Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Identificação de fatores adicionais de segurança e sua aplicabilidade na identidade gov.br

Sandro Leite Furtado

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientador
Prof. Dr. George Marsicano Corrêa

Brasília
2025

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Identificação de fatores adicionais de segurança e sua aplicabilidade na identidade gov.br

Sandro Leite Furtado

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. George Marsicano Corrêa (Orientador)
CIC/UnB

Prof. Dr. John Lenon Cardoso Gardenghi
FCTE/UnB

Prof. Dr. Milton Vinicius Morais de Lima
Instituição CISSA/CESAR

Prof.a Dr.a Edna Dias Canedo
Coordenadora do Programa de Pós-graduação em Computação Aplicada

Brasília, 18 de fevereiro de 2025

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Li Leite Furtado, Sandro
Identificação de fatores adicionais de segurança e sua aplicabilidade na identidade gov.br / Sandro Leite Furtado; orientador George Marsicano Corrêa. Brasília, 2025.
103 p.

Dissertação(Mestrado Profissional em Computação Aplicada) Universidade de Brasília, 2025.

1. Duplo fator de autenticação. 2. Identidade digital. 3. Autenticação digital. 4. Risco baseado em autenticação. 5. Segurança da informação. I. Marsicano Corrêa, George, orient. II. Título.

Dedicatória

Dedico esta dissertação, antes de tudo, à memória do meu querido avô, cuja sabedoria ecoa em cada página deste trabalho. Ele sempre nos lembrava: "Estude, pois o conhecimento ninguém pode tirar de você." Essas palavras foram meu farol ao longo da jornada acadêmica, reforçando que o aprendizado é um tesouro imutável, imune ao tempo e às adversidades.

Meu mais profundo agradecimento e eterna saudade. Que este trabalho seja uma homenagem ao legado de dedicação e amor pelo conhecimento que ele tanto prezava.

Dedico também à minha esposa e família, cujo apoio inabalável me sustentou em cada desafio, e a todos que, de alguma forma, contribuíram para que esta conquista se tornasse realidade. Ao longo da vida, encontramos pessoas que nos impulsionam e outras que duvidam de nosso potencial, que esta dissertação seja a prova de que a determinação e o esforço superam qualquer expectativa imposta por outros.

Agradecimentos

À minha esposa, Sâmmara Ellen Renner Ferrão, pelo amor, paciência e apoio incondicional em cada etapa desta jornada. Sua compreensão e incentivo foram fundamentais para que eu pudesse seguir firme até aqui.

À minha família, em especial aos meus pais, que me ensinaram o valor do conhecimento e sempre estiveram ao meu lado, me incentivando a ir além. Aos meus irmãos e sobrinhos, pela torcida silenciosa, pelas palavras de motivação e por acreditarem em mim mesmo nos momentos em que duvidei de mim mesmo.

Aos meus amigos, que de perto ou de longe, direta ou indiretamente, contribuíram com palavras de incentivo, conselhos e momentos de descontração, fundamentais para manter o equilíbrio nesta caminhada.

Aos meus professores e especialmente meu orientador, George Marsicano Corrêa, por compartilharem conhecimento, abrirem portas para novas ideias e me guiarem com paciência e sabedoria ao longo deste processo. E, por fim, a todos que, de alguma forma, fizeram parte deste percurso, meu mais sincero agradecimento. Cada gesto, cada palavra e cada apoio recebido foram essenciais para que este trabalho se tornasse realidade.

Muito obrigado!

Resumo

Contexto: A Identidade (ID) gov.br é utilizada para prover acessos a diferentes serviços públicos digitais. A ID gov.br é dividida em níveis de acesso e cada nível possui seu critério de ingresso. Diariamente agentes mal-intencionados tentam se apropriar de contas de terceiros para requisitar serviços públicos de natureza financeira na intenção de aplicar golpes no Governo, lesando o cidadão que é o real proprietário e detentor do benefício.
Objetivo: O objetivo geral deste trabalho é contribuir para análise e viabilidade em aprimorar a segurança de identificação e autenticação dos usuários na plataforma gov.br.
Método: Para isto, foi proposto e executado um protocolo de revisão sistemática da literatura (RSL) e na sequência será realizado um Estudo de Caso para aplicabilidade na ID gov.br.
Resultados: A pesquisa analisou 248 trabalhos identificados a partir da *string* de busca, resultando em 9 após a aplicação dos critérios de seleção e 5 após a avaliação de qualidade. A condução da RSL buscou contribuir para a identificação de cinco fatores adicionais de segurança em contextos de autenticação/identificação: RBA, Tripwire, login rituals, OTP e OTP com Bluetooth. Dentre esses, o RBA foi implantado e avaliado, demonstrando resultados na detecção de comportamentos atípicos e no bloqueio de acessos suspeitos, especialmente em situações de divergência de localidade de acesso. Este estudo evidencia os potenciais e desafios da aplicação de múltiplos fatores de autenticação no contexto das identidades digitais no Brasil.
Considerações: Esta dissertação empenhou-se em acrescentar para a segurança na plataforma gov.br ao identificar e avaliar fatores adicionais de autenticação. Entre os avanços, destaca-se a implementação do RBA, que demonstrou aspectos positivos ao agregar uma camada adicional de proteção contra acessos não autorizados. No entanto, foram identificados desafios técnicos, como a complexidade de implementação e a necessidade de maior transparência com os usuários. Este estudo estabelece uma base para futuras pesquisas e aplicações práticas, sendo relevante no desenvolvimento de identidades digitais no Brasil.

