IGOR COSTA D'OLIVEIRA
PAULO HENRIQUE DINIZ FERNANDES

# **Negação plausível em sequestros relâmpagos:** implementação do modo pânico em aplicativos bancários.

São Paulo
2024

IGOR COSTA D'OLIVEIRA
PAULO HENRIQUE DINIZ FERNANDES

# **Negação plausível em sequestros relâmpagos:** implementação do modo pânico em aplicativos bancários.

Trabalho de Conclusão de Curso apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do título de Bacharel em Engenharia

Orientador: Prof. Dr. Marcos Antônio Simplício Júnior
Coorientadora: Profa. Dra. Yeda Regina Venturini

São Paulo
2024

# RESUMO

Este projeto de conclusão de curso foi desenvolvido na Escola Politécnica da Universidade de São Paulo (Poli-USP). A obra visa à implementação da negação plausível em sequestros relâmpagos para criar o modo pânico em aplicativos bancários e mitigar os danos causados por esse tipo de crime.

O avanço do sistema PIX no Brasil facilitou a transferência de recursos financeiros entre indivíduos, mas também intensificou os casos de sequestros relâmpagos. O Ministério Público e a Febraban destacaram a necessidade urgente de novas medidas para conter essa tendência. O objetivo principal é proteger os usuários contra acesso indevido a informações financeiras durante situações de emergência, como tentativas de acesso sob coação. O sistema proposto utiliza senhas alternativas e altera temporariamente os dados financeiros visíveis para mitigar riscos e aumentar a segurança bancária.

Implementado nos aplicativos móveis de instituições financeiras, o projeto visa não apenas proteger os clientes, mas também reduzir o impacto dos sequestros relâmpagos tanto para bancos quanto para usuários finais. Espera-se que esta pesquisa contribua para o campo da segurança cibernética em serviços financeiros, oferecendo uma abordagem inovadora para lidar com situações de risco extremo.

**Palavras-chave:** negação plausível, fricção programável, segurança usável, sequestros relâmpagos, segurança bancária

# ABSTRACT

This graduation project was developed at the Polytechnic School of the University of São Paulo (Poli-USP). The work aims to implement plausible deniability (repudiation) in lightning kidnappings to create a panic mode in banking applications and mitigate the damage caused by this type of crime.

The advancement of the PIX system in Brazil has facilitated the transfer of financial resources between individuals but has also intensified cases of lightning kidnappings. The Public Prosecutor's Office and Febraban have highlighted the urgent need for new measures to curb this trend. The main goal is to protect users from unauthorized access to financial information during emergency situations, such as attempts to access under duress. The proposed system uses alternative passwords and temporarily alters the visible financial data to mitigate risks and enhance banking security.

Implemented in the mobile applications of financial institutions, the project aims not only to protect customers but also to reduce the impact of lightning kidnappings on both banks and end-users. It is expected that this research will contribute to the field of cybersecurity in financial services, offering an innovative approach to dealing with extreme risk situations.

**Keywords**: plausible deniability, programmable friction, usable security, lightning kidnappings, banking security

# SUMÁRIO

# 1 INTRODUÇÃO

## 1.1 Histórico

A versão original do Código Penal brasileiro, promulgada em 1940, já incluía a tipificação do crime de extorsão mediante sequestro entre os delitos catalogados. Contudo, o conceito e a tipificação do chamado sequestro relâmpago surgiram mais recentemente.

Uma pesquisa no acervo digital da Biblioteca Digital da Fundação Biblioteca Nacional [1] revela que o termo "sequestro relâmpago" surgiu nos periódicos brasileiros pela primeira vez na década de 1990. Desde então, o *modus operandi* dos criminosos vem se adaptando às novas tecnologias desenvolvidas ao longo do tempo.

Os primeiros caixas eletrônicos (ATMs) chegaram ao Brasil na década de 1980, enquanto os cartões de crédito magnéticos surgiram um pouco antes. Contudo, essas tecnologias só se tornaram amplamente populares na década de 1990. A facilidade de realizar saques rápidos nos caixas eletrônicos foi, por muito tempo, explorada como um dos principais mecanismos de facilitação para os sequestros relâmpagos.

A Secretaria de Segurança Pública do Estado de São Paulo mantém em sua base de dados [2] todas as ocorrências criminais desde 1995. No entanto, o crime de sequestro relâmpago não era categorizado de forma específica. Sua tipificação no Código Penal ocorreu apenas em 2009, quando foi incluído na seção de extorsão. Antes disso, tais crimes eram geralmente investigados como roubos, embora já houvesse uma tendência entre os promotores de enquadrar os envolvidos na categoria de extorsão mediante sequestro [3].

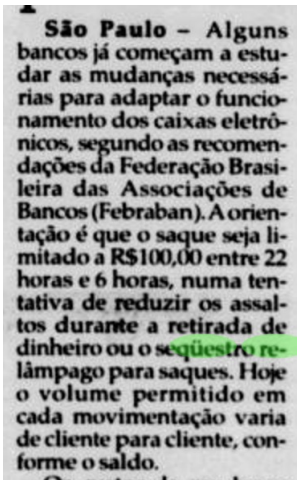

São Paulo – Alguns bancos já começam a estudar as mudanças necessárias para adaptar o funcionamento dos caixas eletrônicos, segundo as recomendações da Federação Brasileira das Associações de Bancos (Febraban). A orientação é que o saque seja limitado a R$100,00 entre 22 horas e 6 horas, numa tentativa de reduzir os assaltos durante a retirada de dinheiro ou o seqüestro relâmpago para saques. Hoje o volume permitido em cada movimentação varia de cliente para cliente, conforme o saldo.

**Figura 1 :** Excerto de solução proposta pela Febraban em 1997 no jornal *O Fluminense* para mitigar danos dos sequestros relâmpagos [4].

Embora as tecnologias tenham evoluído ao longo do tempo, a solução proposta pela Febraban para mitigar os danos causados pelos sequestros relâmpagos permanece a mesma. Como destacado em uma matéria de *O Fluminense* de 1997, ilustrada acima, a

recomendação era limitar o montante disponível para saques em determinados horários do dia, uma medida que continua sendo defendida até os dias de hoje.

### 1.2 Contexto atual

Mais recentemente, a pandemia da COVID-19 desempenhou um papel significativo nesse contexto, gerando um aumento recorde no uso e no registro de plataformas bancárias digitais. Até o final de 2021, cerca de 38 milhões de brasileiros aderiram a esses serviços pela primeira vez [5]. Esse movimento foi impulsionado tanto por necessidades pessoais quanto pelas demandas de consumo durante o período de quarentena, levando muitos a migrarem suas transações financeiras para o ambiente digital.

No final de 2020, a implementação do PIX foi um marco tecnológico importante nesse novo ambiente digital. As transações passaram a ser realizadas de forma muito mais ágil em comparação aos antigos TEDs e DOCs, além de serem irreversíveis. Contudo, essa agilidade também atraiu a atenção de criminosos, que passaram a explorar o PIX como uma oportunidade para obter dinheiro rapidamente em diversos delitos, incluindo sequestros relâmpagos.

Ao longo dos anos, as instituições financeiras investiram no desenvolvimento de novas ferramentas de segurança, como senhas exclusivas para diferentes dispositivos de acesso e autenticação por biometria digital e facial. Além disso, aprimoraram soluções já existentes, como a limitação de valores em transações, incorporando sistemas inteligentes. No entanto, essas iniciativas não foram suficientes para conter o aumento contínuo nos casos de sequestros relâmpagos.

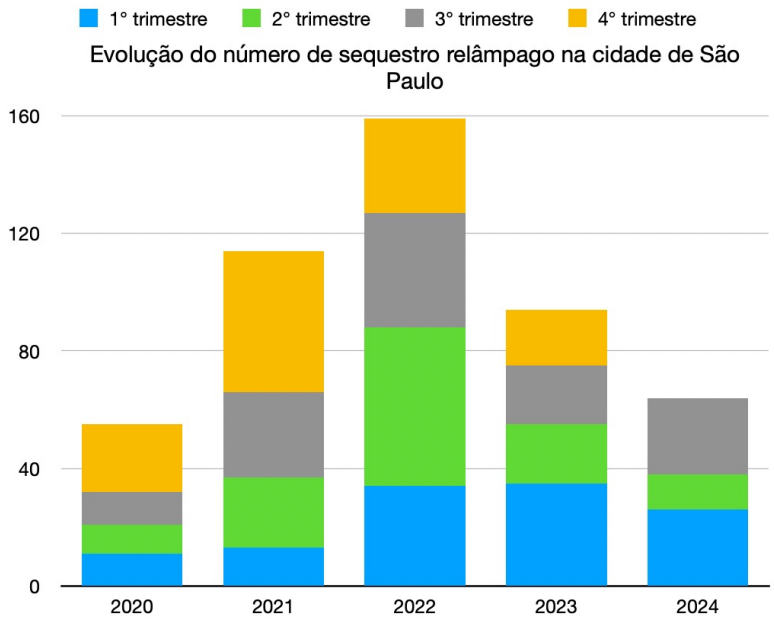



**Figura 2 :** Aumento dos casos de extorsão mediante sequestro na cidade de São Paulo [2].

### 1.3 Motivação

Conforme ilustrado na Figura 2, 2022 registrou o maior número de casos, com um valor absoluto três vezes superior ao de 2020. Já em 2021, houve uma duplicação de casos em comparação a 2020. Embora os anos de 2023 e 2024 apresentem números inferiores a 2022, ambos ainda permanecem significativamente acima dos registrados em 2020. Vale destacar que os dados de 2024 ainda não incluem os casos do último trimestre, visto que esta dissertação foi elaborada nesse período. Mesmo assim, os valores acumulados nos três primeiros trimestres de 2024 já superam o total de 2020.

Em 2023, o Ministério Público destacou a necessidade de desenvolver novas soluções para enfrentar esse problema. Uma das propostas seria a inclusão da geolocalização durante a realização de transações via PIX, com o objetivo de possibilitar a identificação do flagrante delito, conforme indicado pelo promotor Barone [6]. No entanto, em novembro de 2024, o BACEN ainda foca em políticas de segurança que se restringem apenas à limitação do montante das transações financeiras [7].

Quase 30 anos após a proposta de limitação das transações financeiras feita pela Febraban em 1997, o BACEN ainda mantém a mesma abordagem. Essa solução de segurança apresenta diversos inconvenientes para a usabilidade do usuário e não resolve efetivamente o problema. Este projeto surge justamente da necessidade de abandonar soluções arcaicas que não atacam o cerne do problema.

Os principais crimes realizados por meio dos aplicativos bancários estão detalhados na Tabela 1, a qual apresenta o tipo de crime conforme definido pelo Código Penal, o contexto em que ocorre, a forma de ameaça e as soluções atuais (A), bem como potenciais soluções futuras (S), discutidas posteriormente nesta dissertação. Este projeto visa apresentar soluções para o problema dos sequestros relâmpagos, situado na última linha da tabela 1.

Atualmente, duas principais abordagens estão sendo utilizadas com o intuito de mitigar esse tipo de crime. Uma delas consiste em monitorar o GPS do dispositivo da vítima durante a transação do PIX, identificando se a operação está sendo realizada em um local seguro e conhecido, como a residência do próprio usuário, que já possui um histórico de transações. Em caso de suspeita de fraude e de um possível sequestro, o gerente da conta é o responsável que entra em contato com as autoridades policiais informando a localização onde aconteceu o PIX.

A segunda abordagem é bloquear transferências para destinatários que possuem contas com baixa pontuação de confiança, geralmente associadas a contas recentemente criadas, possivelmente clonadas pelos golpistas para receber as transferências. Contudo, nenhuma das duas medidas se mostrou completamente eficaz na prevenção desse tipo de crime. Por isso, serão propostas as implementações de duas soluções: a solução por meio

| Crime | Cenário | Ameaça | Prevenção |
|---|---|---|---|
| Estelionato qualificado (Art. 171) | Controle parental, auxílio a idosos | Engenharia Social | (A) Quórum mínimo de aprovadores |
| Invasão de dispositivo informático | Invasão de Dispositivo (Art. 154-A) | Malware/cracker | (A) Dispositivos de segurança adicionais |
| Estelionato qualificado (Art. 171) | Criptoativos | Contrato vulnerável, engenharia social | (A) Prevenir transação p/ contratos com score baixo |
| Extorsão mediante sequestro (Art. 159) | Sequestro: condição ou pagamento para resgate | Coerção ("Sequestro premeditado") | (A) Segurança física |
| **Sequestro Relâmpago (Art. 157, § 2º, II)** | **Sequestro: curta ou longa duração para subtrair bens da vítima** | **Coerção ("Sequestro do Pix")** | **(A) Local não confiável (GPS) (A) Contas com score baixo (S) APP oculto (S) Solução Pânico** |

**Tabela 1 :** Mapa com os principais crimes com suas prevenções, com a ênfase para o sequestro relâmpago que delimita o escopo deste projeto.

do **aplicativo oculto** e outra que chamamos de **solução pânico**.

### 1.4 Objetivos Gerais

Tendo em vista esse problema real em aberto, este trabalho tem como objetivo maximizar a redução de danos do sequestro relâmpago utilizando o conceito da **negação plausível**. Para isso, é essencial garantir que o indivíduo sequestrado fique sob efeito coercitivo o menor tempo possível e que ele tenha o menor valor financeiro possível subtraído pelos sequestradores, tudo isso com o cuidado para que as soluções apresentadas não ameacem a integridade física da vítima que é o ativo mais importante deste projeto.

O desenvolvimento dessa ideia requer a implementação de um estado pânico nos aplicativos das instituições financeiras. Esse estado usará a negação plausível para garantir que os criminosos não possam distinguir o estado pânico do estado normal do aplicativo. Dessa maneira, nesse estado pânico alterações serão realizadas para atingir o objetivo da maior redução de danos possível.

## 1.5 Objetivos Específicos

Os objetivos específicos deste trabalho estão delineados a seguir e serão abordados de forma sequencial ao longo do desenvolvimento do projeto:

i. Mapear o sistema atual dos aplicativos bancários das instituições financeiras, com foco nas funcionalidades de segurança voltadas para situações de sequestro.

ii. Identificar as lacunas e os principais problemas presentes no sistema atual.

iii. Analisar os fatores determinantes que afetam a usabilidade dos aplicativos bancários em cenários de sequestro relâmpago.

iv. Definir os requisitos necessários e propor soluções tecnológicas que visem minimizar as perdas em casos de sequestro.

v. Desenvolver um Produto Mínimo Viável (MVP) para implementar as soluções sugeridas.

vi. Validar a eficácia do MVP em conformidade com os requisitos previamente estabelecidos.

## 1.6 Justificativa

Ao longo do tempo, o sistema financeiro vem aperfeiçoando o nível de segurança de seus sistemas. Com a maior utilização do sistema bancário de maneira digital (Internet Banking), foram criadas diferentes tipos de senha. Em geral, os bancos utilizam a senha com quatro dígitos para o cartão, seis dígitos para confirmação da transferência via aplicação e uma senha de oito dígitos para o acesso inicial ao aplicativo [8]. Variações entre as instituições financeiras existem, mas não mudam o cerne das ideias apresentadas.

Evidentemente que a criação desse conjunto de senhas não evitou a continuação de crimes. Qualquer indivíduo que possuísse esse conjunto de senhas poderia realizar todas as transações que desejasse pelo aplicativo. Para solucionar esse problema de autenticação do usuário, foi implementada a opção de validação biométrica, mais recentemente foi desenvolvida a biometria facial que agrega um nível extra de validação do usuário responsável pelas transações [9].

No entanto, nenhuma dessas tecnologias de autenticação resolve o problema de um indivíduo que está sob coação física (escopo desse trabalho). A solução pela negação plausível surge para responder essa demanda.

## 1.7 Organização do Trabalho

Este trabalho é organizado em seis tópicos principais, cada um contribuindo para uma compreensão abrangente e sistemática do projeto de engenharia proposto. A seguir,

são delineados os conteúdos que serão abordados em cada seção:

Na **introdução** é apresentado o histórico, os dados estatísticos, o contexto geral do projeto, delineando a importância e a relevância da pesquisa sobre negação plausível em sequestros relâmpagos. Serão destacados os objetivos, a motivação por trás do estudo e uma visão geral da estrutura do trabalho.

Os **aspectos conceituais** fornecerão um embasamento teórico sobre os conceitos fundamentais relacionados ao projeto, desde as propriedades fundamentais de segurança, até a conceituação de sequestro relâmpago. Esses conceitos-chave são essenciais para um bom entendimento das soluções e problemáticas apresentadas no projeto.

No **método de trabalho** é descrito o método utilizado para conduzir a pesquisa, incluindo abordagens de investigação, coleta de dados, ferramentas computacionais e experimentos planejados. Será detalhado como a metodologia escolhida será aplicada para alcançar os objetivos propostos.

Na **especificação de requisitos** definirá requisitos funcionais e não funcionais do sistema proposto, identificando as necessidades dos usuários, os cenários de uso e as restrições do projeto. Será elaborada uma lista completa e detalhada dos requisitos que o sistema deve atender.

No **desenvolvimento do trabalho** será apresentado o processo de implementação do sistema de negação plausível em sequestros relâmpagos, desde a concepção até a fase de testes e validação. Serão discutidas as etapas de desenvolvimento de software, algoritmos utilizados e decisões de design tomadas durante o processo.

Por último, nas **considerações finais** serão apresentadas as conclusões do trabalho, incluindo *insights* obtidos, contribuições para a área de estudo e possíveis direções para pesquisas futuras. Será feita uma reflexão sobre os resultados alcançados em relação aos objetivos inicialmente propostos.

## 1.8 Estado da Arte

No campo da segurança digital em sistemas bancários, o estado da arte revela algumas implementações de medidas preventivas contra crimes cibernéticos, embora poucos tenham sido especificamente direcionados aos sequestros relâmpagos.

Soluções adotadas pelos bancos, como autenticação multifatorial, criptografia avançada e sistemas de alerta precoce, têm sido exploradas para proteger os usuários contra acessos não autorizados e garantir a integridade das transações financeiras. Além disso, novas abordagens como a ocultação do aplicativo e/ou valores, ou ainda, a restrição de transações via PIX com base na localização do usuário, têm sido levantadas como resposta direta ao aumento dos crimes relacionados ao uso dessas tecnologias.

Nesse sentido, no final de 2022 o banco NuBank criou o “modo rua” [10]. Essa opção foi ofertada ao usuário com o intuito de limitar a quantia das transações fora de uma rede Wi-Fi pré-definida. No segundo semestre de 2024, a carteira digital PicPay criou o modo “seguro”, com as opções de saldos “protegido” e “invisível” [11]. Esse modo é parecido com o modo rua, mas utilizando geolocalização, ao invés da localização por uma rede Wi-Fi. As soluções apresentadas se limitam a restrição do pix ou a segurança por ocultação de serviços e valores, elas não usam o conceito de negação plausível em sua totalidade tal qual ela é exposta neste trabalho.

Vale destacar que as soluções apresentadas acima podem desencadear ações violentas por parte dos criminosos como demonstraremos neste trabalho e que somente a implementação correta da solução por negação plausível é capaz de mitigar. Vale pontuar que as instituições financeiras estão tentando achar soluções para os casos de roubo e furto, e em todas essas tentativas existe o entendimento que a coparticipação do usuário é necessária para melhor adaptação da solução, relacionando-se assim os conceitos de segurança usável e fricção programável.

Em 2024, alguns aplicativos têm sido utilizados para ocultar outros apps e proteger a privacidade no sistema Android, com destaque para o *App Hider*, *Hide It Pro* e *Vault*. Esses aplicativos permitem ocultar aplicativos sensíveis e arquivos pessoais por meio de senhas ou PINs, oferecendo uma camada adicional de segurança para os usuários [12]. No entanto, foram identificadas vulnerabilidades no uso dessas ferramentas. Por exemplo, ao buscar esses aplicativos na Play Store, eles ainda são visíveis, o que compromete parcialmente a discrição oferecida. Destaca-se que a opção de esconder os aplicativos é uma opção nativa em alguns tipos de celulares modernos.

