Paraíba (UFPB) e estou realizando uma pesquisa como parte do meu Trabalho de Conclusão de Curso (TCC), sob orientação da professora Dra. Diana Teixeira de Carvalho.

O objetivo deste estudo é analisar como experiências com fraudes bancárias impactam a sua relação com os bancos, especialmente nos aspectos de confiança, segurança, recomendação e continuidade.

Antes de começar, é importante que você saiba:

- Não há respostas certas ou erradas;
- As respostas são confidenciais e anônimas;
- Sua participação é voluntária, ou seja, você pode recusar-se a responder ou desistir de participar a qualquer momento.
- O tempo estimado para responder o questionário é de aproximadamente 4 minutos.

Os dados obtidos serão analisados de forma agregada e não individual, garantindo o sigilo, a privacidade e a confidencialidade.

Qualquer dúvida você poderá entrar em contato comigo, através do e-mail: [mayra.marinho@academico.ufpb.br](mailto:mayra.marinho@academico.ufpb.br).

Ao prosseguir com o questionário, você declara que tem mais de 18 anos, está ciente das informações acima e concorda em participar da pesquisa de forma voluntária. Você pode optar por encerrar sua participação no estudo a qualquer momento e por qualquer motivo.

Desde já, agradeço muito pela sua colaboração!

Declaro ter mais de 18 anos e concordo em participar da pesquisa:

- ( ) Eu concordo, começar o estudo
- ( ) Eu não concordo, não desejo participar do estudo

**APÊNDICE C – Instrumento de coleta de dados**

|                     |
|---------------------|
| <b>QUESTIONÁRIO</b> |
|---------------------|

**1. Qual o seu gênero?**

- a) ☐ Masculino
- b) ☐ Feminino
- c) ☐ Outro: \_\_\_\_\_

**2. Qual é a sua idade?**

- a) Entre 18 e 29 anos
- b) Entre 30 e 39 anos
- c) Entre 40 e 49 anos
- d) Entre 50 e 59 anos
- e) Acima de 60 anos

**3. Qual o seu último grau de escolaridade?**

- a) Ensino Fundamental Incompleto
- b) Ensino Fundamental Completo
- c) Ensino Médio Incompleto
- d) Ensino Médio Completo
- e) Ensino Superior Incompleto
- f) Ensino Superior Completo
- g) Pós-graduação Incompleto
- h) Pós-graduação Completo

**4. Qual é a sua renda pessoal mensal?**

- a) Até R\$ 1.518,00
- b) Acima de R\$ 1.518,00 até R\$ 2.000,00
- c) Acima de R\$ 2.000,00 até R\$ 3.000,00
- d) Acima de R\$ 3.000,00 até R\$ 5.000,00
- e) Acima de R\$ 5.000,00

**5. Você já foi vítima de alguma fraude bancária?**

(Por fraude bancária ou financeira, estamos nos referindo a casos em que alguém tentou/conseguiu roubar dinheiro de uma de suas contas bancárias ou tentou/conseguiu enganar você para enviar dinheiro a eles.)

- a) Sim
- b) Não

**Abaixo, você encontrará um breve texto que servirá de base para as afirmações apresentadas na próxima etapa do questionário:**

As fraudes bancárias afetam milhares de pessoas ao longo dos últimos anos e em muitos casos, as vítimas não percebem que sofreram um golpe, até o momento que descobrem o prejuízo financeiro. São exemplos de fraudes:

- **Phishing**, em que os criminosos usam e-mails falsos de empresas de confiança para obter os dados pessoais das vítimas;
- **Golpe no WhatsApp**, que envolve a clonagem da conta por meio do envio de códigos de SMS, o que acaba afetando os contatos próximos da vítima;

- **Golpe do PIX**, onde o fraudador induz a vítima a devolver uma suposta transferência bancária por engano;
- **Golpe da Falsa Central de Atendimento**, no qual o criminoso se passa por um funcionário do banco para capturar senhas e outras informações bancárias.