Palavras-chave: Identidade Digital, Autenticação Digital, Duplo Fator de Autenticação

Abstract

Context: The gov.br Identity (ID) is used to provide access to different digital public services. The ID gov.br is divided into access levels and each level has its entry criteria. Every day, malicious people try to take over third-party accounts to request public services of a financial nature with the intention of applying coups to the Government, harming the citizen who is the real owner and holder of the benefit.

Goal: The general goal of this work is to improve identification and authentication security of users on the gov.br ID platform.

Method: For this, a systematic literature review (SLR) protocol was proposed and executed and followning a Case Study methodology will be done for the applicability into gov.br ID.

Results: The research analyzed 248 works identified through the search string, resulting in 9 studies after applying the selection criteria and 5 after quality assessment. The SLR contributed to identifying five additional security factors for authentication/identification contexts: RBA, Tripwire, login rituals, OTP, and OTP with Bluetooth. Among these, RBA was implemented and evaluated, demonstrating results in detecting atypical behaviors and blocking suspicious accesses, especially in cases of location mismatch during access attempts. This study highlights the potential and challenges of applying multi-factor authentication in the context of digital identities in Brazil.

Considerations: This dissertation contributed to enhancing security on the gov.br platform by identifying and evaluating additional authentication factors. Among the advancements, the implementation of RBA stands out, as it provided positive results by adding an extra layer of protection against unauthorized access. However, technical challenges were identified, such as implementation complexity and the need for greater transparency with users. This study lays a foundation for future research and practical applications, playing a significant role in the development of more robust digital identities in Brazil.

Keywords: Digital Identity, Digital Authentication, Two-Factor Authentication

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

O Governo Federal está criando uma Identidade Digital (ID) que tem como proposta garantir a correta identificação do cidadão que, estando devidamente reconhecido, terá acesso a serviços públicos e dados pessoais seguindo as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD) [2].

A Secretaria de Governo Digital (SGD) da Secretaria de Desburocratização, Gestão e Governo Digital do Ministério da Economia (ME) possui como diretriz [3] prover plataformas tecnológicas que facilitem o cidadão a utilizar os serviços públicos. O Governo Federal publicou por meio do Decreto nº 10.332,de 28 de abril de 2020 a Estratégia de Governo Digital 2020-2022 (EGD) [4], consta entre seus objetivos a iniciativa "12.2.Disponibilizar identidade digital ao cidadão, com expectativa de emissão de quarenta milhões", até 2022.

A SGD responsável por gerir e fomentar o uso da plataforma ID gov.br e sobretudo salvaguardar os dados de +120 (cento e vinte) milhões de IDs criadas. Essas IDs concedem acesso a mais de 3 (três) mil serviços públicos digitais. Para autenticação do cidadão na plataforma ID gov.br são necessários mecanismos de identificação e autenticação. A identificação é uma combinação de características ou atributos que tornam uma pessoa única para a ID gov.br enquanto a autenticação é uma forma de validar a veracidade de algo ao alguém.

Soluções de autenticação por si sós, com senha estáticas, podem muitas vezes ser vulneráveis a ataques e por isso, fatores adicionais de autenticação são utilizados para melhorar este processo. O fato adicional de autenticação pode ser entendido como a utilização de mais de um componente para ratificar a identidade do usuário no processo de autenticação.

Neste contexto, o objetivo desta pesquisa é melhorar a segurança de identificação e autenticação dos usuários na plataforma ID gov.br buscando por fatores adicionais de autenticação na literatura que possam ser aplicados na ID do Governo Federal. A metodo-

logia adotada consiste em uma Revisão Sistemática da Literatura (RSL)[5], que permitiu identificar soluções emergentes no campo de autenticação digital, e em um estudo de caso que avaliou a implementação prática dessas soluções na plataforma gov.br. Após avaliação dos mecanismos adicionais selecionados pela RSL, uma avaliação pragmática sobre a validade dos mecanismos em relação a segurança, usabilidade e impacto de implementação foi efetuada.