Adicionalmente, aplicativos de segurança, como *Life360* e *bSafe*, ganharam destaque como mecanismos para proteger os usuários contra situações de risco, incluindo sequestros relâmpagos. Esses aplicativos oferecem funcionalidades como rastreamento em tempo real, envio automático de alertas de emergência e compartilhamento de localização com contatos de confiança, o que contribui para o aumento da segurança pessoal em contextos de emergência. No entanto, uma limitação importante é que, apesar de melhorarem a comunicação e rastreamento, nenhum deles oferece uma solução para evitar a subtração de valores financeiros de contas bancárias em momentos de risco.

A própria Febraban destaca a urgência de soluções adaptáveis, considerando que os principais usuários dessas ferramentas nem sempre possuem pleno domínio de sua utilização e frequentemente estão em estado emocional abalado durante um sequestro. Isso reforça a necessidade de respostas eficazes por parte das instituições financeiras e regulatórias para enfrentar essa problemática.

No início de 2023 o promotor Barone conversou com a Febraban sobre a impor-

tância de se adicionar a geolocalização nos aplicativos bancários como forma de coibir as ações de sequestro relâmpago [6]. No entanto, até o presente momento a Febraban e o Banco Central continuam com medidas de segurança que não abarcam diretamente o problema do sequestro relâmpago. Em Novembro de 2024, foram divulgadas novas medidas que envolvem mais restrição do montante do PIX envolvendo o tipo de dispositivo e o aperfeiçoamento da identificação de transações atípicas [13].

Nesse contexto, as soluções propostas neste projeto representam um grande avanço. Primeiro pelo uso da negação plausível em sua totalidade, o uso da geolocalização para identificação da localidade das transações e o aviso automático às autoridades policiais.

# 2 ASPECTOS CONCEITUAIS

## 2.1 Sequestro Relâmpago

Ainda no levantamento de requisitos deste projeto, foram feitas entrevistas com alguns atores envolvidos neste processo. Segundo o delegado de policia da delegacia anti-sequestro Rafael Guimarães Lodi, o **sequestro relâmpago** mudou o perfil nos últimos anos, se antes eles sequestravam o indivíduo para ir até caixas eletrônicos e retirar o dinheiro, hoje existem facilidades como o PIX que ajudam esse tipo de sequestro.

Ainda segundo o delegado, na cidade de São Paulo o público alvo tem sido homens vítimas do que se chama de "golpe do amor", nessas redes esses homens se expõe financeiramente, e portanto, cria-se uma expectativa alta de retorno do crime cometido por parte dos sequestradores. Após o sequestro e leitura dos dados bancários da vítima, normalmente ocorre a ratificação da expectativa inicial.

## 2.2 Serviços básicos de segurança

Dentre as propriedades básicas da segurança da informação, esse projeto trabalha diretamente com as propriedades da **Confidencialidade** e do **Não-repúdio**. Quanto às demais propriedades como disponibilidade, integridade e autenticidade, assume-se que funcionarão normalmente como no sistema atual.

### 2.2.1 Confidencialidade

A **Confidencialidade** possui dois vieses importantes. O primeiro trata da confidencialidade dos dados, os dados privados ou confidenciais não podem estar disponíveis para indivíduos não autorizados. O segundo trata do conceito de privacidade, que pode ser entendida também como confidencialidade das entidades, nela os indivíduos controlam quais informações relacionadas a eles podem ser coletadas e armazenadas e por quem e para quem essas informações podem ser divulgadas.[14]

A confidencialidade dos dados pode ser garantida eficientemente por criptografia (e.g., envio de dados por um meio não seguro) ou ainda pela negação plausível que não mostra os dados reais a um terceiro. O criminoso não pode ter a capacidade de discernir em qual modo o usuário está acessando o sistema, se os valores mostrados na tela são reais ou não, idealmente ele não deve saber nem mesmo se o usuário tem ambas as opções de login disponíveis.

### 2.2.2 Não-repúdio

O não-repúdio fornece garantia da origem ou entrega de dados, a fim de proteger o remetente contra a falsa negação por parte do destinatário de que os dados foram

recebidos, ou para proteger o destinatário contra a falsa negação por parte do remetente de que os dados foram enviados [15]. Alguns autores preferem tratar esse principio como parte de um princípio maior como auditabilidade [14].

### 2.2.3 Negação plausível

Stallings e Brown definem *Repudiation* como a situação em que "Um usuário nega o envio de dados ou um usuário nega o recebimento ou a posse dos dados" [14]. Alguns outros autores consideram a *Non-repudiation* (o contrário da *repudiation*) como uma propriedade básica de segurança.

A palavra *repudiation* pode ser traduzida como **negação plausível**. Nesse projeto, esse conceito é aplicado no caso onde o ator usuário pode negar o acesso dos seus dados no sistema a um terceiro, sem que esse terceiro saiba se o ator deu um acesso falso (modo pânico) ou verdadeiro (modo normal) ao sistema. Essa ideia será aplicada tornando indistinguível o modo pânico do modo normal do aplicativo bancário.

## 2.3 Segurança usável

Segurança usável refere-se ao design de sistemas que oferecem proteção robusta contra ameaças, mas de forma intuitiva e acessível, garantindo que os mecanismos de segurança não sejam tão complicados ou intrusivos que afastem ou confundam o usuário legítimo.

Whitten e Tygar em seu artigo *Why Johnny Can't Encrypt* definem que um software seguro é usável se os usuários: estão cientes das tarefas de segurança que necessitam executar, são capazes de descobrir como executar suas tarefas com êxito, não cometem erros perigosos e estão suficientemente confortáveis com a interface [16].

Portanto, o foco é criar soluções que não apenas protejam os dados e transações, mas também reduzam o esforço cognitivo e operacional necessário para utilizá-las. Exemplos já consolidados incluem autenticação biométrica fácil de usar, interfaces claras que ajudam a identificar atividades suspeitas e fluxos de navegação que não criem frustrações desnecessárias.

## 2.4 Fricção programável

Fricção programável é a introdução deliberada de barreiras ou etapas adicionais em processos de interação, ajustadas dinamicamente com base no nível de risco. Diferentemente de aplicar as mesmas medidas de segurança para todos os usuários e situações, a fricção programável permite respostas personalizadas e contextuais. Por exemplo, em uma transação considerada de alto risco, como o envio de dinheiro para uma conta desconhecida, o sistema pode exigir validação extra, como um código enviado por SMS ou

autenticação biométrica. Em transações de baixo risco, essas etapas podem ser omitidas, oferecendo uma experiência mais fluida.

## 2.5 Arquitetura MVC

A arquitetura MVC (Model-View-Controller) é uma abordagem de desenvolvimento de software que promove a separação de responsabilidades em um aplicativo. Desse modo, o sistema é dividido em três componentes principais: Modelo, Visão e Controlador. Essa divisão facilita a organização do código, tornando o sistema mais modular. Esse padrão arquitetural foi utilizado no desenvolvimento do protótipo deste projeto.

# 3 MÉTODO DE TRABALHO

## 3.1 Metodologia

O desenvolvimento deste projeto seguirá um processo comum em projetos de engenharia, guiado pela necessidade de mitigar os efeitos de sequestros relâmpagos. As fases deste processo são definidas com base nas características do sistema. Inicialmente, será realizado um levantamento dos requisitos do projeto, com foco na mitigação dos efeitos de um sequestro relâmpago. Os requisitos incluirão a redução do tempo de sequestro, minimização de agressões físicas e perdas financeiras da vítima.

Posteriormente serão definidas soluções para enfrentar os desafios identificados, fundamentadas no conceito de negação plausível. Por exemplo, o aplicativo poderá oferecer estratégias como ocultar o saldo real da vítima ao ativar o modo pânico, enviar a localização via GPS e ativar o microfone para auxiliar as autoridades policiais. Essas estratégias serão detalhadas nas fases subsequentes do projeto.

No desenvolvimento do protótipo, será adotada a arquitetura MVC (Model-View-Controller). O primeiro passo será a criação do modelo, responsável pela lógica de negócios do aplicativo. Essa etapa abrange a definição de esquemas de banco de dados, bem como a implementação de classes e métodos para acessar e manipular os dados.

Em seguida, será desenvolvida a visualização, responsável por apresentar os dados aos usuários. Essa fase envolve a criação das páginas do aplicativo móvel e a aplicação de conceitos de UI e UX, garantindo uma interface intuitiva, funcional e agradável.

Por fim, será implementado o controlador, que faz a ponte entre o modelo e a visualização. O controlador gerencia as entradas do usuário, aplica a lógica de negócios, atualiza o modelo conforme necessário e define rotas para diferentes telas do aplicativo, controlando como os dados são exibidos.

Por fim, com todas as partes principais implementadas, serão realizados testes e a depuração do sistema. Isso incluirá testes unitários, de integração e de aceitação para verificar o funcionamento correto dos componentes e garantir que o aplicativo atenda aos objetivos definidos no projeto.

# 4 ESPECIFICAÇÃO DE REQUISITOS

Após a pesquisa e análise do funcionamento dos sistemas bancários, foram elaborados casos de uso focados nos sistemas de autenticação, no acesso aos aplicativos atuais e no fluxo lógico em situações de sequestro. Esse processo aprofunda a compreensão do cenário atual, fundamenta o desenvolvimento dos requisitos do projeto e estabelece uma base sólida para a criação dos casos de uso das soluções propostas.

## 4.1 Sistema atual

Os casos de uso descritos são compostos pelos atores usuário, dispositivo móvel e banco, que interagem entre si para fornecer os serviços financeiros aos usuários. Adicionalmente outros atores como gerente, polícia e criminosos compõe com os atores anteriores os casos de uso durante a ação criminosa.

### 4.1.1 Casos de uso

A figura abaixo ilustra o caso de uso em que a vítima é o ator principal durante um sequestro. O fluxo lógico é conduzido pelas ações e decisões, geralmente guiadas pelos sequestradores, embora estes não estejam explicitamente representados no caso de uso.

Durante o sequestro, os criminosos iniciam uma investigação sobre a vida financeira da vítima, verificando se ela possui contas bancárias, qual é sua renda e quais características ou recursos estão associados às suas contas.

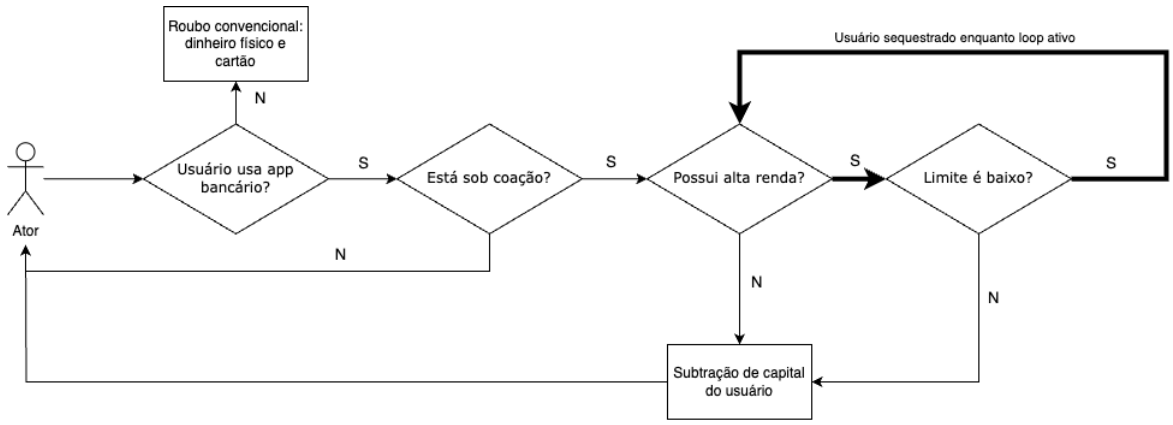



**Figura 3 :** Funcionamento atual.

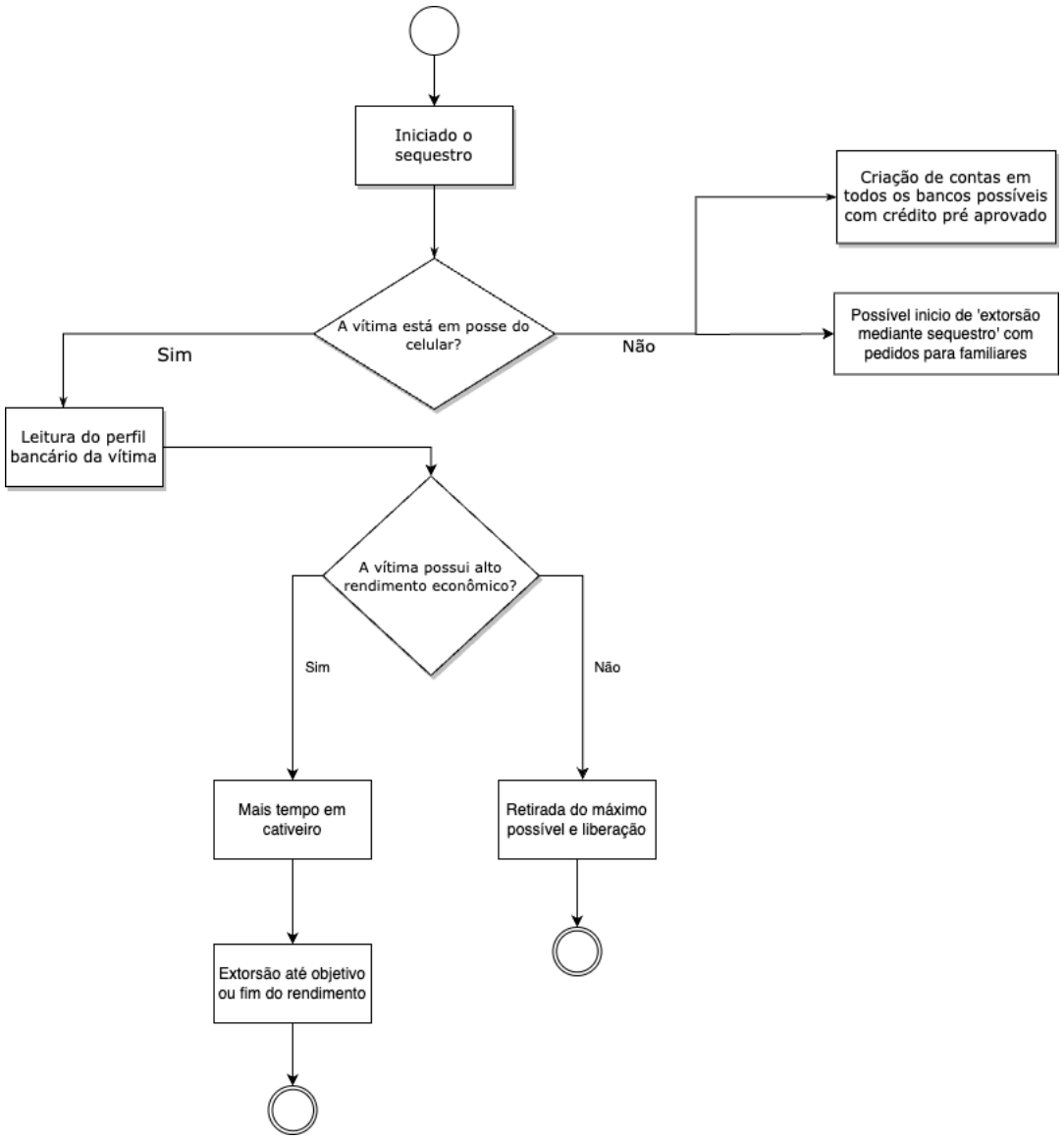



**Figura 4 :** Fluxograma das principais situações no sequestro relâmpago.

Após a investigação inicial, os criminosos avaliam o potencial de roubo dos ativos da vítima. Quando identificam um alto potencial econômico, como um saldo bancário elevado ou grandes investimentos, decidem prolongar o tempo de sequestro. O indivíduo de alto perfil permanece sob coação, como ilustrado no *loop* da seta em negrito na figura 3, até que o máximo possível de recursos seja subtraído.

Para potencializar a subtração de ativos, os criminosos recorrem a diversos mecanismos. Eles maximizam os limites de saques e transferências, resgatam antecipadamente todos os investimentos possíveis e solicitam empréstimos pré-aprovados automaticamente pelo banco. Em seguida, iniciam a subtração por meio de transferências via PIX para terceiros, pagamento de boletos, transferências de criptomoedas, entre outras ações.

A solução para mitigar o dano causado pela ação criminosa passa pela equação entre a expectativa inicial e o retorno obtido. No sequestro relâmpago, o perfil da vítima

é presumido antes da ação. Os criminosos avaliam o poder aquisitivo da vítima com base em indicadores como a região de captura, o tipo de veículo utilizado e até mesmo o nível de vestuário. Portanto, uma abordagem eficaz implica na criação de um perfil fictício que seja plausível para a vítima, mas que não revele informações reais.

Em certos casos, será imperativo ocultar detalhes, como os investimentos; em outras situações, simular valores inferiores aos reais, como nos créditos ou nos saldos (de contas correntes e poupanças), torna-se uma medida estratégica. Em geral, uma medida eficaz para todos os públicos é a de aumentar os gastos do usuário no modo pânico, mesmo usuários de alta renda que costumam ter alto fluxo de entrada, podem possuir também alto fluxo de saída e isso deve ser usado como forma de aumentar a verossimilhança do modo pânico com o modo normal.

### 4.1.2 Diagrama de acionamento policial

Atualmente, não há diferenciação no acesso entre o usuário legítimo e o sequestrador quando ambos possuem a senha de acesso ao aplicativo bancário. Em casos de transferências incomuns realizadas pelo cliente — como valores elevados ou transações para destinatários previamente identificados em fraudes — o sistema bancário pode acionar automaticamente o gerente. Caso o gerente considere necessário, ele pode acionar os órgãos de segurança pública.

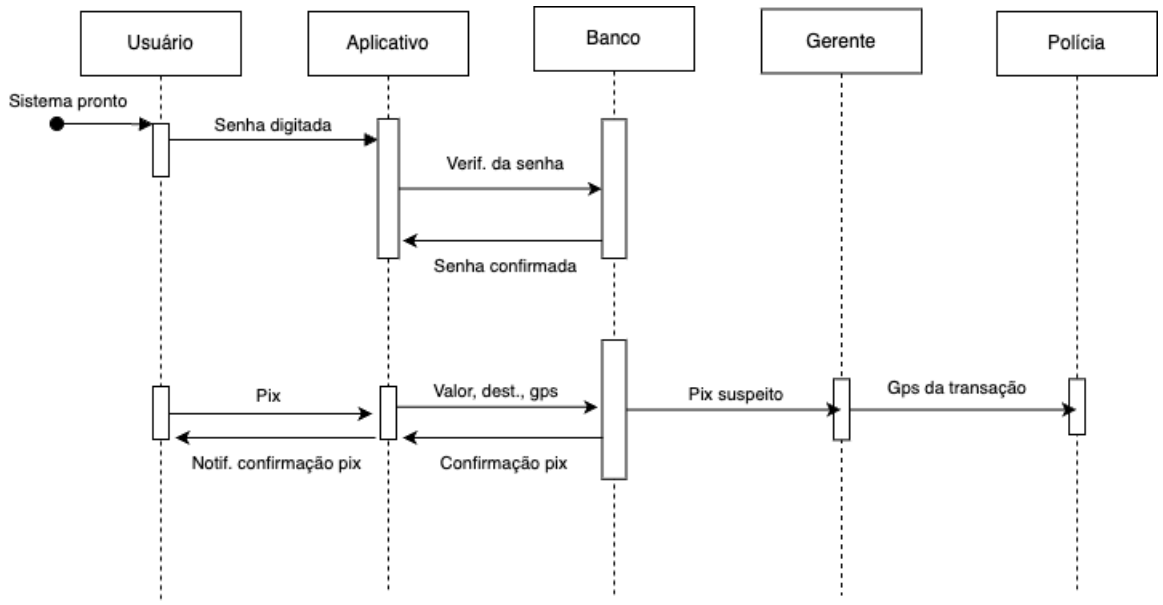



**Figura 5 :** Diagrama de sequência para o sistema atual de notificação do órgão de segurança em caso de fraude.

A figura acima apresenta um diagrama de sequência que demonstra o funcionamento atual. O ator usuário entra e faz login no aplicativo do banco, após isso ele está autorizado para realizar transferências de acordo com as especificações da sua conta. Se

a transferência de PIX ocorre como habitual, o gerente não precisa ser comunicado, mas em caso de discrepância com as suas transações normais, o gerente é acionado e ele pode contactar a polícia. Muitas vezes outra senha é pedida para a efetivação do PIX, mas a ideia central permanece a mesma.