6. A seguir, apresentamos uma série de afirmações. Pedimos que você indique o grau de concordância com cada uma delas, utilizando a escala abaixo: **1 indica “Discordo totalmente” e 7 indica “Concordo Totalmente”**, e os demais valores indicam níveis intermediários de concordância.

|                                                                                                                                                                      |   |   |   |   |   |   |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|
| Eu acredito que o meu banco é confiável.                                                                                                                             | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu sei quais são as iniciativas de prevenção de fraudes desenvolvidas pelo meu banco.                                                                                | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Mesmo se eu sofresse uma fraude bancária, eu ainda teria uma forte intenção de continuar um relacionamento com o meu banco.                                          | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu teria a intenção de recomendar o uso dos serviços de internet banking aos meus amigos e familiares, independentemente de ter sofrido uma fraude bancária.         | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu sigo as regras de segurança do meu banco (por exemplo, “não compartilhe as suas senhas bancárias com ninguém”) para me proteger contra fraudes bancárias on-line. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu considero que manter a segurança dos serviços de Internet Banking do meu banco está sob meu controle.                                                             | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**7. Em quais desses bancos ou instituições financeiras você possui conta bancária?**

- a) Caixa Econômica Federal
- b) Bradesco
- c) Itaú
- d) Banco do Brasil
- e) Santander
- f) Sicredi
- g) C6 bank
- h) Nubank
- i) Inter
- j) Mercado Pago
- k) Outros: \_\_\_\_\_

**8. Em qual cidade/estado você reside? \_\_\_\_\_**

9. Continue a responder às questões, usando a mesma escala, **onde 1 indica “Discordo totalmente” e 7 indica “Concordo totalmente”**, e os demais valores indicam níveis intermediários de concordância.

|                                                                                                                            |   |   |   |   |   |   |   |
|----------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|
| Eu acredito que o meu banco cumpre as promessas que me faz.                                                                | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu me considero bem informado(a) sobre as ações antifraude do meu banco.                                                   | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Se eu enfrentasse uma fraude financeira, eu ainda teria uma forte intenção de permanecer com meu banco por um longo tempo. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu definitivamente pediria aos meus amigos e familiares                                                                    | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

|                                                                                             |   |   |   |   |   |   |   |
|---------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|
| para usarem o serviço de internet banking, mesmo se eu tivesse sofrido uma fraude bancária. |   |   |   |   |   |   |   |
| Eu estou disposto(a) a cumprir as orientações de segurança online do meu banco.             | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**10. Há quanto tempo você é cliente do seu banco ou instituição financeira, aproximadamente?**

- a) 1 ano
- b) 2 a 3 anos
- c) 4 a 5 anos
- d) 6 a 10 anos
- e) Mais de 10 anos
- f) Não sei

**10.** Continue a responder às questões, usando a mesma escala, onde **1** indica “**Discordo totalmente**” e **7** indica “**Concordo totalmente**”, e os demais valores indicam níveis intermediários de concordância.

|                                                                                                                                                             |   |   |   |   |   |   |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|
| Eu acredito que eu posso confiar no meu banco o tempo todo.                                                                                                 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu acredito que me proteger contra fraudes bancárias online está sob meu controle.                                                                          | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Mesmo se eu fosse vítima de uma fraude bancária, eu ainda teria uma forte intenção de manter meus produtos atuais no meu banco.                             | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu recomendaria fortemente que outras pessoas usassem os serviços do Internet Banking oferecidos pelo meu banco, mesmo que eu sofresse uma fraude bancária. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu tenho certeza de que seguirei as regras de segurança sugeridas pelo meu banco.                                                                           | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**11. Nos últimos meses, quantas vezes você foi vítima de algum tipo de fraude?**

- a) 1 vez
- b) 2 a 4 vezes
- c) 5 a 6 vezes
- d) Mais de 6 vezes
- e) Não fui vítima de fraude

**12. Indique qual das seguintes opções abaixo descreve melhor a fraude que você foi vítima nos últimos meses:**

- a) Pediram-me para confirmar dados bancários ou clicar em links recebidos por e-mail, o que me trouxe prejuízos financeiros posteriormente.
- b) Recebi mensagens ou ligações de alguém se passando por um atendente do meu banco, solicitando os meus dados para uma “verificação de segurança”. Após fornecer as informações, tive a minha conta bancária invadida e perdi dinheiro.
- c) Durante a compra de um produto, realizei uma transação bancária ou via PIX em um site não confiável e não recebi o produto.