O Risco Baseado em Autenticação (RBA) foi o mecanismo com maior avaliação de adaptabilidade ao cenário da plataforma gov.br e seguiu os passos do protocolo de estudo de caso. A implementação do RBA demonstrou que o RBA pode contribuir para aprimorar a segurança da plataforma, reforçando a importância de estratégias proativas na mitigação de riscos associados aos roubos de identidade, fraudes financeiras e crimes cibernéticos contribuindo para a evolução tecnológica da plataforma.

1.1 Problema de Pesquisa

A facilidade do login único para acesso a serviços de Governo tornou-se um atrativo para as agentes mal-intencionados, uma vez que o roubo ou sequestro de uma ID dessa plataforma, pode ser utilizada, por exemplo, para solicitar benefícios sociais no INSS, cita-se ainda outros serviços de cunho tributários e trabalhistas, caso o cidadão vítima possua esse direito.

Segundo a Diretoria de Identidade Digital, no último trimestre de 2021, a plataforma ID gov.br foi alvo de robôs na criação de contas, eles se valeram da exploração do Carrossel de Perguntas, em inglês *Knowledge-based authentication* (KBA), essa vulnerabilidade permitiu que fossem criadas aproximadamente 1.2 milhões de contas. Posteriormente identificadas essas contas foram excluídas da plataforma e a brecha de segurança foi sanada.

Esse cenário reforça a importância dessa plataforma que possui alta criticidade. Nesse sentido, a lacuna identificada, que este trabalho visar contribuir, está relacionada à fatores adicionais de autenticação a serem analisados e implementados em plataformas de autenticação cujo o objetivo é garantir que o cidadão seja o fiel proprietário de sua identidade no momento da criação de sua conta e em um segundo momento quando de sua utilização. A plataforma ID gov.br será utilizada para avaliar a hipótese proposta neste trabalho afim de aprimorar a sua segurança de autenticação com uma camada adicional de proteção para o cidadão.

1.2 Justificativa

Com a crescente digitalização de serviços, os vazamentos de dados pessoais tornaram-se um problema recorrente, gerando impactos negativos tanto para indivíduos quanto para organizações. Estudos apontam que, entre 2021 e 2024, houve um aumento expressivo no número de incidentes de segurança envolvendo informações sensíveis, como CPF, nome e data de nascimento [6], [7]. Esses vazamentos ocorrem, muitas vezes, devido a falhas na infraestrutura tecnológica das instituições, ataques cibernéticos sofisticados ou até mesmo negligência no tratamento de dados, expondo milhões de cidadãos a fraudes e golpes financeiros [8], [9].

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em agosto de 2020, as instituições públicas e privadas tem despendido esforços para adequarem seus processos bem como seus sistemas a nova legislação. Segundo Menegazzi [10], a dificuldade em se entender e aplicar a norma, aliada a falta de profissionais de Tecnologia da Informação (TI) capacitados com esse conhecimento jurídico, faz com que essa adequação avance em ritmo lento.

A proteção de dados pessoais é uma obrigação regulatória estabelecida pela LGPD. No entanto as recorrentes tentativas de roubo e sequestro de identidades, atividades ilícitas que infringem essa legislação, estão aumentando substancialmente por fraudadores que conseguem acesso a dados pessoais de vítimas. Algo relativamente fácil considerando os recentes vazamentos de atributos, tais como CPF, Nome, Data de Nascimento [6, 7, 8, 9, 11, 12].

Outrossim, torna-se essencial adotar estratégias que ampliem a resiliência das infraestruturas digitais e reforcem a proteção dos dados pessoais. A conscientização dos usuários sobre boas práticas de segurança, o fortalecimento das normas de conformidade e a aplicação rigorosa das penalidades previstas na LGPD são medidas fundamentais para minimizar riscos [12]. Além disso, a cooperação entre órgãos reguladores e empresas do setor de tecnologia pode contribuir para o desenvolvimento de soluções inovadoras que reduzam a incidência de vazamentos e garantam maior privacidade e segurança à população.

Neste sentido, considerando a exploração não autorizada de dados e a obrigação regulatória de proteção de dados pessoais, principalmente em virtude de vários incidentes de vazamentos ocorridos, elevou-se a preocupação com a privacidade de dados assim como a necessidade de identificação de como fatores adicionais de segurança podem auxiliar no enfrentamento dessa vulnerabilidade, o que justifica a execução deste trabalho.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é buscar contribuir para melhoria da segurança de identificação e autenticação dos usuários na plataforma ID gov.br.

1.3.2 Objetivo Específico

Para alcançar o objetivo geral deste trabalho, os seguintes objetivos foram definidos:

OE.1 Identificar na literatura os trabalhos que contenham fatores adicionais de autenticação de segurança aplicados a uma Identidade Digital;

OE.2 Avaliar a aplicabilidade dos fatores adicionais de autenticação de segurança identificados na plataforma ID gov.br e propor melhorias no fluxo de autenticação;

OE.3 Avaliar os benefícios e/ou problemas identificados após a aplicação.