Tendo em vista esse funcionamento, nem todas as transações via PIX feitas pelo sequestrador serão notificadas ao gerente, e mesmo em caso de notificação, cabe a um humano a decisão final de notificar os órgãos de segurança competentes. Nessas duas etapas muitas falhas podem acontecer, seja erro do sistema que identifica transferências não-usuais, seja pelo gerente que pode deixar escapar uma transferência numa situação de risco como o sequestro.

O cerne da solução deste projeto passa por um sistema de autenticação que reconheça a diferença e dê acesso a dois modos distintos para o mesmo usuário, o que chamamos de modo pânico e modo normal, e apesar das funcionalidades do aplicativo continuarem absolutamente iguais, alguns atributos da conta do cliente serão alterados. Além disso, o sistema bancário não armazenará somente a localização no momento do PIX, em caso de entrada no modo de pânico, o sistema bancário terá acesso à localização em tempo real do aparelho, a sua câmera e ao microfone.

## 4.2 Sistema com soluções propostas

### *Modus operandi* ideal com soluções

O esquema da figura abaixo segue o mesmo grau de abstração do esquema da figura 3, no entanto, aqui temos o fluxo de ações tendo em vista as implementações mostradas na tabela 1. As soluções modo pânico e ocultação do aplicativo levam ao objetivo geral de otimização da redução de danos: o usuário fica sob coerção o menor tempo possível e tem a menor soma de dinheiro subtraída.

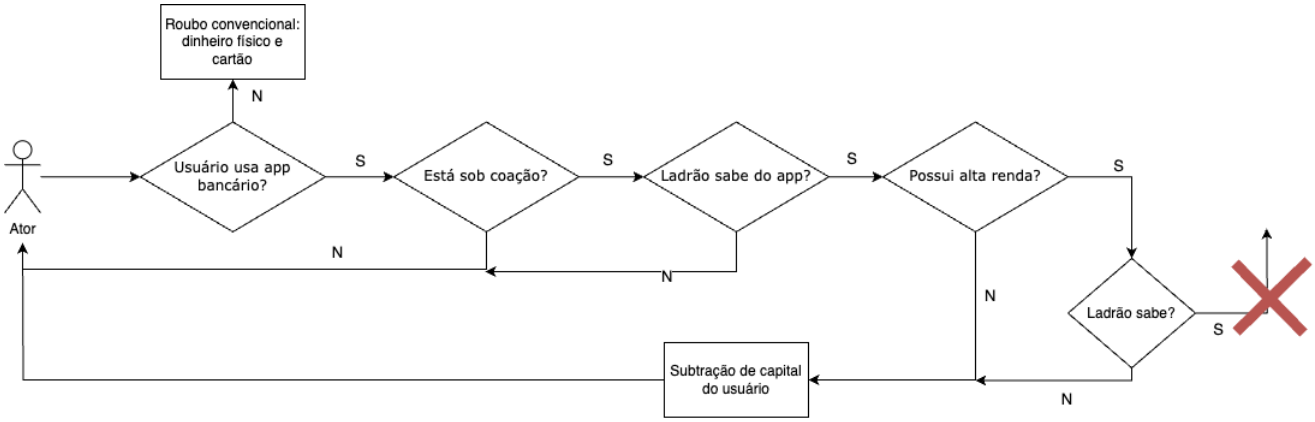



**Figura 6 :** Diagrama do funcionamento de um sequestro com soluções em funcionamento.

### 4.2.1 Ocultação do aplicativo

A pergunta "Ladrão sabe do app?" consiste na solução de ocultações dos aplicativos bancários, se o criminoso não sabe da existência do aplicativo, teoricamente ele não irá tentar coagir a vítima a entrar no sistema bancário. Em teoria nenhuma nenhuma soma de dinheiro é subtraída.

No entanto, de acordo com o delegado Lodi, nos casos em que as vítimas não possuem contas bancárias ou têm contas apenas em determinados bancos, os criminosos costumam criar novas contas em instituições nas quais a vítima não tenha vínculo. Se a vítima possui alto poder aquisitivo e boa renda em outros bancos, ele provavelmente terá crédito pré-aprovado no novo banco.

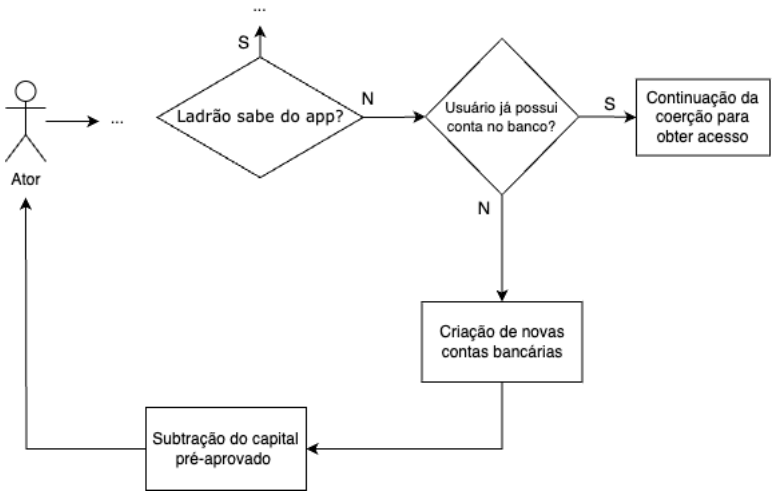



**Figura 7 :** Sequência da ocultação dos aplicativos.

As consequências dessa situação são extremamente graves tanto para os bancos para o usuário. Muitas vezes a vítima só toma conhecimento de que possui uma dívida no novo banco meses após o sequestro, quando começam a chegar as faturas.

A solução pela ocultação do aplicativo possui dois principais tipos de riscos que acontecem no momento em que o criminoso tenta criar uma nova conta bancária para realizar empréstimos pré-aprovados no nome da vítima. O primeiro acontece se vítima já possuir conta e o banco notificar que ela já é seu cliente, a solução da ocultação não funcionou e a extorsão continua. O segundo caso é quando a vítima realmente não é seu cliente e o banco abre uma conta em seu nome e libera um crédito pré-aprovado, é necessário buscar uma solução para a não permissão de empréstimos em seu nome.

Para solucionar o primeiro risco, não se deve dar indícios que o usuário já possui conta naquela instituição financeira. Caso o usuário já tenha um cadastro de conta com modo pânico, é preferível que se deixe criar a nova conta, no entanto, sem saldo disponível para empréstimo ou com valor de empréstimo imediato muito baixo. É possível deixar o

perfil em análise de crédito por “30 dias úteis” o que frustrará a continuação do golpe.

Já no segundo caso, uma forma de mitigar seria com um sistema interoperável de comunicação entre os bancos. Os usuários que possuem contas com modo pânico podem decidir no momento da personalização de sua conta pânico, em negar crédito facilitado de maneira automática por outras instituições financeiras. Além disso, esse sistema interoperável poderia ativar o modo pânico em todas as contas bancárias do cliente de uma vez só, protegendo assim todas as contas ao mesmo tempo. A comunicação entre as instituições financeiras é essencial nesta solução.

No segundo caso, ainda há a possibilidade de transferir o risco. A instituição financeira, ao permitir que o usuário personalize sua conta pânico, oferece, por meio de sua seguradora, um seguro anti-sequestro que cobre esse tipo de dano patrimonial, com extensões para seguro de vida e outras coberturas relacionadas.

**Soluções multifator**

### 4.2.2 Token/tag NFC

Para os usuários de altíssima renda, é razoável existir um nível de autenticação a mais. Propõe-se um modo que chamamos de *“daily”* em que ele poderia usar normalmente sem acionamento da polícia, mas com todos os valores de renda e investimento mais abaixo por padrão. No *“daily”* ele poderia realizar seus gastos do dia a dia.

No caso em que ele precise entrar no modo normal, ele usaria um token ou uma tag NFC. Sem esse token/tag, ele só poderia acessar o modo pânico ou o modo *“daily”*. Essa solução é uma solução que envolve autenticação multi-fator, incluindo algo que ele possui com algo que ele sabe.

Dentre as soluções existentes atualmente, a solução “modo rua” do Nubank não oculta ou altera os valores de saldos e investimentos do usuário, ela apenas altera o valor de transferência limite para regiões fora de um Wi-Fi designado seguro pelo usuário. No nosso modelo, o modo “daily” faria essas alterações.


**Figura 8 :** Celular com token inserido na entrada para validar autenticidade do usuário. No caso da tag NFC, apenas a aproximação é suficiente.

### 4.2.3 Custodiante

Uma outra solução envolve a autorização de um custodiante. Esse custodiante pode ter duas atribuições (não exclusivas): autorizar a autenticação da conta do usuário ou validar a transação financeira.

Inicialmente, essa abordagem é vista como uma alternativa para auxiliar os idosos ou ainda como uma medida contra a engenharia social. Contudo, ela também pode ser eficaz na prevenção de perdas financeiras substanciais em casos de sequestro relâmpago. Por exemplo, se um casal configurar previamente a necessidade de autorização do cônjuge para transferências superiores a 10 mil reais, é possível impedir o roubo de valores acima desse limite pré-estabelecido.

Da mesma forma, em cenários em que o acesso à conta conjunta ou à conta no modo normal dependa da autorização de ambos os celulares, essa medida pode evitar ações fraudulentas durante uma situação de risco. Essa solução também poderia ser usada em contas empresariais onde todos os sócios teriam que autorizar o acesso ou transferências relacionadas a conta da pessoa jurídica.

### 4.2.4 Modo pânico

O acesso negado ao sim na pergunta “Ladrão sabe?” da figura 6 pode ser feito pela aplicação da solução pânico. O modo pânico nega ao criminoso a possibilidade de confirmar a renda da vítima, ele nunca saberá se o que está observando no aplicativo é a situação real da vítima ou se é o modo pânico em ação.

Os criminosos saberem da existência da solução pânico não altera a eficiência de seu funcionamento, pois somente o usuário tem a capacidade de saber se ele possui ou não essa solução, ou ainda, se essa solução está ativa ou não naquele momento. O termo negação plausível vem da possibilidade da vítima poder negar acesso do modo normal ao criminoso sem que o criminoso saiba qual modo está acessando.

Para o caso em que a vítima entre no modo pânico e o criminoso suspeite que não é a verdadeira conta, de nada adiantará coagir a vítima a colocar a outra senha, pois os valores disponíveis para roubo irão diminuir a cada troca de senha. O estado pânico permanecerá como o status fixo do sistema e não retornará enquanto o dono da conta não for em segurança numa agência física reverter esse status da sua conta.

**Autenticação e modo pânico**

Em geral, os sistemas bancários tem duas senhas principais, a senha para o acesso ao aplicativo com 8 ou 6 dígitos dependendo do banco, e a senha forte de validação da transação bancária, em geral de 6 dígitos. Para ativação do modo pânico, o usuário teria uma senha alternativa para cada uma delas. Chamaremos de senha fraca a senha de

entrada no aplicativo, a senha forte para a senha de validação de transação financeira e as senhas alternativas para as senhas fracas e fortes que ativam o modo pânico. A tabela abaixo descreve o funcionamento dos casos de uso.

| **Caso** | **Ação** |
|---|---|
| Uso das senhas alternativas fraca e forte | Ativação do modo pânico com todas as suas funcionalidades características. |
| | Após a utilização da senha alternativa forte para validar a transação, será gerado um alerta máximo de intrusão. |
| Uso apenas da senha alternativa fraca | Ativação do modo pânico com todas as suas funcionalidades características, enquanto o sistema inteligente de verificação de usuário utiliza outros parâmetros para a tomada de decisão em relação à intervenção policial. |
| Uso apenas da senha alternativa forte | Perfil pânico **não** é ativado. Começo do registro de dados de câmera, áudio e GPS. O sistema inteligente irá decidir com esses e outros parâmetros alertar ou não as autoridades policiais. |

**Tabela 2 :** Descrição dos casos de utilização de senhas alternativas.

Dada a ativação do modo pânico, a senha de acesso ao modo normal ainda continua válida. No entanto, em caso de acesso à conta por meio da senha normal após um uso da senha alternativa, os valores de renda serão ainda mais baixos que os do primeiro acesso. Explica-se: a vítima entra em sua conta no modo pânico, alega ao criminoso que aquela é sua conta no modo normal, o caso em que o criminoso insiste para a vítima coloque a segunda senha, deve-se baixar ainda mais os valores como se a senha normal ativasse então o modo pânico.

Dessa forma, a vítima sempre poderá afirmar que entrou a primeira vez no modo normal (mesmo que não seja verdade). O criminoso nunca poderá validar essa informação. A partir do momento em que esse *modus operandi* for estabelecido e conhecido pelos criminosos, eles serão obrigados a se contentar com o montante disponível no primeiro acesso já que um segundo login com outra senha sempre resultará na redução do valor disponível para roubo e não permitirá que ele retorne ao valor exibido no primeiro acesso.

É costumeiro a realização da primeira autenticação pela biometria digital cadastrada para destravar o celular. Considerou-se a possibilidade de designar apenas um dedo como autenticador real do sistema, enquanto os demais ativariam o modo pânico. No entanto, essa abordagem apresenta um problema: na prática, a maioria dos usuários utiliza apenas dois dedos para essa função, geralmente o indicador ou o polegar. Além do que, mesmo escolhendo um dedo aleatoriamente, a probabilidade de 10% para acessar o modo normal ainda seria muito alta.

Uma solução proposta seria a inclusão de uma etapa anterior à leitura da digital. Antes de posicionar o dedo no leitor, o usuário desenharia na tela um número ou uma

letra, sem que o desenho fosse exibido. Caso essa etapa fosse ignorada ou realizada incorretamente, o modo pânico seria ativado. Com esse artifício, seriam adicionadas 36 novas possibilidades, e, combinadas com a digital, a probabilidade de uma combinação aleatória acessar a conta real do usuário seria reduzida para menos de 0.3%. Para efeito de comparação, a NIST SP 800-63B estabelece que um sistema biométrico deve trabalhar com uma taxa máxima de falha de 0.1%. Provando-se assim uma ordem de grandeza razoável para a solução proposta.

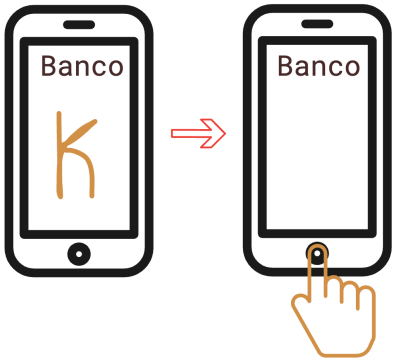



**Figura 9 :** Autenticação com letra/número mais digital para a entrada na conta real do usuário.

Solicitar duas entradas aumentaria significativamente a segurança. Contudo, isso prejudicaria a experiência do usuário, contrariando o conceito de segurança usável. No entanto, outras combinações de fatores e métodos de autenticação são possíveis e podem resolver o problema.

Neste projeto específico, as biometrias digital e facial não resolvem o problema do sequestro relâmpago, pois a vítima está fisicamente sob coerção no local. Além disso, a NIST SP 800-63B evidencia que a biometria, seja qual for, não deve ser usada isoladamente, devendo sempre ser combinada com outros fatores de autenticação, mesmo em situações normais de não perigo.

### Funcionamento do modo pânico

Após a primeira autenticação com a senha alternativa fraca, duas ações simultâneas são acionadas no sistema. A primeira é a *ativação do perfil de pânico coerente*, que corresponde ao perfil do usuário com a modificação dos parâmetros. A palavra "definitiva" no diagrama é utilizada para enfatizar que, uma vez que o sistema entre nesse estado, ele permanecerá assim até ser desativado presencialmente em uma agência bancária.

Simultaneamente, o sistema entra em estado de alerta e inicia a criação de um dossiê, que inclui logs, dados de localização e outras informações relevantes. Nesse está-

gio, a polícia pode ser acionada automaticamente por um sistema, sem a necessidade de intervenção do gerente, como ocorre atualmente.

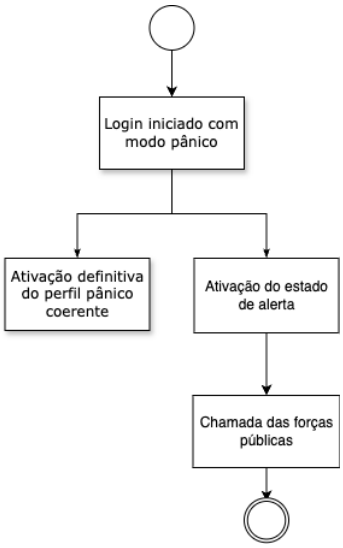



**Figura 10 :** Diagrama de alto nível desde a autenticação do modo pânico até o chamado das forças públicas de segurança.

### Ativação definitiva do perfil pânico

Na ativação definitiva do perfil pânico coerente, um perfil secundário verossímil com o usuário é mostrado na interface do aplicativo. Nesse perfil são realizadas algumas alterações, dentre elas podemos citar: um saldo mais baixo, sem ou com valores de investimentos bem abaixo dos reais, extrato e histórico de transações de acordo com esse perfil de nova renda, um crédito disponível reduzido de acordo com essa nova renda, aumento da fatura do cartão, PIX limitado de maneira coerente e seguros ofertados de acordo com o perfil.


**Figura 11 :** Alterações principais realizadas no perfil do usuário.

Dentre essas características, algumas deverão ser imputadas pelo usuário, enquanto outras serão automaticamente calculadas pelo banco, utilizando seu sistema, como ocorre atualmente na criação de contas. Por exemplo, imagine um perfil de alta renda, como o de um pequeno empresário que recebe cerca de 60 mil reais por mês, possui investimentos totalizando 1,5 milhão de reais e saldo disponível de 200 mil reais. Esse perfil poderia ser facilmente disfarçado com um perfil que oculta os investimentos, com as mesmas entradas de 60 mil, mas com alto fluxo de saída de capital, seja com cartão, empréstimos, compras etc, o que resultaria num saldo bem abaixo dos 200 mil reais que estariam à mercê dos criminosos. O aumento dos gastos do usuário é a melhor forma de deixar mais verossímil o perfil pânico.

**Construção do perfil pânico**

O perfil pânico deve ser verossímil, mas isso varia consideravelmente de pessoa para pessoa. Uma automatização completa na criação desses perfis poderia comprometer drasticamente a segurança do sistema, pois tornaria evidente que ele está no modo pânico. Além disso, quando o usuário está sob coação, ele pode ser questionado pelos criminosos sobre seus gastos, saldos e investimentos. Se as informações não corresponderem à ordem de grandeza do perfil de pânico, isso aumentaria o risco de identificação da ativação do modo pânico.

Para resolver isso, a proposta é que o próprio usuário defina alguns parâmetros iniciais de sua conta pânico, especialmente relacionados aos seus gastos. Se ele configurar sua conta pânico com rendimentos semelhantes aos reais, mas com o cartão de crédito no limite, empréstimo consignado realizado, histórico de despesas como pensão alimentícia para filhos e outros gastos, será muito mais plausível que os criminosos acreditem no saldo reduzido que verão nesse modo.

Como pode ser observado no esquema abaixo, a fonte de renda também pode ser escolhida pelo usuário. No entanto, essa escolha deve ser feita de maneira cautelosa e restrita a um público específico. Por exemplo, muitas vezes é possível saber, ou pelo menos estimar, quanto uma pessoa ganha (como no caso de um servidor público, com base na Lei de Transparência), mas é impossível estimar com exatidão quanto essa pessoa gasta.