- d) Recebi mensagens no WhatsApp de alguém fingindo ser uma empresa de confiança ou banco, e fui induzido(a) a compartilhar códigos de SMS ou realizar transferências bancárias com urgência.
- e) Recebi uma transferência PIX “por engano” e fui induzido(a) a devolver o valor para uma chave informada pelo suposto remetente, o que me gerou prejuízo duplo devido ao fraudador ter acionado o MED (Mecanismo Especial de Devolução).
- f) Durante a venda de um produto ou serviço, o suposto cliente enviou um comprovante de PIX falso, alegando ter feito o pagamento. Após ter liberado a pessoa, percebi que o valor não foi creditado na minha conta.
- g) Recebi mensagens no WhatsApp de alguém fingindo ser uma pessoa de confiança, e fui induzido(a) a realizar transferências bancárias com urgência.
- h) Eu sofri uma tentativa de fraude, mas identifiquei antes de sofrer prejuízo financeiro.
- i) Não sofri nenhuma das fraudes listadas / Sofri um tipo diferente de fraude.

**13.** Continue a responder às questões, usando a mesma escala, **onde 1 indica “Discordo totalmente” e 7 indica “Concordo totalmente”**, e os demais valores indicam níveis intermediários de concordância.

|                                                                                              |   |   |   |   |   |   |   |
|----------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|
| Eu me sinto seguro(a) com as iniciativas de prevenção de fraudes do meu banco.               | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu acredito que o meu banco está genuinamente preocupado com minhas necessidades             | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Eu tenho intenção de seguir as regras de proteção do meu banco contra fraudes online.        | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Caso eu sofresse uma fraude bancária, eu ainda manteria meu vínculo com o meu banco.         | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Acredito que eu sou o principal responsável por me proteger contra fraudes bancárias online. | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**15.** Nos últimos meses, quantas vezes você soube que pessoas próximas a você (amigos ou familiares) foram vítimas de fraudes bancárias, aproximadamente?

- a) 1 vez
- a) 2 a 4 vezes
- b) 5 a 6 vezes
- c) Mais de 6 vezes
- d) Não vi ninguém próximo ser vítima de fraude



## APÊNDICE D – Itens finais das escalas e medidas descritivas

### [CF] Confiança

| Itens                                                                                      | Média | Desvio |
|--------------------------------------------------------------------------------------------|-------|--------|
| [CONFI 1] Eu acredito que o meu banco é confiável                                          | 5,33  | 1,643  |
| [CONFI 2] Eu acredito que o meu banco cumpre as promessas que me faz                       | 5,17  | 1,753  |
| [CONFI 3] Eu acredito que eu posso confiar no meu banco o tempo todo                       | 4,57  | 1,804  |
| [CONFI 4] Eu acredito que o meu banco está genuinamente preocupado com minhas necessidades | 4,66  | 1,829  |

### [SP] Segurança - Percepção da Segurança Antifraude

| Itens                                                                                             | Média | Desvio |
|---------------------------------------------------------------------------------------------------|-------|--------|
| [SEG_PERC1] Eu sei quais são as iniciativas de prevenção de fraudes desenvolvidas pelo meu banco. | 3,69  | 2,110  |
| [SEG_PERC2] Eu me considero bem informado(a) sobre as ações antifraude do meu banco.              | 4,37  | 1,882  |
| [SEG_PERC3] Eu me sinto seguro(a) com as iniciativas de prevenção de fraudes do meu banco.        | 4,79  | 1,817  |

### [SM] Segurança - Motivação para se proteger

| Itens                                                                                                                                                                           | Média | Desvio |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------|
| [SEG_MOT1] Eu sigo as regras de segurança do meu banco (por exemplo, “não compartilhe as suas senhas bancárias com ninguém”) para me proteger contra fraudes bancárias on-line. | 6,33  | 1,240  |
| [SEG_MOT2] Eu estou disposto(a) a cumprir as orientações de segurança online do meu banco.                                                                                      | 6,34  | 1,196  |
| [SEG_MOT3] Eu tenho certeza de que seguirei as regras de segurança sugeridas pelo meu banco.                                                                                    | 6,24  | 1,330  |
| [SEG_MOT4] Eu tenho intenção de seguir as regras de proteção do meu banco contra fraudes online.                                                                                | 6,23  | 1,369  |

### [SC] Segurança - Locus de Controle

| Itens                                                                                                                | Média | Desvio |
|----------------------------------------------------------------------------------------------------------------------|-------|--------|
| [SEG_CONT1] Eu considero que manter a segurança dos serviços de Internet Banking do meu banco está sob meu controle. | 6,00  | 1,466  |
| [SEG_CONT2] Eu acredito que me proteger contra fraudes bancárias online está sob meu controle.                       | 6,01  | 1,431  |
| [SEG_CONT3] Acredito que eu sou o principal responsável por me proteger contra fraudes bancárias online.             | 6,01  | 1,411  |