1.4 Fronteira de Pesquisa

Este trabalho delimita seu escopo ao explorar a aplicação da autenticação baseada em risco (RBA) como um mecanismo de segurança complementar para a plataforma gov.br. O objetivo central é investigar a viabilidade e o impacto da implementação do RBA, visando fortalecer a segurança da identidade digital dos usuários. Nesse sentido, algumas abordagens amplamente reconhecidas na área de segurança da informação, desenvolvimento de software seguro e defesa cibernética não foram contempladas diretamente na pesquisa, seja por sua abrangência ou por não estarem no escopo metodológico definido.

Embora o campo da segurança da informação e do desenvolvimento de software seguro ofereça uma gama de abordagens, esta pesquisa optou por concentrar seus esforços no RBA. Consequentemente, algumas metodologias e *frameworks* amplamente reconhecidos não foram explorados em profundidade.

É importante ressaltar que a pesquisa não se dedica a uma análise exaustiva de vulnerabilidades do gov.br sob a ótica do OWASP Top 10. A atenção está voltada para a implementação do RBA, sem realizar um mapeamento específico de vulnerabilidades.

Da mesma forma, a correlação entre os vetores de ataque catalogados pelo MITRE ATT&CK e as soluções de segurança propostas não foi objeto de investigação detalhada. O modelo *Cyber Kill Chain*, embora relevante para a compreensão do ciclo de ataques cibernéticos, não foi utilizado como base para avaliar a eficácia do RBA.

O ciclo de desenvolvimento de software, incluindo práticas de DevSecOps e estratégias de codificação segura, também não foram abordados. A pesquisa reconhece a importância dessas práticas, mas delimitou-se por na implementação do RBA em si.

Este estudo também não tem como escopo a identificação, categorização ou análise de ameaças cibernéticas, como *phishing*, *malware*, ataques de força bruta ou exploração de vulnerabilidades. Embora o conceito de autenticação baseada em risco esteja relacionado à mitigação de alguns desses riscos, a dissertação não propõe uma taxonomia de ameaças, tampouco se aprofunda na defesa contra ataques cibernéticos avançados.

Adicionalmente, a análise da arquitetura completa da plataforma gov.br e a proposição de mudanças estruturais em seus componentes internos estão fora do escopo desta pesquisa. O foco reside na viabilidade e no impacto do RBA, sem realizar comparações aprofundadas com outras plataformas de autenticação governamentais.

1.5 Estrutura do Trabalho

Este trabalho está organizado da seguinte maneira: O Capítulo 2 apresenta a fundamentação teórica necessária para a elaboração deste trabalho, bem como os trabalhos correlatos.

O Capítulo 3 demonstra o design da pesquisa e quais foram os métodos definidos, além das fases e objetivos de cada uma delas. Além disso, registra a execução da revisão sistemática de literatura e a aplicação do estudo de caso na plataforma gov.br.

O Capítulo 4 apresenta os resultados, limitações do estudo e ameaças à validade do estudo executado por esta dissertação.

Por fim, o Capítulo 5 discorre sobre as considerações finais e trabalhos futuros.

Capítulo 2

Referencial Teórico

Este capítulo tem como objetivo conceitualizar os elementos chave discorridos ao longo do trabalho. Sendo eles similares e complementares entre si é necessário que estejam delimitadas as suas definições. Na Seção 2.1, são apresentados os conceitos iniciais sobre identificação e autenticação, trazendo que as características e particularidades de uma pessoa são formas de inferir sua identificação. Por parte da Identidade Digital, Seção 2.2, esclarece-se sobre a perspectiva do usuário e como ele interage de maneira exclusiva no mundo digital, o bem como o ciclo de vida da identidade e apresenta-se os princípios e níveis da Identidade gov.br no contexto brasileiro. Por fim, na Seção 2.3, e ainda dentro da contextualização, define-se como um elemento adicional pode garantir uma maior segurança a plataforma.

2.1 Identificação e Autenticação Digital

Uma identidade se refere a combinação de características ou atributos que torna uma pessoa única em dado contexto [1]. O processo de identificação estabelece/determina a identidade de uma pessoa coletando e provando informações relevantes da identidade [1]. Em outras palavras, a identificação é o processo de certificar que determinado atributo escolhido de uma entidade do mundo real demonstra pertencer a esta entidade [13]. Segundo o Guia ID4D [1], os sistemas de identificação ajudam a responder uma ou mais das seguintes questões:

- Quem é você?
- Você é aquele que diz ser?
- Você está autorizado ou elegível para alguma coisa?