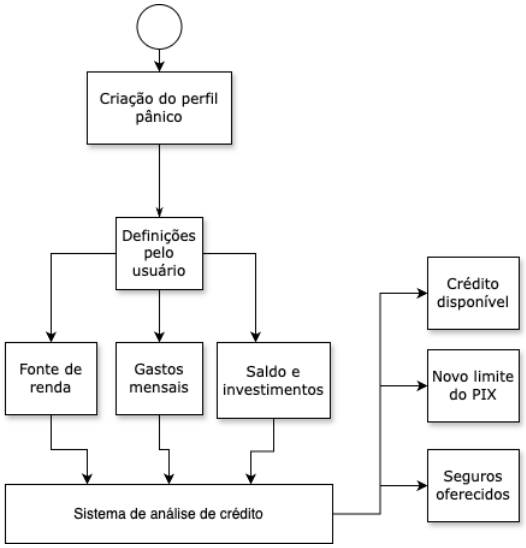



**Figura 12 :** Etapas para a construção do perfil pânico.

Os outros parâmetros serão gerados automaticamente pelo sistema. Em posse dos dados fictícios, o sistema calculará o crédito oferecido para esse cliente, dará um novo limite de PIX diário, os seguros e outros serviços oferecerão outros planos com base no novo perfil.

No final, o sistema contará com três perfis distintos para o usuário: um perfil normal (com os valores reais) e dois perfis de pânico (um com valores abaixo do real e outro ainda mais reduzido). O perfil normal será exibido enquanto o usuário não ativar a senha pânico. Ao utilizar a senha pânico, o sistema entrará no primeiro modo de pânico, bloqueando a conta nesse estado enquanto essa senha for utilizada para acessá-la.

Posteriormente, no caso do usuário alterar para a senha normal, o sistema automaticamente ativará e restará no segundo modo de pânico, exibindo um perfil com valores ainda mais baixos que os anteriores. Esse *modus operandi* faz parte da solução para coibir que os criminosos forcem a vítima a inserir outra senha além da primeira.

**Ativação do estado de alerta**

Dado a ativação do estado de alerta, o sistema começa a criar um dossiê que será salvo no banco de dados da instituição financeira e só será enviado para a policia após determinação de um *sistema inteligente de identificação do usuário*, que baseado em um sistema de pontuação determinará a probabilidade do usuário não ser o verdadeiro dono da conta acessada.

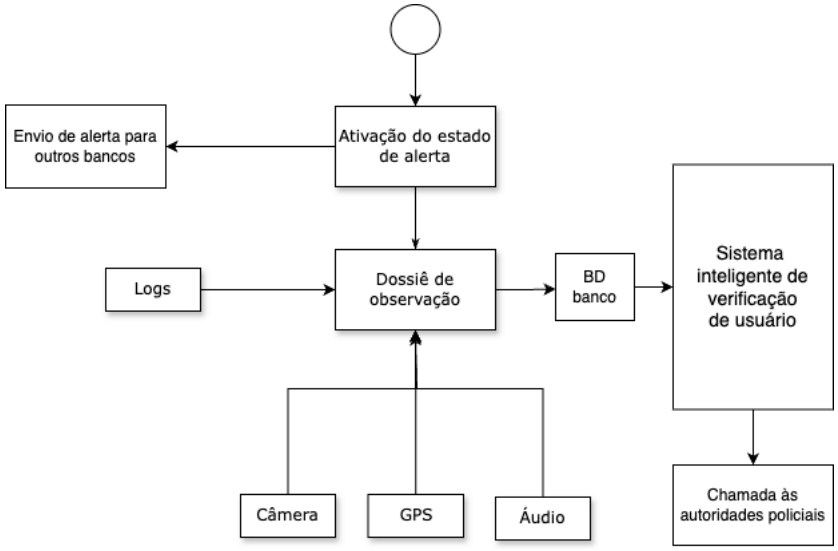



**Figura 13 :** Diagrama que representa em parte o fluxo de dados do estado de alerta até a notificação às autoridades policiais.

Os dados da câmera, do GPS e de áudio serão imediatamente coletados após a ativação do estado de alerta e serão salvos no dossiê. Todos os logs também irão compor esse dossiê.

Os logs indicarão todas as ações dentro do aplicativo (visualização de histórico, de saldo, de empréstimos, realização de PIX etc) realizadas pelo usuário. Esse dossiê será construído continuamente. Ele será salvo no banco de dados do banco e passará por um processo de verificação inteligente da identidade do usuário.

Caso o GPS da vítima seja desativado pelos criminosos, a perda da localização em tempo real será registrada nos logs e contabilizada no sistema de pontos como um aumento significativo no risco ao usuário. O último valor da localização será salvo e incluído no dossiê, pois essa informação pode indicar com precisão o local onde a vítima esteve e provavelmente será perto do local onde ela foi capturada pelos criminosos.

O sistema inteligente receberá todos esses dados para só assim determinar a necessidade ou não do acionamento da polícia. No caso do PIX, ele verificará a localização onde foi feita essa transferência (se o usuário tem o hábito de fazer PIX nessa região), se o destinatário é um destinatário habitual do usuário ou se é de uma conta já visada pelas autoridades policiais, se os valores são condizentes com os habituais pelo usuário.

Com os dados da câmera e do áudio, é possível identificar se o usuário que está manuseando o celular é o verdadeiro titular da conta. Se não for, um alerta de alta probabilidade de fraude será gerado. Caso seja o verdadeiro usuário, a idoneidade da ação ainda não é garantida e o sistema continuará a verificação. A partir do áudio, o sistema pode identificar se há instruções de coerção dirigidas à vítima, se há mais de uma voz presente e como essas vozes interagem no contexto.

Essa etapa é crucial, pois, atualmente, o contato com a polícia não é automático, dependendo do gerente da conta do usuário para acioná-la. Atualmente esse sistema inteligente já existe nas instituições financeiras, ele também funciona com um sistema de pontuação, no entanto, seu uso se limita a pedir mais "confirmações" de autenticidade ao usuário. Em geral, quando se inicia uma série de ações não habituais a pontuação de confiabilidade do usuário cai, e a partir de um limiar, o sistema pede um reforço de senha ou até biometria facial para reforço da confiabilidade. Como já discutido anteriormente, esse tipo de validação de autenticidade não ajuda no caso do sequestro relâmpago, pois a vítima está sob coação dos sequestradores e pode ter suas digitais e rosto usados para a autenticação.

Neste projeto, serão adicionadas ao sistema existente novas entradas que auxiliarão no processo de detecção de um indivíduo sob extorsão. A decisão de acionar a polícia ficará a cargo do sistema. Atualmente, essa responsabilidade é atribuída ao gerente da conta do usuário, o que está sujeito a erros humanos e a um atraso no tempo que pode custar até a vida da vítima.

| **Meio** | **Situação** | **Ação** |
|---|---|---|
| Câmera | Não identificação biométrica facial. | Aumentar score |
| | Identificação de objetos perigosos ou suspeitos. | Alertar polícia |
| | Presença de mais de uma pessoa na cena. | Aumentar score |
| | Usuário em situação de risco evidente. | Alertar polícia. |
| Áudio | Escuta-se gritos ou pedidos de socorro. | Alertar polícia |
| | Presença de palavras ou frases coercitivas. | Alertar polícia |
| | Mais de uma voz identificada. | Aumentar score |
| GPS | Localização em área de risco conhecida. | Aumentar score |
| | Desativação do GPS. | Aumentar score |
| | Deslocamento rápido e errático do dispositivo. | Aumentar score |
| | Uso de protocolos de anonimato (e.g., Tor ou VPN). | Aumentar score |
| Logs | **Visualização** | |
| | Visualização de limites de saque e transferência. | Aumentar score |
| | Visualização de histórico de transações. | Aumentar score |
| | Visualização de saldo e investimentos. | Aumentar score |
| | Visualização de crédito disponível. | Aumentar score |
| | **Configurações** | |
| | Alteração de senhas ou e-mail de autenticação. | Aumentar score |
| | Majoração de limites de saque/transferência. | Aumentar score |
| | Adição de novo dispositivo à lista de confiáveis. | Aumentar score |
| | Desativação de autenticação de dois fatores (2FA). | Aumentar score |

| | |
|---|---|
| Desativação de notificações de segurança por e-mail/SMS. | Aumentar score |
| **Comportamental** | |
| Atividade bancária em horários incomuns. | Aumentar score |
| Tentativa de acesso simultâneo a múltiplas contas. | Aumentar score |
| Acesso ao aplicativo de lugar não usual. | Aumentar score |
| Cadência de digitação diferente da usual. | Aumentar score |
| **Transações** | |
| Resgate antecipado do fundo de previdência. | Aumentar score |
| Resgate antecipado do fundo de garantia. | Aumentar score |
| Resgate antecipado de investimentos. | Aumentar score |
| Pagamentos de boletos de terceiros de valores elevados. | Aumentar score |
| Solicitação de um novo empréstimo ou financiamento. | Aumentar score |
| Transferências próximas do limite a novas contas. | Aumentar score |

**Tabela 3 :** Meios de coleta de dados, situações e ações tomadas. Saturação da cor indica intensidade da ação.

## 4.3 Atores

Nesta seção são apresentados os principais atores. Cada ator desempenha um papel específico para garantir o funcionamento seguro e eficiente do sistema, abrangendo desde o Usuário, que utiliza o aplicativo em situações de risco, até outros agentes responsáveis pela infraestrutura, monitoramento e suporte, como o banco e as autoridades. A especificação de requisitos para cada ator detalha suas responsabilidades, ações esperadas e limitações, estabelecendo um panorama claro para o desenvolvimento e a operação do sistema.

### 4.3.1 Usuário

O ator usuário representa o indivíduo que interage diretamente com o sistema, seja como cliente de um banco ou como pessoa em situação de risco potencial. Ele é responsável por configurar sua conta no modo pânico, definindo parâmetros como saldo fictício, histórico de transações e outros dados verossímeis.

Durante situações de coerção, o usuário pode ativar o sistema utilizando recursos como uma senha alternativa ou outros mecanismos de emergência. Sua experiência com o aplicativo deve ser intuitiva e segura, priorizando a facilidade de uso para configurações de rotina e respostas rápidas em momentos críticos. A segurança do usuário é o foco principal, garantindo proteção sem comprometer a usabilidade.

**Dados gerais do usuário**

Os dados do usuário podem ser organizados em três categorias principais: informações pessoais, informações bancárias e dados de segurança. Essa categorização facilita

a estruturação e o gerenciamento dos parâmetros essenciais para atender aos requisitos do projeto. A tabela abaixo apresenta os parâmetros mapeados para cada categoria, destacando sua relevância e aplicação no contexto do sistema.

| **Informações pessoais** | **Informações bancárias** | **Informações de segurança** |
|---|---|---|
| Nome | Agência | Biometria |
| Idade | Conta | Senha no modo normal |
| Celular | Banco | Senha no modo pânico |
| E-mail | Saldo bancário | Senha para transferências |
| CEP | Fatura atual | |
| | Limite de crédito | |
| | Empréstimo | |
| | Histórico de transações | |

**Tabela 4 :** Dados gerais do usuário.

As informações pessoais englobam os principais dados de identificação do indivíduo, sendo essenciais para processos como a abertura de contas bancárias e a associação de perfis ao sistema. Esses dados servem como base para garantir a autenticidade e a vinculação adequada do usuário ao serviço.

As informações bancárias abrangem elementos como saldo disponível, histórico de transações e limites de crédito. Esses dados financeiros são fundamentais para a gestão da conta e o monitoramento das atividades do usuário, oferecendo uma visão de sua situação financeira e comportamentos de consumo.

Por fim, os dados de segurança incluem elementos como senhas e chaves criptográficas, desempenhando um papel central na autenticação do usuário e na proteção contra acessos não autorizados. Esses dados são projetados para garantir a segurança e a integridade das interações com o sistema.

**Exemplos fictícios**

Para garantir a funcionalidade do modo pânico, é essencial que o aplicativo gere exemplos fictícios de transações, extratos e saldos que simulem atividades financeiras reais. Esses exemplos serão projetados para refletir o perfil típico de gastos do usuário, mas com ajustes que incluam um aumento de despesas e dívidas simuladas, de forma a justificar saldos menores e tornar o perfil mais verossímil durante situações de coação.

As tabelas abaixo fornecem as informações de um usuário fictício do banco.

| **Informações Pessoais** | **Valores** |
|---|---|
| Nome | Maria Silva |
| Idade | 32 anos |
| Celular | (11) 91234-5678 |
| E-mail | maria.silva@gmail.com |
| CEP | 12345-678 |

**Tabela 5 :** Dados pessoais.

| **Informações Bancárias** | **Valores** |
|---|---|
| Agência | 0001 |
| Conta | 5123423-0 |
| Banco | 0310 |
| Saldo bancário | R$ 23.250,00 |
| Fatura atual | R$ 4.450,00 |
| Limite de crédito | R$ 5.000,00 |
| Limite de empréstimo | R$ 15.000,00 |
| Histórico de transações | - 10/Dez: Mercado, - R$ 150,00<br>- 12/Dez: Transferência, - R$ 200,00<br>- 18/Dez: Depósito, + R$ 500,00 |

**Tabela 6 :** Dados bancários.

| **Informações de Segurança** | **Valores** |
|---|---|
| Biometria | Impressão digital |
| Senha no modo normal | 812934 |
| Senha no modo pânico | 123456 |
| Senha para transferências | 21473813 |

**Tabela 7 :** Dados de segurança.

### Usuário no modo pânico

No modo pânico, o sistema deve alterar apenas os dados bancários do usuário para simular um perfil financeiro mais restrito. O crédito apresentado no aplicativo será reduzido, limitando a capacidade de realizar grandes transações ou saques e será adicionado novos gastos e dívidas ao usuário, justificando assim um saldo menor e limites de crédito abaixo dos reais.

| **Informações Bancárias** | **Valores no modo pânico** |
|---|---|
| Agência | 0001 |
| Conta | 5123423-0 |
| Banco | 0310 |
| Saldo bancário | **R$ 3.250,00** |
| Fatura atual | **R$ 2.450,00** |
| Limite de crédito | **R$ 1.000,00** |
| Limite de empréstimo | **R$ 3.000,00** |
| Histórico de transações | - 10/Dez: Compra, - R$ 150,00<br>- 12/Dez: Transferência, - R$ 200,00<br>- 14/Dez: Consignado, **- R$ 1000,00**<br>- 16/Dez: Pensão, **- R$ 1500,00**<br>- 17/Dez: Aluguel, **- R$ 2000,00**<br>- 17/Dez: Carro, **- R$ 750,00**<br>- 18/Dez: Depósito, + R$ 500,00 |

**Tabela 8 :** Dados bancários no modo pânico. Dados em vermelho correspondem a valores fictícios adicionados.

### 4.3.2 Instituições financeiras

A comunicação do banco com o dispositivo móvel no modo pânico será aumentada. Todas as situações presentes na tabela 3 serão reportadas e guardadas do lado do servidor bancário. Para isso, a comunicação precisa utilizar protocolos seguros para garantir que todos os dados sejam transmitidos de forma criptografada, evitando intercepções e ataques durante a transmissão.

A garantia da confidencialidade desses envios é essencial para assegurar a negação plausível da vítima diante do criminoso. Se o criminoso conseguir interceptar os dados e descobrir que está sendo monitorado, quebra-se a possibilidade da vítima negar que ativou o modo pânico.

A camada de sessão lida com a autenticação e a gestão dos dados do usuário em tempo real. É importante que, no modo pânico, o sistema consiga diferenciar as sessões, oferecer um conjunto de dados fictício ao criminoso, sem comprometer a integridade dos dados reais do usuário, além de transmitir os dados de monitoramento para o servidor do banco.

Mais especificamente, é essencial garantir que toda a comunicação esteja protegida contra ataques de *downgrade*, o que torna a escolha dos protocolos fundamental. O uso obrigatório do TLS 1.3 é crucial para evitar vulnerabilidades já conhecidas, sendo igualmente importante monitorar de forma contínua a aplicação correta e atualização dos protocolos mais seguros.

**Autenticação do usuário**

A autenticação do usuário pode ser feita utilizando múltiplos fatores. No caso do modo pânico, o usuário poderá inserir uma senha alternativa que ativa o modo pânico ou ainda qualquer dos métodos já mencionados. A autenticidade dessas informações será garantida por meio de verificações contínuas durante a sessão, sem interferir na usabilidade do sistema.

**Modo pânico**

No modo pânico, o sistema entra em uma sessão especial onde todos os dados apresentados ao usuário e ao sequestrador são fictícios. Os bancos permitem transações, mas os valores reais permanecem ocultos. O sistema utiliza técnicas de obfuscação para garantir que o sequestrador não consiga detectar a ativação do modo pânico.

**Comunicação com autoridades**

Caso o sistema identifique atividades suspeitas durante o modo pânico (como tentativas de saques em locais incomuns ou comportamentos coercitivos), ele pode enviar um alerta silencioso às autoridades, fornecendo a localização e outras informações relevantes para uma possível intervenção. Esta comunicação será feita de forma automática pelo sistema do banco, sem que os criminosos percebam.

### 4.3.3 Autoridades policiais

Atualmente a polícia afirma ter uma linha direta com os bancos em que em caso de notificação, eles agem imediatamente. Com a solução pânico em ação, o sistema bancário irá enviar um dossiê à polícia quando ele decidir que o seu usuário está sob perigo. Esse dossiê não existe atualmente e a sua criação pode ajudar a atividade policial em si.

**Software policial**

O software policial deve ser capaz de receber o dossiê completo da vítima e as informações do seu celular. Esse sistema permitirá, de forma confidencial, estabelecer uma linha direta entre a polícia e o sistema bancário.

Ele precisa ser interoperável com todos os bancos, além de ser de fácil acesso e leitura, garantindo que os agentes policiais compreendam rapidamente a situação do usuário. Isso possibilitará uma intervenção policial ágil e eficaz, quando necessário.

### 4.3.4 Seguradoras

As seguradoras possuem um papel essencial na construção da solução pânico. Ela é uma parte interessada diretamente envolvida conjuntamente com os bancos.

**Modelo de negócios**

A solução pânico é uma solução financeiramente muito rentável para as segurado-

ras, pois pode-se ofertar seguros no momento da criação do perfil pânico pelo usuário. Além de que, com a mitigação dos valores roubados, as seguradoras terão menor valor para reembolsar as vítimas que contrataram seus serviços.

Além dessas vantagens, as seguradoras já possuem experiência no gerenciamento de dados estatísticos dos clientes, o que poderia facilitar o processo de criação do perfil pânico. Por isso, elas devem desempenhar um papel ativo e de liderança na implementação dessa solução de segurança.

# 5 DESENVOLVIMENTO DO TRABALHO

## 5.1 Artefatos

Alguns artefatos utilizados em gerenciamento de projetos foram utilizados nesse trabalho para auxiliar na organização, na metodologia e desenvolvimento. Esses artefatos são métodos consolidados que embasam as soluções propostas nesse projeto.

**Análise das partes interessadas**

Primeiramente foi identificada as partes interessadas, são elas: as instituições financeiras, as seguradoras, clientes de médio e alto capital financeiro, órgãos da segurança pública e os criminosos.

### 5.1.1 Registro das partes interessadas

O registro das partes interessadas é um documento que contém informações sobre as partes interessadas já identificadas do projeto. Esse registro trata de avaliar o nível de engajamento e a classificação das partes interessadas, definir o nível de interesse, poder e influência, como essas partes participam ou vão influenciar o andamento da solução proposta.

**Instituições financeiras**

As instituições financeiras, em particular os bancos, estão diretamente envolvidos, pois são atores que estão perdendo ativos financeiros com os sequestros relâmpagos e estão diretamente envolvidos na implementação das soluções propostas nesse trabalho.

Por ter influência sobre as políticas de segurança financeira, eles são os únicos que podem fornecer suporte em termos de integração de sistemas, monitoramento de transações suspeitas e notificação em tempo real para prevenir ou mitigar o impacto de um sequestro.