**[CT] Continuidade**

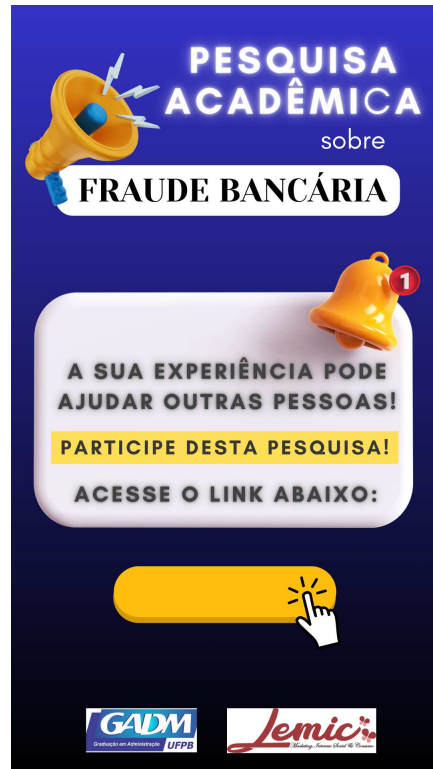
| <b>Itens</b>                                                                                                                              | <b>Média</b> | <b>Desvio</b> |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------|
| [CONTI 1] Mesmo se eu sofresse uma fraude bancária, eu ainda teria uma forte intenção de continuar um relacionamento com o meu banco.     | 5,45         | 1,777         |
| [CONTI 2] Se eu enfrentasse uma fraude financeira, eu ainda teria uma forte intenção de permanecer com meu banco por um longo tempo.      | 5,58         | 1,778         |
| [CONTI 3] Mesmo se eu fosse vítima de uma fraude bancária, eu ainda teria uma forte intenção de manter meus produtos atuais no meu banco. | 5,44         | 1,849         |
| [CONTI 4] Caso eu sofresse uma fraude bancária, eu ainda manteria meu vínculo com o meu banco.                                            | 5,49         | 1,836         |

**[RC] Recomendação**

| <b>Itens</b>                                                                                                                                                           | <b>Média</b> | <b>Desvio</b> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------|
| [RECOM 1] Eu teria a intenção de recomendar o uso dos serviços de internet banking aos meus amigos e familiares, independentemente de ter sofrido uma fraude bancária. | 5,62         | 1,875         |
| [RECOM 2] Eu definitivamente pediria aos meus amigos e familiares para usarem o serviço de internet banking, mesmo se eu tivesse sofrido uma fraude bancária.          | 5,46         | 1,918         |
| [RECOM 3] Eu recomendaria fortemente que outras pessoas usassem os serviços do Internet Banking oferecidos pelo meu banco, mesmo que eu sofresse uma fraude bancária.  | 5,57         | 1,886         |

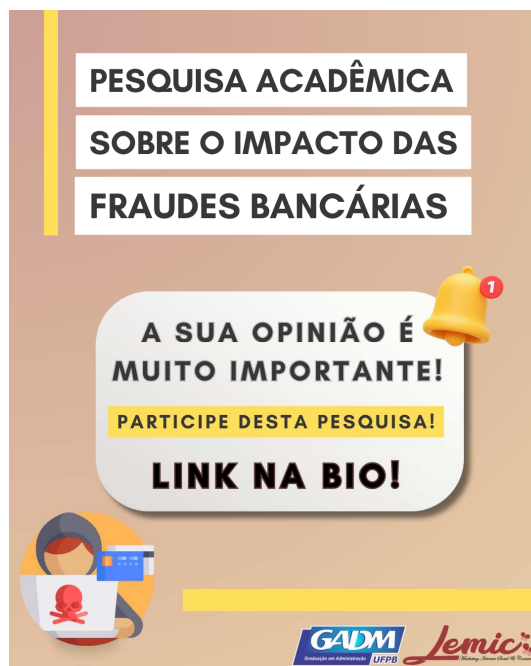
## APÊNDICE E – Convites para participação da pesquisa

Figura 3 – Convite compartilhado nos stories do instagram



Fonte: Elaborado pelo autor (2025)

Figura 4 – Convite compartilhado no feed do instagram



Fonte: Elaborado pelo autor (2025)