Autenticação é o processo de determinar se alguém ou algo é, de fato, quem afirma ou declara ser [14]. Segundo Ashibani, Yosef e Mahmoud [15], existem dois tipos de

autenticação, que são explicíta e implícita. A autenticação implícita não necessita da intervenção do usuário, sendo que a explícita exige a intervenção. Segundo Ford [13], existem cinco métodos de autenticar uma pessoa: algo que a pessoa sabe, algo que a pessoa possui, algo que a pessoa é, local que a pessoa se encontra no momento da autenticação e estabelecimento de autenticação por terceiro confiável.

Os sistemas de identificação e autenticação, às vezes, podem acessar informações adicionais que extrapolam as fronteiras do próprio sistema de identificação, isto é, um intercâmbio de informações entre órgãos do Governo. Esta troca de informações faz-se necessária para complementar e validar a identificação de um usuário por aquela instituição. Em outras casos, o mesmo sistema de identificação pode fornecer atributos necessários para autorização ou determinação de elegibilidade.

2.2 Identidade Digital

O conceito de Identidade Digital (ID) pode ser entendido como uma representação exclusiva de uma pessoa envolvida em uma transação online[16]. Com o aumento da adoção de IDs, sobretudo com o uso de biometria na validação da pessoa, eleva-se a demanda de soluções para proteção contra a expansão de crimes virtuais e roubos de identidade[17]. A aplicação do conceito de ID carrega o desafio de verificar indivíduos em uma rede aberta, fornecendo terreno para oportunidades de roubos de identidade e outros ataques que reivindicam de maneira fraudulenta a ID de um outro indivíduo[16].

Para se identificar uma pessoa e usar a sua identidade em processos de identificação de um sistema é necessário uma série de etapas, chamadas de "ciclo de vida". Esse ciclo de vida é importante para estabelecer confiança em uma variedade de operações entre pessoas, provedores de identidade e entes púbicos e privados [1]. Esta série de etapas do ciclo de vida do processo de identificação está representada na Figura 2.1.

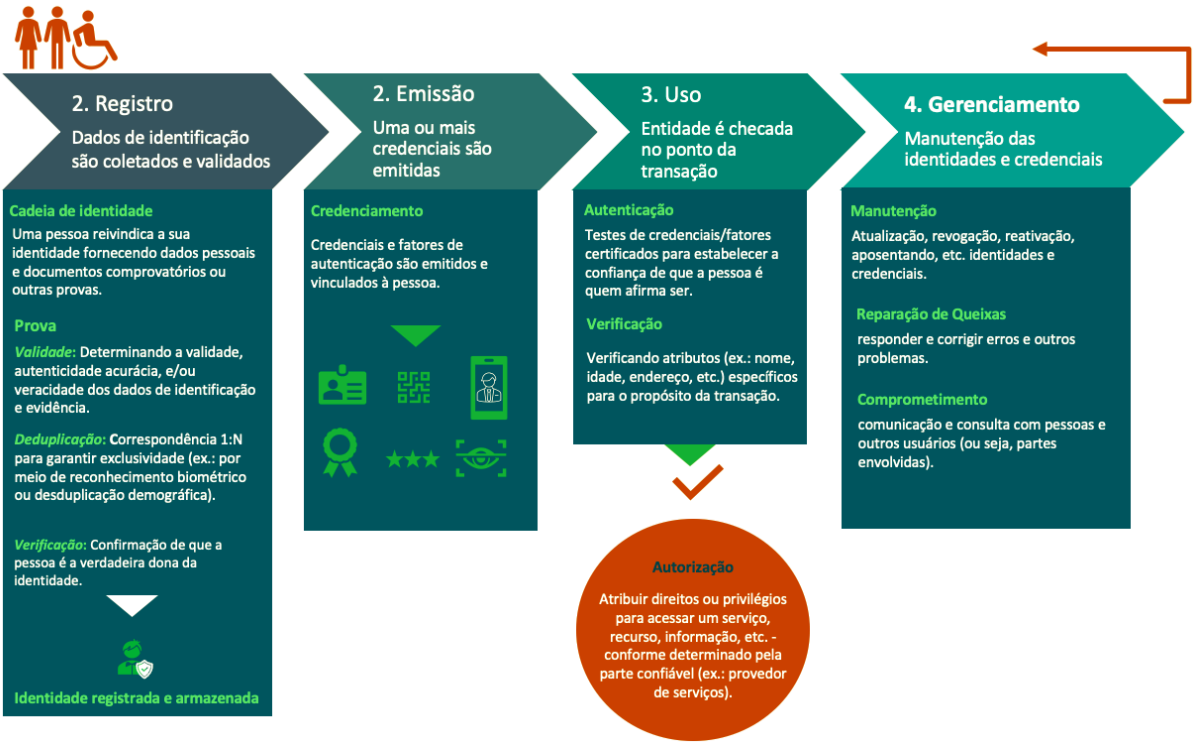

Figura 2.1: Ciclo de vida da identidade. Fonte: Autor adaptado em [1]

No Brasil, a Secretaria de Governo Digital (SGD) construiu a plataforma ID gov.br, sua solução de identidade digital que está em operação desde 2018. Neste primeiro trimestre de 2022 aplicação conta com mais de 126 (cento e vinte e seis) milhões de contas digitais. Tendo esta plataforma de autenticação conceitos de níveis de identidade, sendo elas: bronze, prata e ouro.