Hoje eles ocupam o nível de engajamento de conscientes do problema, mas precisa alcançar o nível de engajamento de líderes desse projeto.

**Seguradoras**

As seguradoras muitas vezes estão integradas aos bancos, no entanto, a importância do seu engajamento é alta e precisa ser destacada. Há um espaço de mercado enorme para as seguradoras expandirem seu modelo de negócios nesse projeto.

A oferta de um seguro contra sequestro relâmpago entra no seu modelo de negócios e ainda fornece uma ideia de segurança para o cliente de seus ativos roubados. O oferecimento de um seguro para o cliente no momento em que ele cria seu perfil pânico é uma parte essencial desse projeto. Além disso, quanto menor o valor subtraído pela

vítima, menor será o valor a restituir por parte da seguradora.

Outro ponto importante é a base de dados que as seguradoras possuem, essa base de dados pode auxiliar na criação de perfis pânicos verossímeis aos usuários que contratam seus seguros.

O engajamento das seguradoras hoje é neutro, mas deve mudar o status para, no mínimo, Apoiadores. Idealmente o status de Líderes juntamente com os bancos alavancaria o projeto.

**Usuários (vítimas potenciais)**

Essa parte interessada são as possíveis vítimas, que buscam segurança e maneiras de reduzir os riscos de perda de seus ativos durante o sequestro. Elas desempenham um papel crucial em todas as etapas do processo. Será necessário que participem ativamente na adaptação do modo pânico, o que requer um processo de educação para que compreendam completamente o funcionamento de todo o sistema.

Esses usuários são usuários de média e alta renda. Eles possuem receio de perder seus ativos durante esse tipo de crime e geralmente eles possuem alta escolaridade, em geral, possuem capacidade intelectual e cognitiva para entender todo o processo da solução pânico e de aceitar conscientemente os riscos e oportunidades oferecidas por essa solução.

Atualmente eles estão no nível de engajamento desinformados e precisam passar para o nível de apoiadores.

**Órgãos de segurança pública**

As autoridades policiais são fundamentais na resposta a incidentes criminosos, desempenhando um papel chave no monitoramento e na intervenção rápida durante um sequestro. Elas também são essenciais no processo de implementação do projeto, pois a automatização do chamado policial depende do desenvolvimento de uma solução de software do lado deles para receber esses chamados.

No entanto, ao conversamos com integrantes da instituição, sentimos uma enorme resistência de mudança no processo como ele é feito hoje. Outro ponto é a resistência com a ideia do modo pânico ter um "pouco" de dinheiro, eles se mostraram bastante inflexíveis com esse "ganho" por parte dos criminosos.

O nível de engajamento dos policiais hoje é resistente e precisa passar para o status de apoiadores.

**Criminosos**

Os criminosos são partes envolvidas diretas no ato criminoso. É preciso analisar todas suas ações para o melhor detalhamento do processo de solução pânico.

Atualmente o nível de engajamento dos criminosos é desinformados, mas com o

modo pânico em atividade eles passarão a ser resistentes, pois buscarão modos de burlar a solução e auferir maiores ganhos pelo ato criminoso. Entender como eles agem hoje e como irão reagir à solução é essencial para uma maior efetividade do projeto.

### 5.1.2 Matriz de avaliação do nível de engajamento das partes interessadas

É a matriz que compara os níveis de engajamento atual e desejado das partes interessadas, para que seja possível definir uma estratégia adequada do nível de engajamento de cada parte interessada do projeto.

| **Parte Interessada** | **Nível Atual** | **Nível Desejado** |
|---|---|---|
| Instituições Financeiras | Conscientes | Líderes |
| Seguradoras | Neutro | Apoiadores/Líderes |
| Usuários | Desinformados | Apoiadores |
| Órgãos de Segurança Pública | Resistentes | Apoiadores |
| Criminosos | Desinformados | Resistentes |

**Tabela 9 :** Matriz de Engajamento das Partes Interessadas

**Monitoramento e comunicação com as partes interessadas**

O monitoramento de todas as partes envolvidas no projeto é essencial para alcançar o sucesso planejado do projeto. Se os bancos e seguradoras não tomarem a voz ativa de liderança, ficará muito difícil a implementação real dessa solução. Mostrar as vantagens econômicas aos clientes é uma forma de engajar as partes interessadas no projeto e pressionar os bancos e seguradoras pela implementação da solução.

A comunicação eficaz e eficiente serão essenciais nesse projeto, ela precisará ser feita com base numa estratégia adequada para a elevação do nível de engajamento de cada parte interessada do projeto. A estratégia será importante, pois como temos partes interessadas bem distintas, precisará de uma adaptabilidade comunicativa com cada parte envolvida.

### 5.1.3 Matriz RACI

A matriz de responsabilidades (também conhecida como matriz RACI) é um artefato de informação visual importante na atribuição de responsabilidades em um projeto. A interação harmônica entre as partes interessadas é essencial para o sucesso do projeto e isso passa pela clareza da responsabilidade de cada um.

Usualmente ela é feita para atribuir responsabilidades aos atores (gerentes, desenvolvedores entre outros) dentro de um projeto. Neste projeto a matriz RACI é usada para atribuir responsabilidades às partes interessadas. É importante definir quem tem a responsabilidade pela execução(R), responsabilidade pela aprovação/decisão (A), quem

será consultado (C) e quem será apenas informado (I), para o caso de nenhuma ação será indicado com o hífen (-).

Em geral, a matriz RACI tem ao menos um responsável para cada atividade e exclusivamente um aprovador para cada tarefa. No entanto, aqui usaremos mais a ideia de alocar responsabilidades e forçar a interação entre as partes interessadas, descartando assim essas obrigações que existem normalmente num gerenciamento de projetos.

Por exemplo, a atividade de criação do perfil pânico, ela é de responsabilidade da Instituição Financeira e dos Usuários, no entanto, é de total interesse das Seguradoras que nessa criação seja ofertado um seguro para os ativos financeiros possivelmente roubados, ou ainda uma oferta de seguro de vida, portanto, ela apesar de não responsável é de boa prática que as seguradoras sejam consultadas para ajudarem na criação desse formulário de criação do perfil pânico pelo usuário. As seguradoras podem ajudar de qual maneira o banco vai oferecer esses pacotes de seguro, como deve ser feito o formulário e em qual momento deve ser ofertado.

| **Atividade / Parte Interessada** | **Instituições Financeiras** | **Seguradoras** | **Usuários** | **Órgãos de Segurança Pública** |
|---|---|---|---|---|
| Definição da política de score | R | I | I | C |
| Mudança na política de criação de contas já existentes | R | I | I | I |
| Alteração na autenticação do app bancário | R | I | C | I |
| Criação de token bancário | R | I | I | I |
| Mudança dos valores dos atributos no modo pânico | R | R | R | I |
| Criação do sistema inteligente de verificação do usuário | R | I | I | C |
| Criação do perfil pânico | R | C | R | - |
| Desenvolvimento de um sistema para recepção automática de chamados | C | I | I | R |

**Tabela 10 :** Matriz RACI das Partes Interessadas

### 5.1.4 Matriz SWOT

A análise SWOT fornece subsídios para análise de forças (S), fraquezas (W), oportunidades (O) e ameaças (T), com a finalidade de identificar riscos. As ameaças e fraquezas são riscos negativos, as forças e oportunidades riscos positivos. Em geral, as forças e fraquezas estão relacionadas a algo interno e as oportunidades e ameaças a algo externo.

| **Forças (Strengths)** | **Fraquezas (Weaknesses)** |
|---|---|
| Sistema inteligente com monitoramento contínuo e contato automatizado das autoridades policiais. | Dependência da precisão do sistema de detecção para evitar falhas de segurança. |
| Implementação de múltiplos tipos de autenticação segundo perfil do usuário. | Vulnerabilidade a falhas humanas, como senhas esquecidas ou utilizadas de forma inadequada. |
| Modo pânico com forte proteção contra a descoberta e uso indevido. | Potencial sobrecarga de chamadas de emergência em caso de falso positivo. |
| **Oportunidades (Opportunities)** | **Ameaças (Threats)** |
| Avanço das tecnologias de IA que podem melhorar a detecção e minimização de riscos. | Falhas técnicas no sistema que podem comprometer a segurança e permitir ação criminosa. |
| Amplo modelo de negócio para banco e seguradoras | Engenharia social que pode comprometer o acesso à autenticação pânico por manipulação do usuário. |
| Aumento da segurança para a sociedade | Riscos de escalada da violência ou extorsão caso os criminosos descubram o uso do modo pânico. |

**Tabela 11 :** Matriz SWOT para identificação de riscos.

#### Análise de riscos

Antes de validar as soluções, é necessário realizar uma análise dos riscos envolvidos nesse processo. Os ativos mais importantes deste projeto são a integridade física do usuário, a preservação de sua vida e seus ativos financeiros. A solução de ocultação do aplicativo e a solução de pânico geram riscos secundários que precisam ser analisados e tratados continuamente até sua aceitação.

#### Modo pânico

Com base na matriz SWOT realizada, faremos uma análise de risco para os riscos **negativos** envolvidos na solução pânico.

**Riscos de falso positivo**

1) Risco do usuário entrar com a senha fraca alternativa sem estar numa situação de perigo. O risco de falso positivo poderia sobrecarregar as forças policiais se essas fossem chamadas logo após a senha fraca alternativa. No entanto, o sistema inteligente usará essa entrada apenas como uma das variáveis a ser levada em conta para o chamado policial. Esse risco tem impacto baixo e probabilidade alta.

Solução: **mitigar risco** de sobrecarga do chamado policial. Só a senha fraca alternativa não é motivo suficiente para chamar as autoridades de segurança pública. O modo pânico é ativado, e um dossiê começa a ser gerado. Caso a confirmação seja feita por meio de uma segunda senha forte alternativa, a polícia é acionada e recebe essas informações imediatamente.

**Riscos de falso negativo**

2) Risco do usuário entrar com a senha fraca original estando em situação de perigo. Esse é o risco de falso negativo. Essa situação é a mais perigosa, pois caso o usuário "esqueça" sua senha pânico e entre com a senha original, o sistema irá mostrar o valor verdadeiro de seus ativos financeiros e consequentemente eles estarão à visão dos criminosos.

Nesse modo, outros fatores continuam sendo monitorados continuamente pelo sistema inteligente que pode por si só desconfiar que não é o usuário verdadeiro que está em posse do seu celular, ele poderá pedir biometria e outros fatores de autenticação para evitar acesso de terceiro sem a presença do usuário verdadeiro (como já acontece atualmente).

No entanto, em casos de sequestro e extorsão, será necessário aguardar que o usuário insira a senha forte alternativa durante a transferência para acionar as autoridades policiais. Vale ressaltar que, nessa situação específica, o perfil pânico não pode ser ativado, pois os ativos financeiros do usuário já foram expostos aos criminosos. Contudo, isso não dispensa o sistema inteligente de monitorar o usuário, analisando sua câmera, sons e outros fatores, a fim de, em conjunto com outras informações, determinar a necessidade de acionar a polícia e preservar a integridade física do usuário. Esse risco apresenta um impacto alto e uma probabilidade média.

Solução: **mitigar risco** e suas consequências. O perfil pânico não é ativado, mas, caso a transferência seja confirmada como resultado de extorsão, a polícia deve ser contatada automaticamente. Além disso, é crucial tomar medidas para minimizar os danos da extorsão, considerando que a vítima ainda está sob custódia dos criminosos, os quais podem tentar cometer outros crimes contra ela.

### 5.1.5 Matriz de confusão

Essas classificações serão realizadas pelo sistema inteligente que utilizará técnicas de IA que fogem do escopo desse projeto, mas vale destacar que será necessário criar o que se chama de Matriz de confusão (também chamada de matriz de erros) que metrifica os falsos positivos (erro do tipo I) e falsos negativos (erro do tipo II) em relação com os verdadeiros positivos e negativos.

Essa técnica envolve a determinação de parâmetros como acurácia, precisão, recall, especificidade e F-score. Para o escopo deste projeto, o importante é destacar que o falso positivo tem baixo impacto nos ativos, enquanto que o falso negativo tem alto impacto em todos os ativos (vida e recursos financeiros). Por isso, devem ser usadas técnicas que reduzem ao máximo os falsos negativos.

| | | **Predito** | |
|---|---|---|---|
| | | **Condição positiva prevista** | **Condição negativa prevista** |
| **Verdade** | **Positivo** | Verdadeiro Positivo | Falso Negativo (Erro Tipo II) |
| | **Negativo** | Falso Positivo (Erro Tipo I) | Verdadeiro Negativo |

**Tabela 12 :** Matriz de Confusão.

**Riscos sobre o modo pânico**

3) Risco de desconfiança dos criminosos que o usuário entrou em modo pânico.

Solução: **aceitar risco**. Mesmo que os criminosos desconfiem que está entrando no modo pânico da conta do usuário, ele nunca poderá ter certeza disso, pois há uma similaridade dos perfis normal e pânico e uma verosimilhança da conta pânico com a vida do usuário. Esse risco tem impacto baixo e probabilidade média.

4) Risco de descoberta que o usuário possui uma conta em modo pânico.

Solução: **aceitar risco**. Mesmo que o criminoso saiba antecipadamente que o usuário possui uma conta que possui o modo pânico, ele não poderá saber se a senha colocada pelo usuário vai entrar na conta em seu modo normal ou no seu modo pânico, tendo que se contentar com o valor que terá na conta após entrada. Esse risco tem impacto baixo e probabilidade baixa.

5) Risco de descoberta que o usuário entrou no modo pânico.

Solução: **aceitar risco**. Mesmo que os criminosos de algum modo descubram que o usuário entrou na conta no modo pânico e obriguem o usuário a colocar a senha original correta, a conta uma vez ativada no modo pânico não poderá voltar ao modo normal sem que o usuário passe numa agência física, onde ele mudará a senha original e senha

alternativa.

A conta está bloqueada nesse estado, evitando mais extorsões. No entanto, esse risco tem um impacto médio, pois pode escabar em violência se os criminosos quiserem se vingar do usuário que não entrou na conta original, mas tem probabilidade baixa, pois o projeto em si é baseado em que o modo pânico seja indistinguível do modo real.

**Riscos de falhas no sistema**

6) Risco de falha técnica no sistema inteligente

Esse risco envolve a possibilidade de o sistema não funcionar corretamente em momentos críticos devido a falhas técnicas, como indisponibilidade de servidores, erros na detecção de situações de perigo, quedas de conexão ou bugs inesperados no software. Essas situações podem comprometer a segurança do usuário, uma vez que o sistema pode não conseguir identificar uma situação de risco ou realizar as ações necessárias, como chamar as autoridades ou bloquear a conta no modo pânico.

Apesar de ter probabilidade baixa, considerando que o sistema deve ser projetado para alta disponibilidade e redundância, o impacto de uma falha desse tipo é alto, pois coloca em risco a integridade física e os ativos financeiros do usuário.

Solução: **aceitar risco**. Ainda na fase de projeto, serão implementadas soluções para que a probabilidade desse risco seja baixa, podemos citar: implementar infraestrutura redundante, mecanismos de failover e monitoramento constante para identificar e resolver problemas rapidamente. Dada a disponibilidade como de alta importância, resta aceitar o risco.

### 5.1.6 Matriz de Probabilidade e Impacto

A matriz de probabilidade e impacto é um artefato de análise qualitativa. O foco é a priorização dos riscos. Por exemplo: o risco 6, antes de ser colocado no projeto que cabe um sistema de alta disponibilidade para o sistema inteligente, a probabilidade dele era média com alto impacto, para reduzir isso, o risco foi **mitigado** colocando no projeto um sistema de alta disponibilidade, levando o risco 6 para uma escala de baixa probabilidade, o que culminou com a **aceitação** desse risco.

Essa matriz deve ser revista periodicamente, com o objetivo de reduzir constantemente a probabilidade e o impacto dos riscos associados. Com o surgimento de novas tecnologias e ideias, surgem também novas soluções que podem mitigar riscos, mas, por outro lado, muitos outros riscos podem emergir e devem ser catalogados e analisados minuciosamente.

| **Probabilidade/ Impacto** | **Baixo** | **Médio** | **Alto** |
|---|---|---|---|
| **Alta** | Risco 1 | | |
| **Média** | Risco 3 | Risco 5 | Risco 2 |
| **Baixa** | Risco 4 | | Risco 6 |

**Tabela 13 :** Matriz de Probabilidade e Impacto

## 5.2 Arquitetura do Sistema

O desenvolvimento do protótipo do aplicativo de pânico será realizado utilizando o React Native. O protótipo tem o objetivo de validar os requisitos funcionais da solução pânico que envolve a negação plausível em situações de sequestro relâmpago.

A arquitetura de software de um aplicativo móvel é composta por três camadas principais: camada de apresentação, camada de aplicação e camada de dados. Nesta seção, serão detalhadas as características e os processos de desenvolvimento associados a cada uma dessas camadas, destacando suas funções e interações no contexto do sistema.

### 5.2.1 Camada de Apresentação

A camada de apresentação é responsável pela interação entre o usuário e o aplicativo, sendo o ponto de entrada para todas as funcionalidades do sistema. Seu principal objetivo é fornecer uma interface que permita ao usuário acessar os recursos bancários, mesmo em situações de risco, como no caso do modo pânico de forma intuitiva.

Para o desenvolvimento desta camada, foi utilizado o React Native, uma tecnologia que possibilita a criação de aplicativos multiplataforma com alto desempenho e uma interface consistente que utiliza linguagens já utilizadas pelos integrantes do projeto.

O uso do React Native se justifica por uma flexibilidade e qualidade. A tecnologia permite compartilhar uma única base de código entre Android, iOS e aplicações web, reduzindo o tempo de desenvolvimento e manutenção do sistema. Além disso, oferece integração robusta com APIs nativas para implementar recursos como biometria, geolocalização e notificações em tempo real, no qual serão usados para o funcionamento do modo pânico. A biblioteca também suporta o uso de frameworks de design, como Material Design, garantindo uma experiência visual padronizada e alinhada às expectativas dos usuários de aplicativos bancários.

O design da interface foi inspirado em aplicativos de bancos digitais utilizados no Brasil, como Nubank, Itaú e Banco do Brasil, reconhecidos por suas interfaces simples e focadas na experiência do usuário. A familiaridade com esse tipo de layout facilita a

navegação dos usuários, especialmente em situações de estresse, como durante a ativação do modo pânico. Elementos como menus laterais, botões de ação destacados e organização clara de informações foram adaptados para garantir o entendimento necessário para o funcionamento seguro do sistema.

A criação da identidade visual do iLLubank foi pensada para reforçar o conceito central do aplicativo, que é a negação plausível, não permitindo ao sequestrador distinguir entre a realidade e a ficção durante situações de sequestro. O nome "iLLubank"foi escolhido justamente para transmitir essa ideia de ilusão e segurança.

As cores azul e branco foram selecionadas, pois poucos bancos no Brasil utilizam essa combinação. Além disso, o azul é tradicionalmente associado à confiança e segurança. O design do logo segue essa linha, sendo simples e direto, mas incorporando elementos que destacam a ideia de uma solução financeira segura.

Para o desenvolvimento de todos os designs das páginas e imagens do aplicativo, foram utilizadas duas ferramentas principais: Photoshop/Illustrator e Figma. O Photoshop e o Illustrator são amplamente utilizados para a criação e edição de elementos gráficos, com recursos para trabalhar com imagens, ícones e outras artes visuais que compõem a identidade do aplicativo. Já o Figma foi utilizado para o design da interface adaptados para diferentes dimensões de celulares. Isso permitiu testar e ajustar a experiência do usuário.

O aplicativo foi desenvolvido com base em quatro páginas principais. A seguir, serão apresentadas cada uma dessas páginas: Login, Menu, Extrato Bancário e Transferências de PIX.