Cada um desses níveis possui um processo definido [18] em que o cidadão é submetido para obter a identidade gov.br. Os níveis e processos requeridos são:

ID - Bronze:

- Cadastro via formulário on-line para validação dos seus dados na Receita Federal;
- Cadastro via formulário on-line para validação dos seus dados no Instituto Nacional do Seguro Social (INSS);
- Cadastro via atendimento presencial nas Agências do INSS.

ID - Prata:

- Validação facial pelo aplicativo Identidade gov.br para conferência da sua foto nas bases da Carteira Nacional de Habilitação (CNH);

- Validação dos seus dados via internet *banking*, de um banco credenciado;
- Validação dos seus dados com usuário e senha do Sistema de Gestão de Pessoas do Governo Federal (SIGEPE), se você for servidor público federal;
- Validação dos seus dados via atendimento presencial nos postos do Departamento Nacional de Trânsito (DENATRAN).

ID - Ouro:

- Validação facial pelo aplicativo Identidade gov.br para conferência da sua foto nas bases da Justiça Eleitoral;
- Validação dos seus dados com Certificado Digital compatível com a Infraestrutura de Chaves Públicas Brasileira do Brasil (ICP-Brasil).

A identidade gov.br permite acesso a diferentes serviços públicos digitais, dessa forma, o cidadão não precisa se deslocar até um balcão de órgão público quando precisar se relacionar com o Estado. Uma visão geral da plataforma ID gov.br é apresentada na Figura 2.2.

Figura 2.2: Plataforma ID gov.br

Com a identidade digital gov.br é possível utilizar os diversos serviços públicos digitais ofertados pelos órgãos e integrados a plataforma. São eles serviços da saúde, serviços

estudantis, tais como, Exame Nacional do Ensino Médio (ENEM), Sistema de Seleção Unificada (SISU), Programa Universidade Para Todos (PROUNI) e Fundo de Financiamento Estudantil (FIES), permite também acessar e portar documentos como a Carteira Nacional de Habilitação (CNH) e o Cadastro de Pessoa Física (CPF), bem como acessar os serviços previdenciários, entre outros.

2.3 Fator Adicional de Autenticação

Os sistemas, em geral, utilizam mecanismos de autenticação estáticos, ou seja, baseados em senhas estáticas, sendo vulneráveis a vários tipos de ataque [19]. Tais vulnerabilidades podem ser mitigadas com a utilização de sistemas com multi-fator de autenticação (MFA), mais especificamente, de duplo fator de autenticação (2FA) [20]. Dessa forma, será utilizado mais de um tipo de elemento para garantir a autenticação, além da senha estática, o que poderia ser feito, dentre outros mecanismos, através do uso de biometria, smart cards e One-Time Passwords (OTP) [19].

OTP é um código gerado por meio de algoritmos, dependendo da configuração pode envolver a combinação de caracteres e símbolos, geralmente, são implementados como um fator adicional de segurança e pode haver uma temporalidade, esse código é utilizado apenas uma vez, tornando-se inválido na sequência [21].

A biometria é um traço comportamental, baseado em medidas biológicas, anatômicas e fisiológicas que podem ser capturadas e utilizadas para fins de reconhecimento. Existem diversas formas de geometria biométrica, tais como, reconhecimento facial, reconhecimento digital, reconhecimento de voz, reconhecimento de assinatura e padrões de pressionamento de tecla ou tela [22]. De acordo com Camp [23], a utilização de tecnologia biométrica para identificação e autenticação digital de indivíduos envolve o emprego de três (3) fases distintas:

1) Fase de Amostragem: Acontece a partir da captura de um conjunto de amostras de atributos biométricos de um indivíduo e, posteriormente, a utilização da medição média para produzir o modelo digital do indivíduo.

2) Fase de armazenamento: é feito a partir da criptografia do modelo digital e do armazenamento desse em um *token* de hardware (smartcard), em um banco de dados, seja esse armazenamento individualizado ou não, ou remotamente em uma nuvem [24].

3) Fase de reconhecimento: envolve a utilização do modelo digital capturado e armazenado como vetor de comparação quando o usuário realizar uma autenticação para obter acesso a uma solução. Neste caso, é imprescindível que ocorra a correspondência entre os dados comparados, isto é, o dado obtido da captura na fase 1 e o dado obtido no momento fase 3.