**Login**

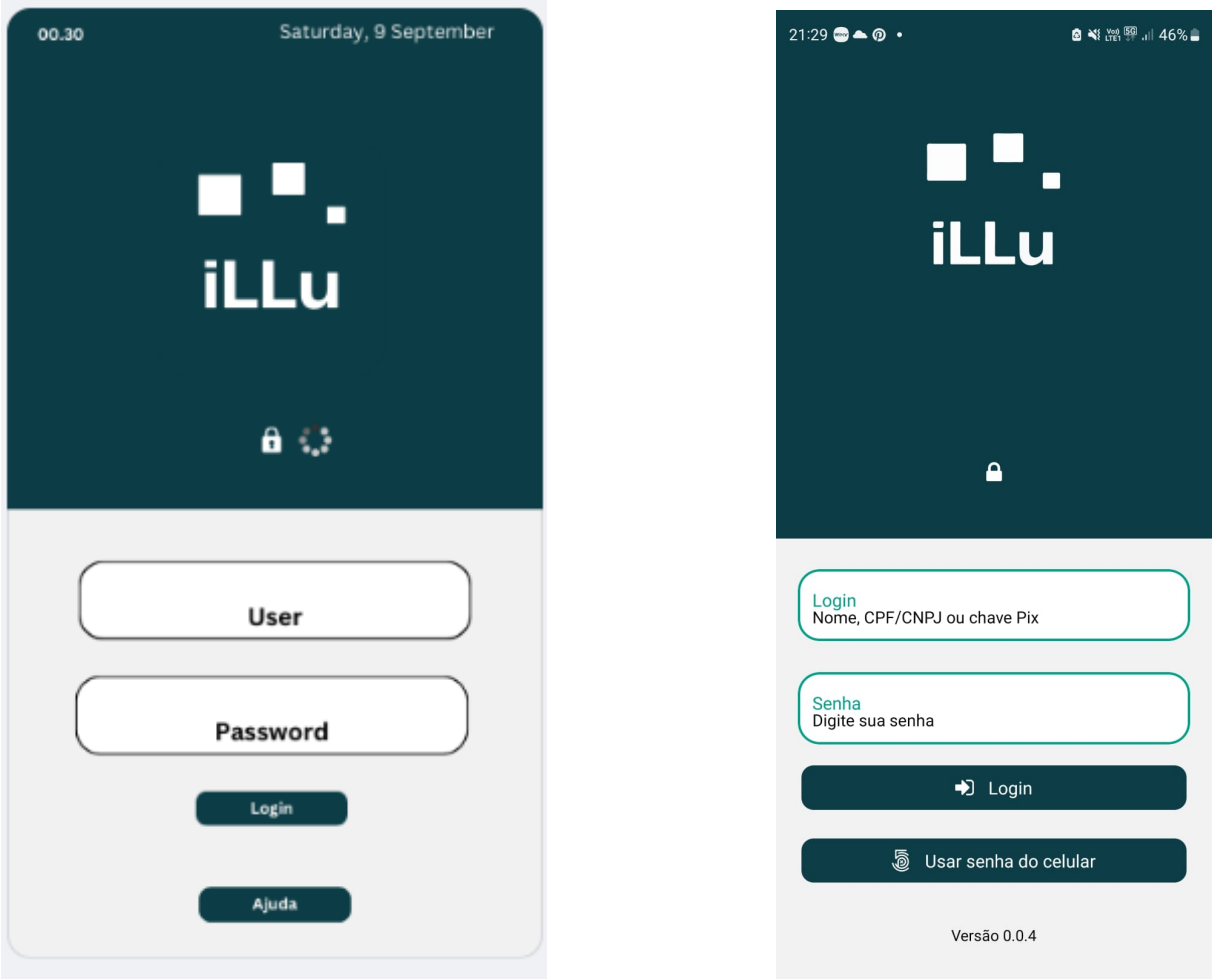
A página de login foi projetada para ser simples e ela conta com os seguintes elementos.

O campo de entrada para o nome de usuário permite que o usuário insira suas credenciais, como e-mail ou CPF. O campo de senha é projetado para ocultar a entrada do usuário, garantindo a privacidade durante o processo de login. O botão de login é a principal ação para autenticar o usuário, acionando a validação das credenciais inseridas. Além disso, foi implementado um botão que permite a autenticação por impressão digital, pensando na agilidade e segurança, facilitando o acesso ao aplicativo sem a necessidade de digitar a senha.

Além desses componentes principais, a página também inclui outros recursos. O ícone de bloqueado é exibido quando a página está aguardando a autenticação ou bloqueando o acesso até que a senha ou a biometria sejam validadas. Durante o processo de login, o ícone de carregando é mostrado, indicando que o sistema está verificando as

credenciais e processando o pedido de acesso. Por fim, a versão atual do aplicativo é exibida no rodapé da página de login.

Por fim, a página projetada no Figma está ilustrada na imagem abaixo à esquerda, enquanto a versão desenvolvida utilizando React é mostrada na imagem à direita. Durante o processo de desenvolvimento, algumas modificações e melhorias foram realizadas entre o esboço inicial e o design final.




**(a)** Esboço feito no Figma. **(b)** Design final no React.

**Figura 14 :** Design da página de login.

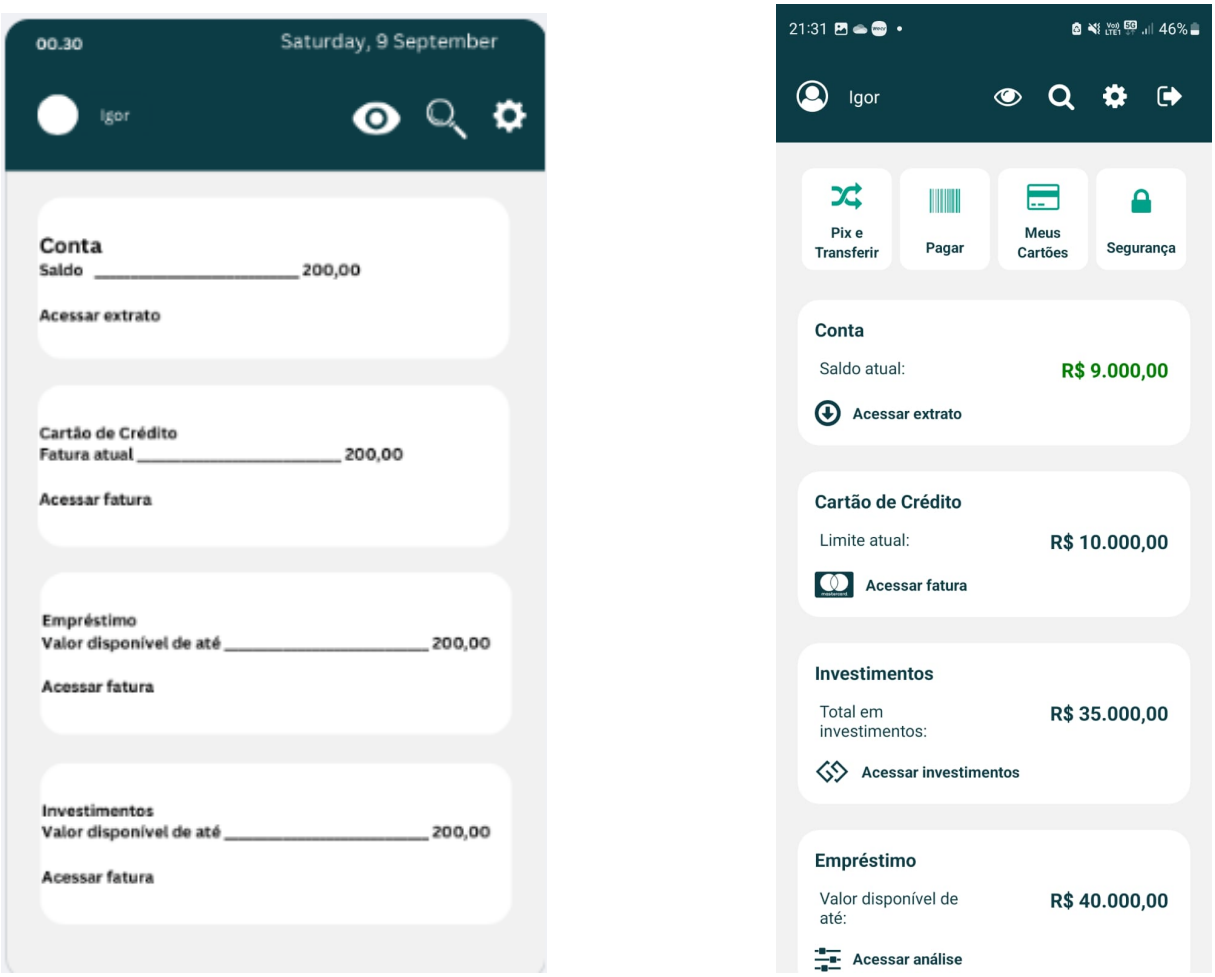
### Menu

A página de Menu é acessada logo após o usuário realizar o login no aplicativo. Ela serve como o ponto central de navegação para todas as funcionalidades. No cabeçalho da página, são exibidas algumas informações do usuário, incluindo sua foto de perfil, nome, a opção de visibilidade do saldo, uma lupa para pesquisa, além de ícones para configurações e logout.

No corpo da página, estão as principais ferramentas do aplicativo, organizadas de

forma intuitiva para facilitar o acesso do usuário. Entre essas ferramentas, encontram-se as opções de transferência PIX, pagar, meus cartões e segurança. Além disso, a página de Menu inclui quatro blocos destacados que fornecem uma visão rápida das informações financeiras do usuário, como o saldo da conta, cartão de crédito, investimentos e empréstimos disponíveis.

A página de Menu projetada no Figma está ilustrada na imagem abaixo à esquerda, enquanto a versão desenvolvida utilizando React é mostrada na imagem à direita.




**(a)** Esboço feito no Figma. **(b)** Design final no React.

**Figura 15 :** Design da página de menu.

### Extrato Bancário e Transferências de PIX

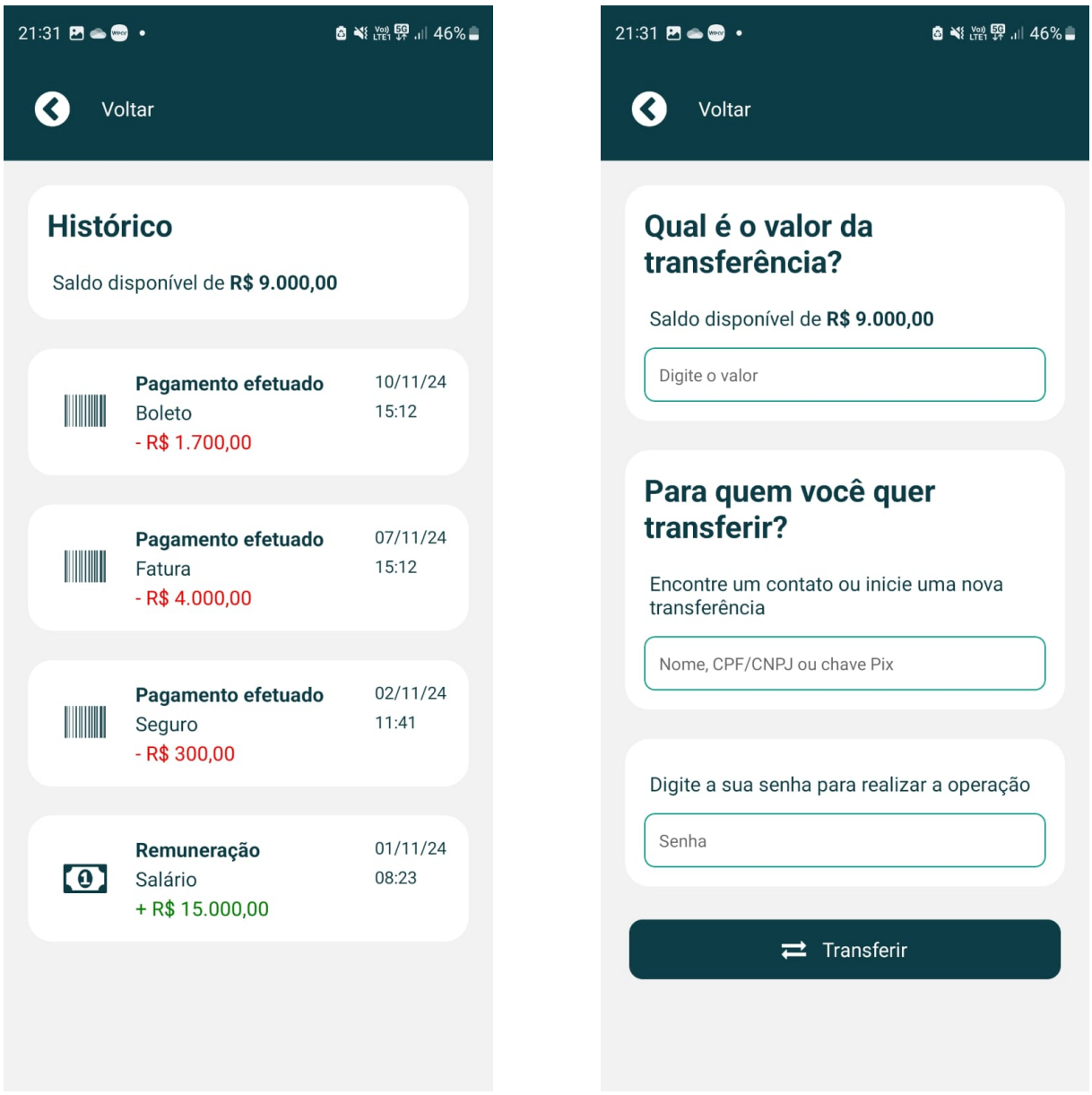
As outras duas páginas do aplicativo, extrato bancário e transferências de pix, são acessadas a partir do menu, clicando nos respectivos botões: "acessar extrato"e "transferência pix".

A página de extrato bancário oferece uma visão das transações financeiras do usuário. Nela, o usuário pode visualizar o saldo disponível, assim como o histórico de movimentações, que inclui pagamentos, salários, entradas e saídas, transferências, consignados,

entre outros. A página também exibe informações sobre cada movimentação, como data e horário, além da origem ou destino das transações.

Por outro lado, a página de transferências de pix foi projetada para ser simples. Ela contém campos de entrada, como uma caixa para digitar o valor da transferência, outra para informar o usuário de destino, e uma terceira caixa para digitar a senha de transação. Por fim, a página inclui um botão de transferir, que, ao ser clicado, realiza a transação, enviando os valores para a conta de destino.

Por fim, a página desenvolvida utilizando React do extrato é mostrada na imagem à esquerda e a página da transferência está ilustrada na imagem à direita.




**(a)** Página do extrato. **(b)** Página das transferências.

**Figura 16 :** Design das páginas secundárias do aplicativo.

**Página para controle de segurança**

Por último, foi desenvolvida uma página adicional para o controle do score do usuário diretamente no celular ao clicar no ícone de segurança no menu. O objetivo dessa página é facilitar os testes do protótipo e fornecer ao desenvolvedor informações importantes sobre a segurança da conta do usuário em tempo real.

A página é composta por quatro blocos principais. O primeiro bloco exibe o score do usuário, que varia de 100 a 0. O segundo bloco mostra o nível do modo pânico, indicando o status atual da proteção da conta. O terceiro bloco apresenta a localização em tempo real da pessoa, permitindo o monitoramento constante do usuário. Por fim, o quarto bloco exibe a quantidade de movimentações estranhas no dia, ajudando a identificar atividades suspeitas. A página está ilustrada na imagem abaixo.


**Figura 17 :** Página do Score.

### 5.2.2 Camada de Aplicação

A camada de aplicação é responsável pela lógica de negócios e pelo processamento das requisições feitas pela interface do usuário, conectando a camada de apresentação aos dados. É nesta etapa que ocorre o gerenciamento de todas as funcionalidades principais, como autenticação, transações financeiras, controle de segurança e integração com sistemas externos.

A camada de aplicação no iLLubank foi desenvolvida utilizando React e suas bibliotecas, garantindo que o fluxo de dados entre a interface e a lógica do sistema seja rápido. Além disso, será utilizado a Expo, que é uma plataforma e um conjunto de ferramentas que simplifica o desenvolvimento de aplicativos móveis utilizando React Native. Ele fornece um ambiente de desenvolvimento com bibliotecas e APIs prontas para uso, o que elimina a necessidade de configurar dependências nativas manualmente.

Serão utilizadas algumas ferramentas da Expo, como a Expo CLI, que facilita a criação e execução de aplicativos React Native para testes. Também será usado o Expo SDK, que oferece APIs prontas para uso, como acesso à câmera, geolocalização, notificações push, autenticação, entre outros recursos. Por último, o Expo Go que é um aplicativo cliente que permite aos desenvolvedores visualizar e testar o aplicativo diretamente em seus dispositivos móveis durante o desenvolvimento, sem a necessidade de compilar ou configurar manualmente o código nativo. Basta escanear um código QR para carregar a versão mais recente do aplicativo no dispositivo, o que acelera o processo de desenvolvimento.

O backend do sistema será desenvolvido utilizando uma arquitetura de microserviços, visando otimizar a escalabilidade do sistema. A escolha pela arquitetura de microserviços permite que cada funcionalidade do sistema seja desenvolvida de forma independente, podendo ser escalada, atualizada ou mantida sem impactar outras partes da aplicação.

Dentre os principais serviços que serão implementados, destacam-se: autenticação, localização por GPS, transferência via PIX, dados em modo pânico e score.

**Criação do ambiente de desenvolvimento**

Para começar o desenvolvimento do aplicativo, foi necessário ter alguns pré-requisitos instalados. Primeiro, é preciso ter o Expo Go instalado em um celular, o que permitirá testar o aplicativo em tempo real. Além disso, é necessário ter o Node.js na versão LTS (Long-Term Support) instalada no sistema. Foi utilizado o VS Code como editor de código para facilitar o processo de codificação. O desenvolvimento pode ser feito em macOS, Linux ou Windows (com PowerShell ou WSL2).

O primeiro passo para inicializar o desenvolvimento do aplicativo Expo é usar o

comando create-expo-app. Após a criação do projeto, é necessário baixar e configurar os ativos que serão utilizados ao longo do desenvolvimento. No passo seguinte, foi executado o script reset-project para remover o código boilerplate e iniciar o desenvolvimento do aplicativo do zero. Para isso, basta executar o comando npm run reset-project no terminal. Após a execução, restarão dois arquivos, index.tsx e _layout.tsx, dentro do diretório app. Todos os outros arquivos e diretórios de código boilerplate (como components, constants e hooks) serão movidos para o diretório app-example. A partir daí, foram criados os próprios diretórios e arquivos conforme avançamos no desenvolvimento.

Por fim, para executar o aplicativo no dispositivo e na web, é necessário iniciar o servidor de desenvolvimento no terminal, utilizando o comando npx expo start. Isso fará com que o servidor seja iniciado, exibindo um código QR na janela do terminal. Ao escanear o código QR, o aplicativo será aberto no dispositivo móvel.

**Comunicação com o EAS**

Para gerar um arquivo APK para o sistema Android, é necessário vincular o projeto ao EAS (Expo Application Services). O primeiro passo para isso é instalar o EAS CLI, a ferramenta de linha de comando do EAS, executando o comando npm install -g eas-cli. Com o EAS CLI instalado, o próximo passo é realizar o login na plataforma utilizando o comando eas login. Esse comando autentica o usuário e o vincula à sua conta no Expo, permitindo o acesso a todos os serviços e funcionalidades oferecidos pelo EAS para construção e distribuição do aplicativo.

Após a autenticação, é preciso configurar o repositório do projeto no Git, criando um repositório remoto para gerenciar o código de forma colaborativa. Em seguida, o comando eas init deve ser executado para inicializar o EAS no projeto. Esse comando cria os arquivos e a configuração básica para que o EAS funcione corretamente com o projeto.

No arquivo app.json, é necessário realizar uma modificação para incluir a chave extra.eas.projectId, atualizando o valor com o ID exclusivo gerado pelo EAS. Esse ID é necessário para identificar o projeto corretamente dentro da plataforma Expo. Depois de realizar essas configurações iniciais, o comando eas build:configure deve ser executado para configurar o projeto para construção no EAS, ajustando as definições necessárias para o processo de build. Por fim, a execução desse comando cria o arquivo eas.json na raiz do diretório, um arquivo de configuração para o processo de build e deploy do aplicativo no EAS.

**Autenticação**

O Firebase Authentication é um serviço oferecido pelo Firebase, uma plataforma de desenvolvimento de aplicativos móveis e web forncecida pelo Google, que simplifica o processo de autenticação de usuários. Ele fornece uma série de métodos de autenticação,

incluindo o uso de e-mail e senha, autenticação por redes sociais como Google e Facebook, e autenticação biométrica. Para este projeto, optamos por utilizar o Firebase Authentication para validar o login do usuário tanto com a combinação de e-mail e senha quanto com a autenticação biométrica, permitindo maior flexibilidade na forma de login.

Na primeira metodologia de autenticação, o usuário insere seu e-mail e senha na página de login. O Firebase Authentication valida essas credenciais ao compará-las com as informações armazenadas no banco de dados do Firebase, garantindo que o usuário esteja autorizado a acessar o sistema. Além disso, o serviço oferece recursos de segurança como a recuperação de senha e verificação de e-mail.

A segunda metodologia de autenticação envolve o uso de biometria, especificamente a impressão digital cadastrada no dispositivo. O Firebase Authentication oferece suporte à autenticação biométrica como uma forma adicional de validação de identidade. Para isso, é necessário utilizar a biblioteca expo-local-authentication, que permite o uso de funcionalidades de biometria em dispositivos móveis. Quando o usuário optar por essa forma de login, o sistema utilizará a autenticação biométrica em conjunto com o e-mail registrado no Firebase.

Para integrar essas funcionalidades ao aplicativo, foi necessário instalar as bibliotecas específicas: npx expo install expo-local-authentication para habilitar a autenticação biométrica e npx expo install firebase para integrar o Firebase Authentication.

O usuário poderá selecionar apenas um método de senha segura para acessar o aplicativo, enquanto os outros dois métodos serão destinados ao modo pânico. Por exemplo, o usuário poderá optar por uma senha numérica tradicional e autenticação biométrica para acesso no modo pânico, e configurar uma segunda senha numérica exclusiva para o modo normal.

**Comunicação com o banco de dados**

O banco de dados utilizado neste projeto foi o Firebase Cloud Firestore, que é uma solução NoSQL ideal para armazenar dados de aplicativos. O Firestore permite o armazenamento e a sincronização de dados em tempo real entre os clientes. Para integrar o Firestore ao aplicativo, foi necessário instalar a biblioteca do Firebase utilizando o comando npx expo install firebase.

Após a integração, foi possível realizar operações no banco de dados. Por exemplo, as funções setDoc e addDoc permitem adicionar ou atualizar documentos em uma coleção do Firestore. Já a função doc é utilizada para acessar um documento específico dentro de uma coleção, enquanto getDocs e getDoc são usadas para recuperar múltiplos documentos ou um único documento. A função collection possibilita acessar uma coleção específica no banco de dados, enquanto query e where permitem realizar consultas avançadas, filtrando e buscando documentos com base em critérios específicos definidos pelo desenvolvedor.

**Localização por GPS**

A funcionalidade de localização por GPS foi implementada de duas formas distintas no aplicativo. A primeira utilização ocorre durante as transferências e pagamentos realizados pelo usuário. Nesse caso, a latitude e longitude do dispositivo serão capturadas e armazenadas no servidor durante essas ações, a fim de registrar a localização exata do usuário no momento da transação.

A segunda aplicação da localização por GPS será durante o uso do aplicativo. A latitude e longitude do usuário serão constantemente monitoradas para comparar com uma localização de segurança predefinida, chamada de "safe point". Caso o usuário se afaste mais de 1 km desse ponto seguro, o score de segurança do usuário será negativamente afetado.

Para implementar essa funcionalidade de localização no aplicativo, foi necessário instalar a biblioteca expo-location com o comando npx expo install expo-location. Essa ferramenta oferece uma maneira eficiente de acessar as informações de localização do dispositivo, permitindo que o aplicativo obtenha a latitude e longitude em tempo real, com baixo impacto no desempenho do sistema.

No contexto deste projeto, a fórmula Haversine foi aplicada para calcular a distância em quilômetros entre as coordenadas de latitude e longitude do dispositivo do usuário e o ponto seguro predefinido. Com isso, é possível monitorar se o usuário se afasta de sua localização segura.

A fórmula Haversine é utilizada para calcular a distância entre dois pontos na superfície de uma esfera, a partir de suas coordenadas geográficas (latitude e longitude). Essa fórmula é amplamente utilizada em sistemas de navegação e geolocalização, pois permite calcular a distância entre dois pontos na Terra, considerando a curvatura do planeta. A Fórmula Haversine leva em conta a esfericidade da Terra e é ideal para medir distâncias precisas entre locais baseados em coordenadas geográficas.

A fórmula Haversine é expressa da seguinte maneira:

$$a = \sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1) \cdot \cos(\phi_2) \cdot \sin^2\left(\frac{\Delta\lambda}{2}\right)$$

$$c = 2 \cdot \operatorname{atan2}\left(\sqrt{a}, \sqrt{1-a}\right)$$

$$d = R \cdot c$$

Onde:

- $\phi_1$ e $\phi_2$ são as latitudes dos dois pontos em radianos.
- $\lambda_1$ e $\lambda_2$ são as longitudes dos dois pontos em radianos.
- $\Delta\phi$ é a diferença entre as latitudes dos dois pontos.
- $\Delta\lambda$ é a diferença entre as longitudes dos dois pontos.
- $R$ é o raio da Terra (em quilômetros ou milhas, dependendo da unidade desejada).
- $d$ é a distância calculada entre os dois pontos.

**Transferência via PIX**

O serviço de transferência via PIX foi projetado para garantir tanto a funcionalidade quanto a segurança das transações. O sistema recebe do usuário as informações necessárias, como os dados do destinatário e o valor a ser transferido. Com base no modo de operação, normal ou pânico, o serviço ajusta automaticamente o limite disponível para transferência. No modo normal, o usuário pode realizar transferências de acordo com o saldo real da conta. Já no modo pânico, o sistema limita o valor disponível, exibindo um saldo fictício previamente configurado, garantindo a ativação discreta da funcionalidade.

A validação da transação é feita através da senha de transferência, que deve ser inserida corretamente para autorizar o envio do valor. Além disso, o microserviço de transferência via PIX integra o serviço de localização por GPS, registrando as coordenadas geográficas (latitude e longitude) do dispositivo no momento da transação. Essas informações são enviadas para o banco de dados, permitindo o monitoramento em tempo real das operações e aumentando a rastreabilidade das movimentações financeiras.

**Score**

O último microserviço é responsável por gerar e atualizar o score de segurança do usuário em tempo real, desempenhando um papel no monitoramento das condições de segurança associadas à conta. Esse score é calculado com base em inputs extraídos de outros microserviços.

Entre os dados utilizados pelo microserviço estão o nível do modo pânico ativado, a distância em relação ao ponto seguro (safe point) e o número de movimentações estranhas registradas nas últimas 12 horas. Esses fatores são processados continuamente para calcular um score que reflete a condição de segurança atual do usuário.

A distância em relação ao ponto seguro (safe point) e o número de movimentações estranhas subtraem até 20 pontos cada no cálculo do score. Já a ativação do modo pânico tem um impacto mais significativo: o nível 1 reduz 30 pontos do score, enquanto o nível 2 subtrai 60 pontos, refletindo o maior grau de risco associado.

Com esses critérios, o score máximo de 100 pontos é alcançado por contas consideradas muito seguras, enquanto, em situações de alto risco, quando todas as condições

são desfavoráveis, o score pode chegar a 0 pontos. Esse modelo fornece uma métrica clara e detalhada para avaliar a segurança da conta em tempo real, auxiliando na tomada de decisões para aumentar a proteção do usuário.

**Arquitetura dos serviços**

A pasta app é o núcleo principal do aplicativo, onde todas as páginas e componentes dos serviços estão organizados. No contexto do Expo Router, essa estrutura é baseada em arquivos, permitindo que cada arquivo dentro da pasta represente uma rota específica no aplicativo.

Dentro da pasta app, encontra-se a subpasta tabs, que agrupa os componentes relacionados à navegação por abas. Essa estrutura é utilizada para gerenciar seções distintas do aplicativo, acessíveis por meio de uma barra de navegação. Isso permite que funcionalidades, como um painel principal ou ferramentas específicas, sejam separadas de maneira lógica.

O arquivo _layout.tsx desempenha um papel importante na definição do layout base do aplicativo. Ele age como um "wrapper", encapsulando elementos compartilhados entre as páginas, como cabeçalhos, rodapés e barras de navegação.

O arquivo index.tsx representa a página de login do aplicativo mapeada para a rota principal (/). Ele serve como ponto de entrada para o usuário. Complementando essa funcionalidade, o arquivo mainPanel.tsx gerencia a tela do menu, que contém informações resumidas, como saldo, transações recentes e atalhos para recursos adicionais do aplicativo.

A funcionalidade de segurança está centralizada no arquivo safety.tsx, que gerencia recursos como o monitoramento do score de segurança, configurações do modo pânico e a análise de comportamentos suspeitos. Já o arquivo transactionStatement.tsx é responsável por exibir o extrato bancário do usuário. Para as transferências financeiras, o arquivo transactionTransfer.tsx gerencia o processo de envio de valores, como no caso de transações via PIX.

Outro elemento da estrutura é o arquivo +not-found.tsx, que é utilizado para lidar com rotas inexistentes ou inválidas. Quando o usuário tenta acessar uma página que não está definida, o Expo Router redireciona para essa página, que exibe uma mensagem apropriada, como "Página não encontrada"ou "Erro 404".

A organização dessa estrutura modularizada e baseada em rotas promove uma separação clara de responsabilidades. Cada arquivo é dedicado a uma funcionalidade específica, o que facilita a manutenção e o desenvolvimento do aplicativo.

### 5.2.3 Camada de Dados

O Firebase Cloud Firestore é um banco de dados NoSQL, o que significa que ele é não relacional. Diferente de bancos de dados relacionais, como o MySQL ou o PostgreSQL, que organizam os dados em tabelas e colunas com relacionamentos entre elas, os bancos de dados não relacionais como o Firestore armazenam os dados de maneira mais flexível em formato de documentos e coleções.

Em vez de uma estrutura rígida de tabelas com chaves primárias e estrangeiras, o Firestore permite armazenar dados de forma mais livre, onde cada documento pode ter diferentes campos e tipos de dados, sem a necessidade de um esquema fixo. A principal vantagem desse banco de dados é a flexibilidade. Ele permite que os desenvolvedores modifiquem a estrutura dos dados sem a necessidade de alterar todo o banco de dados, o que é particularmente útil em aplicativos em constante evolução como este.

Além disso, o Firestore oferece escalabilidade horizontal, permitindo que o banco de dados cresça de acordo com as necessidades da aplicação, sem se preocupar com limitações de capacidade de uma única máquina.

Foram criadas três coleções principais no Firebase Cloud Firestore: "usuarios", "transferencias"e "extrato". Cada uma dessas coleções tem um papel na organização e no armazenamento dos dados do aplicativo.

A coleção "usuarios"armazena os dados pessoais e informações de conta de cada usuário, como nome, e-mail, número de telefone, saldo, limites de crédito, histórico de transações e configurações de segurança, incluindo informações sobre o modo pânico e autenticação biométrica. Na tabela abaixo estão todos os parâmetros com exemplos criados para um documento dessa coleção.

| Campo | Valor | Tipo de Dado |
|---|---|---|
| agencia | 1234 | string |
| banco | 01 | string |
| biometria | true | boolean |
| celular | +55 11 98765-4321 | string |
| cep | 03646-000 | string |
| conta | 56789-0 | string |
| dataUltimoAcesso | 21:38 26/11/2024 | string |
| email | igoor.costa@usp.br | string |
| emprestimo | 40000 | number |
| fatorPanico1 | 0.1 | number |
| fatorPanico2 | 0.05 | number |
| idade | 23 | number |
| investimentos | 35000 | number |
| latitudeSegura | -23.5234132 | number |
| limiteCredito | 10000 | number |
| longitudeSegura | -46.5301852 | number |
| modoPanico | 1 | number |
| nome | Igor | string |
| senhaNormal | 123456 | string |
| senhaPanico | 000000 | string |
| senhaTransferencias | 123456 | string |

**Tabela 14 :** Estrutura do Banco de Dados do Usuário.

A coleção "transferencias"é responsável por armazenar as informações relacionadas a cada transação realizada no aplicativo. Ela inclui dados como o valor transferido, o destinatário e a data e hora da transferência. Esse armazenamento permite que o sistema registre o histórico de todas as transferências realizadas, facilitando tanto o acompanhamento pelo usuário quanto a análise de comportamentos suspeitos em caso de necessidade de investigação.

| Campo | Valor | Tipo de Dado |
|---|---|---|
| data | 15/11/24 | string |
| hora | 09:15 | string |
| latitude | -52.431234 | string |
| longitude | -43.123543 | string |
| nome | Paulo | string |
| nomeOrigem | Wanderlei | string |
| userId | Vq7YvNTBo1NB6qIF6i9h2dSGAZI3 | string |
| userIdOrigem | 541dQu6vvAK98f260dmG2afRAfr2 | string |
| valor | 100 | number |

**Tabela 15 :** Estrutura de Dados de Transferências.

Por fim, a coleção "extrato"armazena o histórico financeiro do usuário, incluindo

todas as movimentações realizadas na conta, como depósitos, pagamentos, transferências e outros ajustes. Cada documento nesta coleção contém detalhes sobre a transação, incluindo o valor, a descrição, a data e o saldo atualizado após a operação.

| **Campo** | **Valor** | **Tipo de Dado** |
|---|---|---|
| data | 01/11/24 | string |
| hora | 08:23 | string |
| nome | Remuneração | string |
| nomeOrigem | Salário | string |
| userId | 3cbvQu6vvYX6zf260dmG2afRAfr2 | string |
| valor | 15000 | number |

**Tabela 16 :** Estrutura de Dados de Extrato.

# 6 TESTES

## 6.1 Testes e Validações

A seção de testes e validações tem como objetivo assegurar que as soluções e o MVP desenvolvido atenda aos requisitos e funcionalidades estabelecidos no início do projeto. Esta etapa é importante para garantir a qualidade do sistema, identificar possíveis falhas e otimizar a performance. Os testes realizados abrangem diferentes aspectos, como segurança, usabilidade, e a integração dos serviços principais.

### 6.1.1 Testes Realizados

Foram realizados vinte testes para verificar se o MVP atendia aos requisitos estabelecidos para o projeto. Os testes foram focados em avaliar os serviços isoladamente, garantindo que cada módulo funcionasse de forma independente e sem falhas.

Primeiramente, foi conduzido um teste específico para validar o processo de autenticação, com o objetivo de verificar se os métodos de login e segurança estavam funcionando corretamente. Para a autenticação, foram realizados testes abrangendo diferentes cenários, conforme descrito abaixo:

1. O usuário entrou primeiramente no modo pânico e depois foi para o modo normal.
2. O usuário entrou primeiramente no modo normal e depois no modo pânico.
3. O usuário entra no modo normal e permanece no modo normal.
4. O usuário entra no modo pânico e permanece no modo pânico.
5. Testes da autenticação por biometria de impressão digital.
6. Testes sobre o que ocorre caso o Wi-Fi ou GPS esteja desativado.

Foram realizados alguns testes para verificar a comunicação com o banco de dados na nuvem. Os testes incluíram os seguintes cenários:

1. Teste com o celular sem acesso à internet, verificando como o sistema lida com a falta de conexão.
2. Teste com a inserção de senhas erradas, para avaliar a segurança e a resposta do sistema em casos de falha de autenticação.
3. Teste para resetar o banco de dados, verificando se o sistema consegue restaurar corretamente o estado inicial e os dados padrão.

Depois, foram realizados testes para validar o serviço de localização. Os testes incluíram os seguintes cenários:

1. Teste do funcionamento do sistema com a permissão de localização negada.

2. Teste do sistema com a localização desligada.
3. Teste do cálculo da distância entre dois pontos geográficos para verificar a precisão dos dados fornecidos.

Também foram realizados testes para validar as transferências via PIX. Os testes incluíram os seguintes cenários:

1. Tentar transferir valores maiores que o saldo disponível, ou valores zerados e negativos.
2. Tentar transferir para uma conta inexistente.
3. Realizar uma transferência com o GPS desligado, verificando o impacto na segurança e validação da transação.
4. Digitar a senha errada durante a transação, avaliando a resposta do sistema a falhas de autenticação.

Por fim, foi testado o serviço de score em diversas situações para validar seu comportamento. Os testes incluíram os seguintes cenários:

1. Todas as condições de segurança estavam favoráveis, resultando em um score de 100.
2. Apenas um fator de segurança foi aplicado, com peso de 20 pontos, resultando em um score de 80.
3. Modos de pânico 1 e 2 foram ativados, verificando a penalização do score em cada nível.
4. O modo de score foi zerado, avaliando a resposta do sistema em uma situação de risco extremo.

### 6.1.2 Comparação de Resultados Esperados vs Resultados Obtidos

Cada teste foi projetado para avaliar aspectos funcionais e operacionais do sistema, garantindo o funcionamento independente de cada módulo.

Nos testes de autenticação, o aplicativo respondeu de forma adequada às combinações de senhas, apresentando o comportamento esperado em cada uma das quatro possibilidades de uso entre os modos normal e pânico. Para os testes de autenticação biométrica, bastou que o usuário permitisse o uso da biometria no aplicativo para que o recurso funcionasse corretamente. Já em situações em que o celular ficou sem sinal, a página de login não conseguiu se comunicar com a nuvem, mas retornou um aviso claro sobre a indisponibilidade de rede.

Os testes com o banco de dados também apresentaram resultados dentro do es-

perado. Em qualquer página acessada pelo usuário, a falta de conexão Wi-Fi impede a atualização das informações, mas o sistema exibe um aviso sobre a indisponibilidade de rede. No caso de inserção de uma senha incorreta durante o login, o aplicativo retorna uma mensagem informando que as credenciais estão incorretas.

Por fim, foi implementado um serviço acionado ao clicar na logo da página de login, projetado para resetar o banco de dados do Firebase. Esse recurso apresentou um comportamento inesperado em alguns casos, criando duplicatas do mesmo usuário. Esse problema foi identificado como um ponto de melhoria.