Com a utilização de múltiplos fatores, presume-se que mesmo que um invasor comprometa um dos fatores, o nível de proteção é maior pois será necessário ao invasor comprometer os fatores restantes [25][26]. Tem-se como benefícios na adoção do MFA fornecer uma forma resiliente de autenticação de usuários e se figura como um mecanismo com grande custo-benefício [25]. Além da autenticação inicial, o segundo fator de autenticação é utilizado para proteger outras transações sensíveis, como por exemplo, transferências bancárias [26].

Capítulo 3

Design de Pesquisa e Métodos

Este Capítulo descreve a estratégia de pesquisa seguida para responder às questões de pesquisa levantadas. Em resumo, será aplicada uma pesquisa de métodos mistos, aliando uma revisão de literatura e um estudo de caso único e exploratório baseado na implementação da teoria encontrada na literatura. Em seguida, os procedimentos e fases deste trabalho são descritos. Tendo este capitulo como objetivo a apresentação das questões de pesquisa, do framework metodológico, o posicionamento filosófico, as fases da pesquisa e os procedimentos metodológicos.

A estrutura da metodológica da pesquisa é apresentada na figura 3.1.

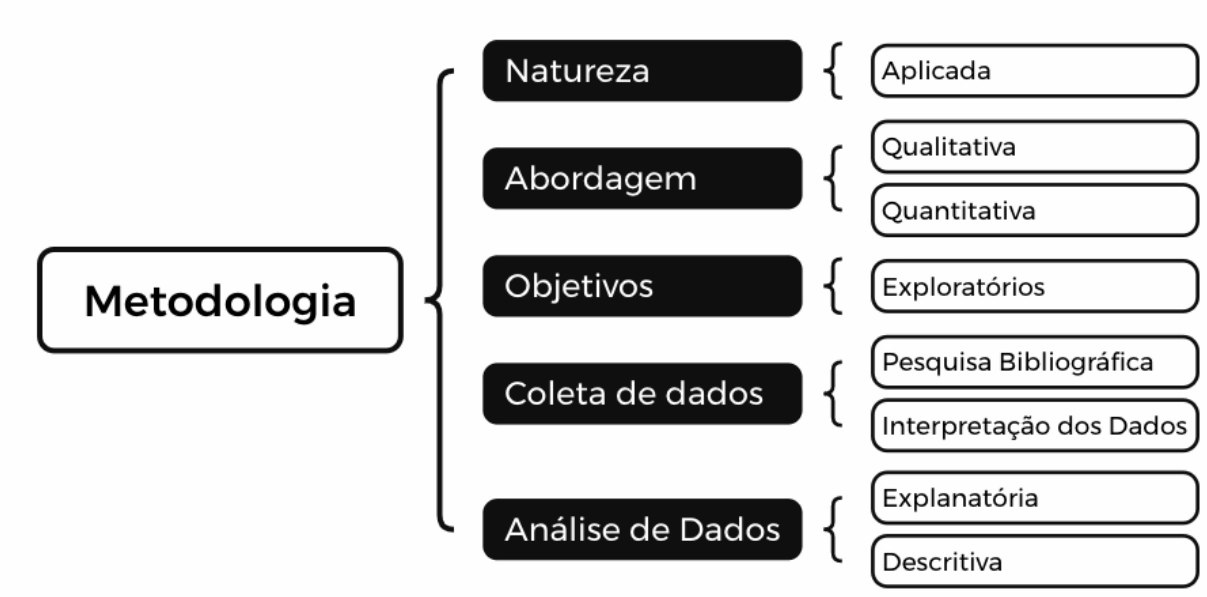

Figura 3.1: Metodologia de Pesquisa. Fonte: autor

Do ponto de vista da natureza, este trabalho adota uma **pesquisa de natureza aplicada**, uma vez que busca contribuir para um problema concreto relacionado à adição de um fator adicional de autenticação digital na plataforma gov.br. O estudo não se limita a uma investigação teórica, mas visa a aplicação do conhecimento para aprimorar a segurança do sistema, avaliando o impacto da implementação de um mecanismo de segurança e seus desdobramentos práticos. Dessa forma, a pesquisa possui um **caráter pragmático**, pois seus resultados podem subsidiar futuras melhorias no processo de autenticação da plataforma.

A **abordagem metodológica combina dados quantitativos e qualitativos**, permitindo uma análise mais abrangente do problema investigado. A dimensão **quantitativa** se dá pela coleta e análise de métricas referentes ao número total de acessos diários, à ativação de verificações adicionais e à frequência de eventos classificados como suspeitos pelo sistema. Esses dados possibilitam a identificação de padrões e tendências na autenticação dos usuários. Já a dimensão **qualitativa** complementa a análise ao examinar os desafios operacionais enfrentados na implementação do mecanismo, as dificuldades dos usuários na utilização do sistema. A combinação dessas abordagens proporciona um entendimento mais profundo do objeto de estudo, alinhando-se à complexidade da autenticação digital no contexto de uma plataforma governamental.