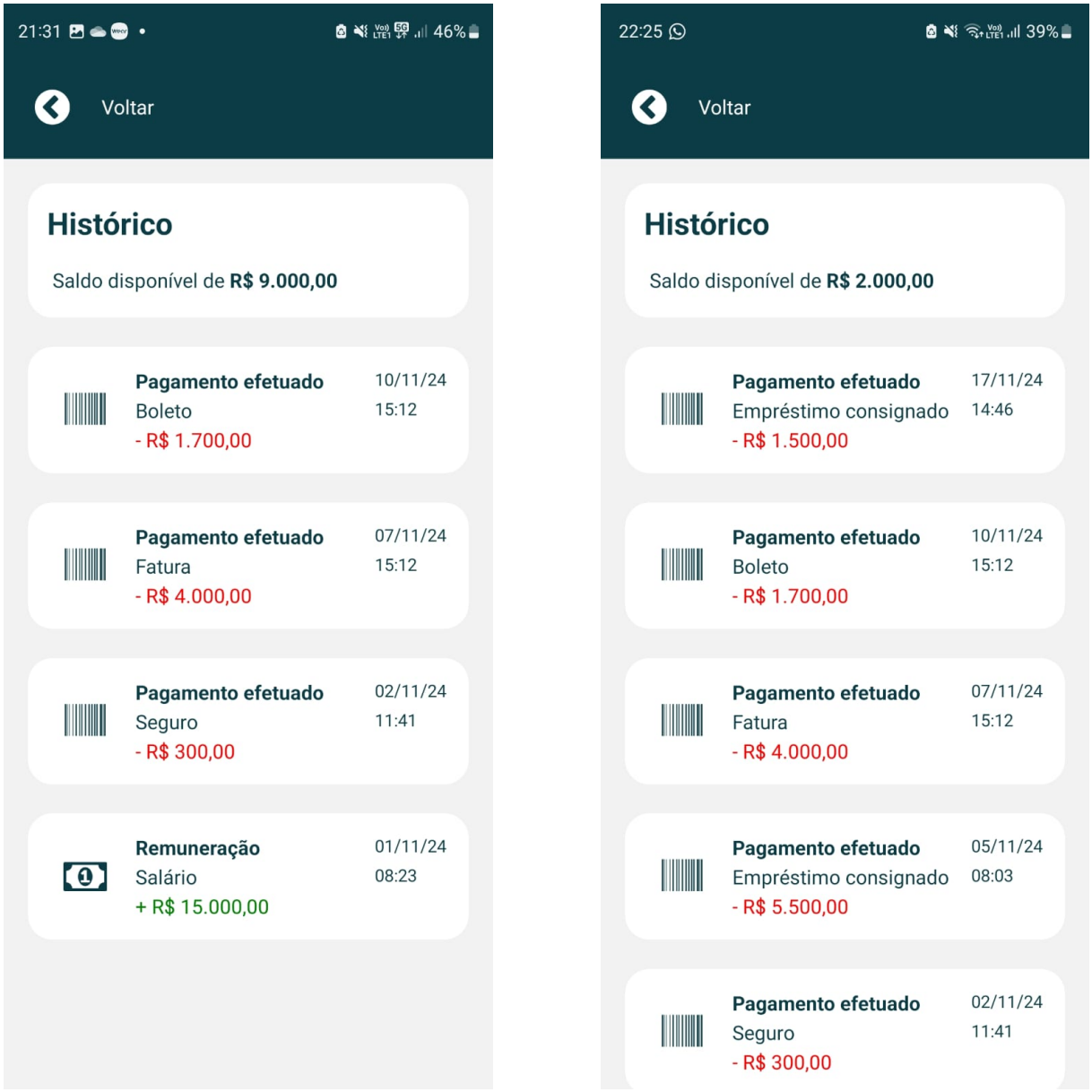
Os testes de localização apresentaram resultados alinhados com os objetivos projetados. Quando a permissão de localização era negada, o aplicativo permanecia na página de login, exibindo um aviso sobre a necessidade de conceder o acesso à localização para prosseguir.

Nos casos em que a localização estava desligada ou o dispositivo estava em modo avião, as funcionalidades principais do aplicativo continuaram funcionando normalmente. Contudo, o score de localização foi impactado negativamente, com uma redução de 20 pontos. Já o cálculo de distâncias foram validados utilizando o algoritmo do Google Maps, com variações de apenas dezenas de metros, confirmando a confiabilidade do sistema para a localização do safe point.

Os testes realizados para validar o sistema de transferências via PIX foram bem-sucedidos. Tentativas de transferir valores maiores que o saldo disponível no modo pânico, bem como valores zerados ou negativos, foram corretamente rejeitadas com a exibição de avisos ao usuário. O mesmo ocorreu ao tentar realizar transferências para contas inexistentes no banco de dados ou ao inserir uma senha incorreta.

Quando o GPS estava desligado durante uma transferência, o sistema enviava valores nulos para latitude e longitude, indicando a ausência de dados de localização, mas sem comprometer a operação.

As imagens abaixo ilustram o extrato nos modos normal e pânico, onde é possível observar que pagamentos foram criados no modo pânico para reduzir o saldo disponível, funcionando conforme o esperado.

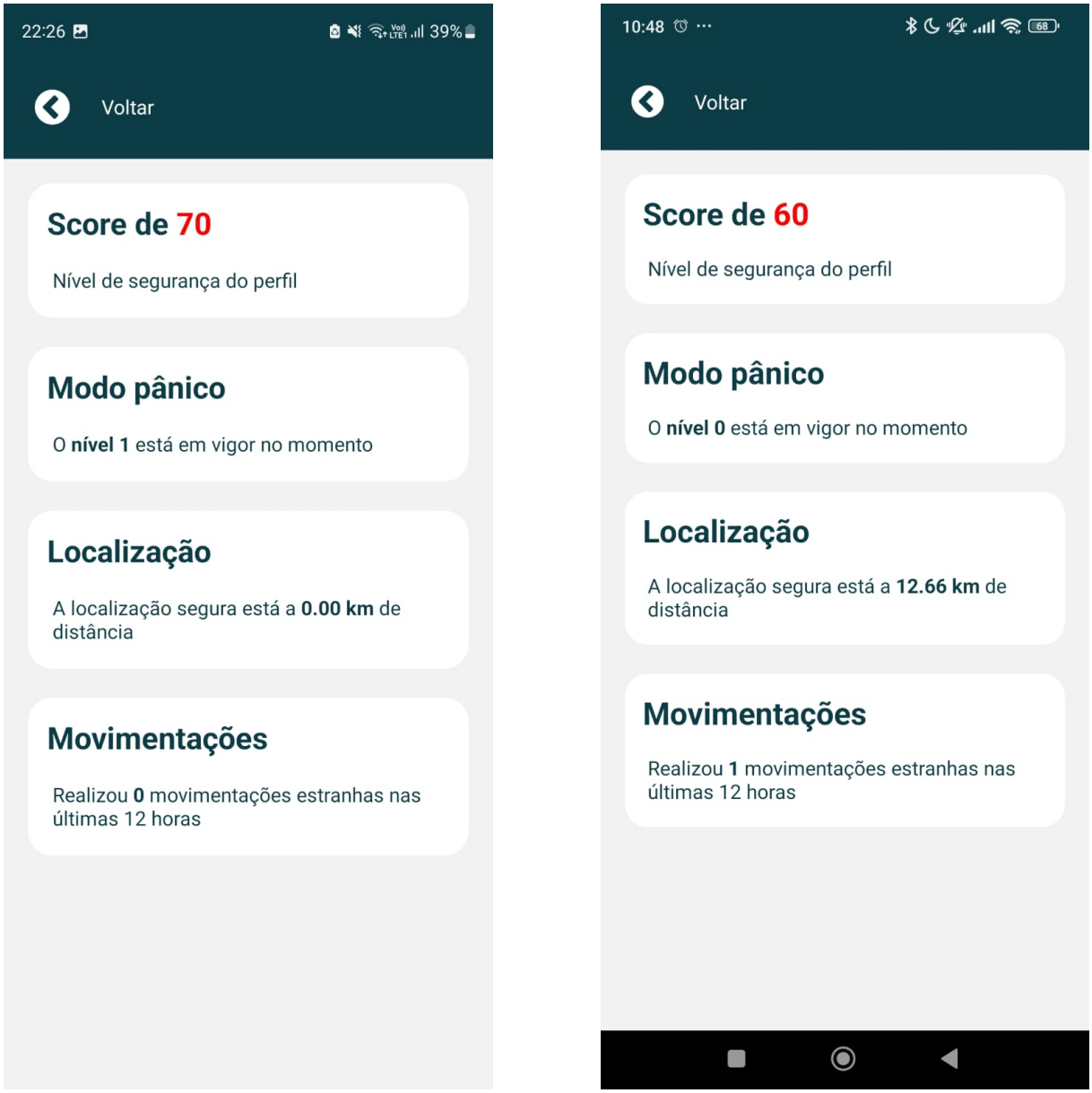



**(a)** Extrato no modo normal. **(b)** Extrato no modo pânico.

**Figura 18 :** Páginas do extrato com diferentes níveis para o modo pânico.

Por fim, o último teste validou o funcionamento do score de segurança do sistema em diferentes situações. Quando o aplicativo operava no modo normal e todas as condições eram consideradas seguras, o score atingia o valor máximo de 100. À medida que estados de alerta eram acionados, o score diminuía gradativamente, podendo chegar a 0.

As figuras abaixo ilustram duas situações distintas do score do usuário, destacando como o sistema ajusta os valores de acordo com as condições de segurança identificadas.




**(a)** Score 70. **(b)** Score 60.

**Figura 19 :** Páginas do Score com diferentes níveis de segurança.

Os resultados dos 20 testes confirmaram que o MVP atende plenamente aos objetivos do projeto, demonstrando ser uma solução funcional, confiável e alinhada às necessidades identificadas nos requisitos estabelecidos.

### 6.1.3 Ajustes Feitos e Melhorias

Durante os testes realizados no MVP, alguns ajustes e melhorias foram implementados para otimizar o desempenho e a experiência do usuário.

Primeiramente, foi adicionada a funcionalidade de carregamento dinâmico de dados nas páginas, permitindo que o conteúdo seja carregado conforme o usuário rola o painel

para baixo. Um comportamento ainda presente no aplicativo é a exibição temporária de informações da última página acessada, por alguns milissegundos, ao trocar de tela. Esse atraso pode ser perceptível para o usuário, o que pode afetar a usabilidade do sistema. Esse problema ocorre devido ao uso de um banco de dados local e precisa ser ajustado para garantir uma transição mais suave entre as páginas.

Outro ponto importante foi a limitação dos testes realizados, que envolveram apenas dois perfis de usuários: vítima e sequestrador. Para melhorar a abrangência dos testes e garantir uma análise mais completa do sistema, será necessária a criação de outros perfis de usuário, permitindo simular diferentes cenários e transações entre um maior número de clientes.

Além disso, como os testes foram realizados exclusivamente em dispositivos Android, será necessário repetir todos esses testes em sistemas iOS e também em plataformas de web para garantir que o aplicativo funcione adequadamente em diferentes ambientes e dispositivos.

# 7 CONCLUSÃO

Este trabalho teve início com uma introdução que detalhou todos os termos e conceitos relacionados ao objeto de estudo. Foi realizada uma contextualização, apresentando os motivos que motivaram o desenvolvimento deste projeto, culminando em uma análise do estado da arte.

Foram especificados os requisitos tanto do sistema atual quanto do sistema proposto como solução para mitigar os danos causados pelo sequestro relâmpago. Diversas alternativas foram avaliadas, sendo a solução "pânico" escolhida como a mais adequada para desenvolvimento. Também foram analisados os atores envolvidos e como cada um impacta na implementação e operação dessa solução.

Durante o desenvolvimento, diversos artefatos de engenharia de software foram utilizados para fundamentar de forma robusta a análise de riscos do projeto, resultando em uma avaliação sólida e consistente.

Por fim, foi criado um protótipo funcional para validar os requisitos da solução "pânico", acompanhado de uma descrição detalhada do processo de desenvolvimento. Este protótipo poderá ser utilizado futuramente para realizar avaliações de usabilidade junto a usuários finais.

A solução pânico se mostrou uma solução sólida contra o problema dos sequestros relâmpagos, muito ainda deve ser analisado e avaliado, no entanto, acredita-se que com esse trabalho fica claro que a solução pela negação plausível é o melhor caminho para lidar com o roubo de ativos financeiros mediante extorsão.

# 8 REFERÊNCIAS


[1] Biblioteca Nacional. Bndigital, 2024. URL https://memoria.bn.gov.br/hdb/periodico.aspx. Plataforma de periódicos históricos digitalizados pela Biblioteca Nacional do Brasil.

[2] Secretaria de Segurança Pública do Estado de São Paulo. Dados Trimestrais - Estatísticas de Criminalidade, 2024. URL https://www.ssp.sp.gov.br/estatistica/dados-trimestrais. Acesso em: 29 nov. 2024.

[3] Senado Federal. Complemento 2 - Documentos Históricos, 2024. URL https://www2.senado.leg.br/bdsf/bitstream/handle/id/316287/complemento_2.htm?sequence=3&isAllowed=y. Acesso em: 29 nov. 2024.

[4] O Fluminense, Jornal do Estado do Rio. *O Fluminense*, Ano 120(35069), December 1997. Edição de 19 de dezembro de 1997.

[5] Pandemia acelera bancarização e transforma setor de meios de pagamento. *Febrabantech*, 2023. URL https://febrabantech.febraban.org.br/temas/meios-de-pagamento/pandemia-acelera-bancarizacao-e-transforma-setor-de-meios-de-pagamento. Acessado em: 29 Mar. 2024.

[6] Mp e febraban discutem como combater uso do pix em sequestros relâmpagos. *InfoMoney*, março 2023. URL https://www.infomoney.com.br/minhas-financas/mp-e-febraban-discutem-como-combater-uso-do-pix-em-sequestros-relampagos/. Acessado em: 29 Mar. 2024.

[7] Banco Central do Brasil. Pix - serão atualizadas as regras de segurança para novos dispositivos cadastrados, 2024. URL https://www.bcb.gov.br/detalhenoticia/20390/noticia. Acesso em: 29 nov. 2024.

[8] Diferentes senhas no banco do brasil. *Site Banco do Brasil*, 2024. URL https://www.bb.com.br/site/setor-publico/seguranca/senhas/. Acessado em: 29 Mar. 2024.

[9] Biometria facial: utilização por instituições financeiras na prevenção a fraudes. *Febrabantech*, 2023. URL https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/biometria-facial-utilizacao-por-instituicoes-financeiras-na-prevencao-a-fraudes. Acessado em: 29 Mar. 2024.

[10] Nubank. Nubank lança modo rua, função inovadora de segurança que limita transações no app ao sair de casa, 2022. URL https://international.nubank.com.b

r/pt-br/consumidores/nubank-lanca-modo-rua-funcao-inovadora-de-seguranca-que-limita-transacoes-no-app-ao-sair-de-casa/. Acessado em 21 nov. 2024.

[11] Blog PicPay. Picpay lança modo seguro que aumenta proteção dos usuários, 2024. URL https://meajuda.picpay.com/hc/pt-br/articles/26808643828243-Qual-a-diferen%C3%A7a-entre-os-tipos-de-prote%C3%A7%C3%A3o-saldos-protegidos-e-saldos-invis%C3%ADveis. Acessado em 21 nov. 2024.

[12] ZDNet. Best apps to hide apps and protect your privacy. 2024. URL https://www.zdnet.com.

[13] GPS Brasília. Regras do pix mudam a partir desta sexta-feira (1º), 2024. URL https://gpsbrasilia.com.br/regras-do-pix-mudam-a-partir-desta-sexta-feira-1o/. Accessed: 2024-11-22.

[14] William Stallings and Lawrie Brown. *Computer Security: Principles and Practice*. Pearson, 2nd edition, 2011.

[15] R. Shirey. Internet Security Glossary. Request for Comments 2828, Internet Engineering Task Force (IETF), May 2000. URL https://datatracker.ietf.org/doc/rfc2828/.

[16] Angela Whitten and Jeffrey D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium*, 1999.

[17] Com pix, número de sequestros no estado de sp bate recorde em 15 anos. *UOL Notícias*, janeiro 2023. URL https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2023/01/17/com-pix-numero-de-sequestros-no-estado-de-sp-bate-recorde-em-15-anos.htm. Acessado em: 29 Mar. 2024.

[18] Marcus Vinicius de Viveiro Dias. Enquadramento típico do chamado "sequestro-relâmpago". *Rev. Minist Públic, Rio de Janeiro, RJ*, 2005. URL https://www.mprj.mp.br/documents/20184/2779433/Marcus_Vinicius_de_Viveiros_Dias.pdf. Acessado em: 29 Mar. 2024.

[19] Esther Kimberly Rodrigues do Nascimento. Percepção dos usuários do mobile banking: confiabilidade, segurança, facilidade e intenções de uso. B.S. thesis, 2023. URL https://repositorio.ifpb.edu.br/bitstream/177683/2683/1/PERCEP%C3%87%C3%83O%20DOS%20USU%C3%81RIOS%20DO%20MOBILE%20BANKING-confiabilidade%2C%20seguran%C3%A7a%2C%20facilidade%20e%20inten%C3%A7%C3%B5es%20de%20uso.pdf. Acessado em: 29 Mar. 2024.

[20] Frederic de Mariz. How will the 2020 crisis accelerate the evolution of the banking system? In *Financial Transformations Beyond the COVID-19 Health Crisis*, pages 667–695. World Scientific, 2022. URL https://dl.acm.org/doi/abs/10.1145/3002170. Acessado em: 29 Mar. 2024.

[21] Malik Mustafa. Mobile banking app development and implementation. 2021. URL https://www.researchgate.net/profile/Editor-Ijmtst/publication/356775326_Mobile_Banking_App_Development_and_Implementation/links/61ab0a5650e22929cd452751/Mobile-Banking-App-Development-and-Implementation.pdf. Acessado em: 29 Mar. 2024.

[22] Cristian Ciurea. The development of a mobile application in a collaborative banking system. *Informatica Economica*, 14(3), 2010. URL https://www.revistaie.ase.ro/content/55/1007%20-%20Ciurea.pdf. Acessado em: 29 Mar. 2024.

[23] Shilpa Shaju and V Panchami. Bisc authentication algorithm: An efficient new authentication algorithm using three factor authentication for mobile banking. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, pages 1–5. IEEE, 2016. URL https://ieeexplore.ieee.org/abstract/document/7916852. Acessado em: 29 Mar. 2024.

[24] Özlem Durmaz Incel, Seçil Günay, Yasemin Akan, Yunus Barlas, Okan Engin Basar, Gülfem Isiklar Alptekin, and Mustafa Isbilen. Dakota: sensor and touch screen-based continuous authentication on a mobile banking application. *IEEE Access*, 9:38943–38960, 2021. URL https://ieeexplore.ieee.org/abstract/document/9367144. Acessado em: 29 Mar. 2024.

[25] JN Ndunagu and UJ Nwoduh. Development of an enhanced mobile banking security: multifactor authentication approach. *Electroscope Journal*, 10:33–42, 2019. URL https://electroscopejournal.org.ng/index.php/ej/article/view/11/11. Acessado em: 29 Mar. 2024.

[26] Nilay Yıldırım and Asaf Varol. Android based mobile application development for web login authentication using fingerprint recognition feature. In *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, pages 2662–2665. IEEE, 2015. URL https://ieeexplore.ieee.org/abstract/document/7130436. Acessado em: 29 Mar. 2024.

[27] Busalire Onesmus Emeka and Shaoying Liu. Security requirement engineering using structured object-oriented formal language for m-banking applications. In *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pages 176–183. IEEE, 2017. URL https://ieeexplore.ieee.org/abstract/document/8009921. Acessado em: 29 Mar. 2024.

[28] Harleen K Flora and Swati V Chande. A review and anaysis on mobile application development processes using agile methodlogies. *International Journal of Research in Computer Science*, 3(4):9, 2013. URL https://d1wqtxts1xzle7.cloudfront.net/34567478/1._Review_and_Analysis_on_Mobile_Application_development_Processes_Using_Agile_Methodlogies-libre.pdf?1409298590=&response-content-disposition=inline%3B+filename%3DA_Review_and_Analysis_of_Existing_Agile.pdf&Expires=1711675450&Signature=WnxUOXnfbgCsjcDq5r5tq5O4bWjdBy5RFHa-ucmzxYEAXQ4zmzAZZmajf2QWELErCM-7CwQc~nVpifb7hGrE9EKCCoy03s5lAaujPce7AxodwL6GVOYFn7DPYw-fY-sWXhJ3OYnM7pA9yyvTHVXGFKCt4JCRv0R9sgVcLYjewywZ6HzjfkCMCJlAdQwtRZSXAzLILix2MPD2qWgrxa~MRHtzBUr5rpkaPtRfktan8OtzHwVWkIT16zKOL1aURL4row~8jzHoKnKA6R~-QwkpF79UORYUxyqzpDFsTRuS0fHLW6ULVJrK3ueUlhI8hD1t0Vt5Bz8KMUwU058MIHTWXQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acessado em: 29 Mar. 2024.

[29] Neymis Misiko Jacob. A review of mobile application development in the agile software development environment. *Global Journal of Computer Science and Technology*, 19(C1):19–22, 2019. URL https://gjcst.com/index.php/gjcst/article/view/447/441. Acessado em: 29 Mar. 2024.

[30] Vincent Bindschaedler, Reza Shokri, and Carl A Gunter. Plausible deniability for privacy-preserving data synthesis. *arXiv preprint arXiv:1708.07975*, 2017. URL https://arxiv.org/abs/1708.07975. Acessado em: 29 Mar. 2024.