Os **objetivos da pesquisa são exploratórios**, pois buscam investigar um aspecto ainda em desenvolvimento na plataforma gov.br e levantar questões que possam fundamentar estudos futuros. De acordo com Yin [27], pesquisas exploratórias são indicadas quando há necessidade de aprofundar o conhecimento sobre um problema pouco estudado, permitindo a formulação de hipóteses e a identificação de variáveis relevantes para análises posteriores.

Para alcançar **seus objetivos, a pesquisa baseia-se na coleta de dados por meio de pesquisa bibliográfica e na análise de dados empíricos** provenientes da plataforma gov.br. A pesquisa bibliográfica permitiu o levantamento de estudos sobre duplo fatores de autenticaçao e modelos de autenticação multifatorial, aportando um embasamento teórico para a interpretação dos dados coletados. A partir dessas informações os **dados empíricos foram analisados com uma abordagem explanatória e descritiva**, alinhada à metodologia de estudo de caso de Yin. A **análise explanatóri**a buscou compreender como a implementação do mecanismo de segurança impactou o sistema e os usuários, enquanto a **análise descritiva** apresentou os dados coletados, destacando métricas relevantes e padrões observados ao longo do período avaliado.

Dessa forma, a metodologia empregada nesta dissertação combina diferentes técnicas e abordagens para garantir uma investigação detalhada do problema estudado. A integração de métodos quantitativos e qualitativos, aliada à análise exploratória, descritiva e

explanatória dos dados, permite não apenas compreender os impactos de um fator adicional de segurança, mas também fornecer subsídios para o aprimoramento das estratégias de autenticação digital em plataformas governamentais.

3.1 Questões de Pesquisa

Em atendimento ao objetivo geral determinado neste trabalho referentes a identificação de mecanismos de segurança relacionados a identidade digital, as seguintes questões de pesquisa foram definidas:

QP.1 Quais fatores de dupla autenticação identificados na literatura estão relacionados a uma Identidade Digital?

QP.2 Quais fatores de multi-autenticação identificados na literatura estão relacionados a uma Identidade Digital?

QP.3 Quais fatores adicionais se diferem dos já implementados e atendem aos critérios para o estudo de aplicabilidade a uma Identidade Digital?

QP.4 Quais os benefícios e/ou problemas identificados após a aplicação dos fatores adicionais a uma Identidade Digital?

3.2 Framework Metodológico

A presente pesquisa se caracteriza por uma abordagem aplicada, com foco na resolução de problemas concretos e na geração de soluções práticas. Ao contrário das pesquisas teóricas, que priorizam a expansão do conhecimento de forma abstrata, este estudo busca aplicar o conhecimento existente para solucionar desafios específicos de um contexto real. [28]. A pesquisa aplicada, portanto, se distingue por sua natureza pragmática, visando contribuir diretamente para a melhoria de processos, produtos ou serviços em diversos âmbitos da sociedade, frequentemente está associada a contextos organizacionais, educacionais, industriais ou sociais[29]. Do ponto de vista metodológico, este trabalho emprega uma estratégia exploratória sequencial, utilizando tanto instrumentos quantitativos quanto qualitativos para coleta de dados, com análise predominantemente qualitativa, pois foram feitas pesquisas de levantamento na literatura para avaliarem os métodos de identificação/autenticação adicional. Além disso, abordagens qualitativas também se aplicam, uma vez que serão feitas análises sobre dados empíricos com a aplicação do estudo de caso para avaliar a melhoria do processo de autenticação da plataforma ID gov.br. Como design de pesquisa, etapa em que a seleção do método de pesquisa do problema ocorre, a

abordagem de *estratégia exploratória sequencial* foi escolhida com início a coleta e análise de dados qualitativos advindos da execução da Revisão Sistemática de Literatura (RSL) e posterior análise qualitativa a partir da execução do estudo de caso. Como métodos de pesquisa, destaca-se que as perguntas para a condução deste trabalho são de natureza descritivas e classificativas, seguindo a classificação de Meltzoff [30]. A coleta de dados de natureza quantitativa e qualitativa foi feita a partir da RSL, será em seguida aplicado um estudo de caso como abordagem de pesquisa para a análise e interpretação dos dados será conduzida de forma qualitativa.

3.3 Fases da Pesquisa

Considerando o framework metodológico definido, esta Seção apresenta o design da pesquisa, bem como suas fases, procedimentos e objetivos. Segundo Creswell, as fases da execução da pesquisa podem ser alteradas, ou seja, o planejamento do estudo não pode ser encarado como algo fixo e imutável [31]. A estrutura da pesquisa com sua correlação entre objetivos, questões fases e procedimentos estão exemplificadas na Figura 3.2, e descritas abaixo:

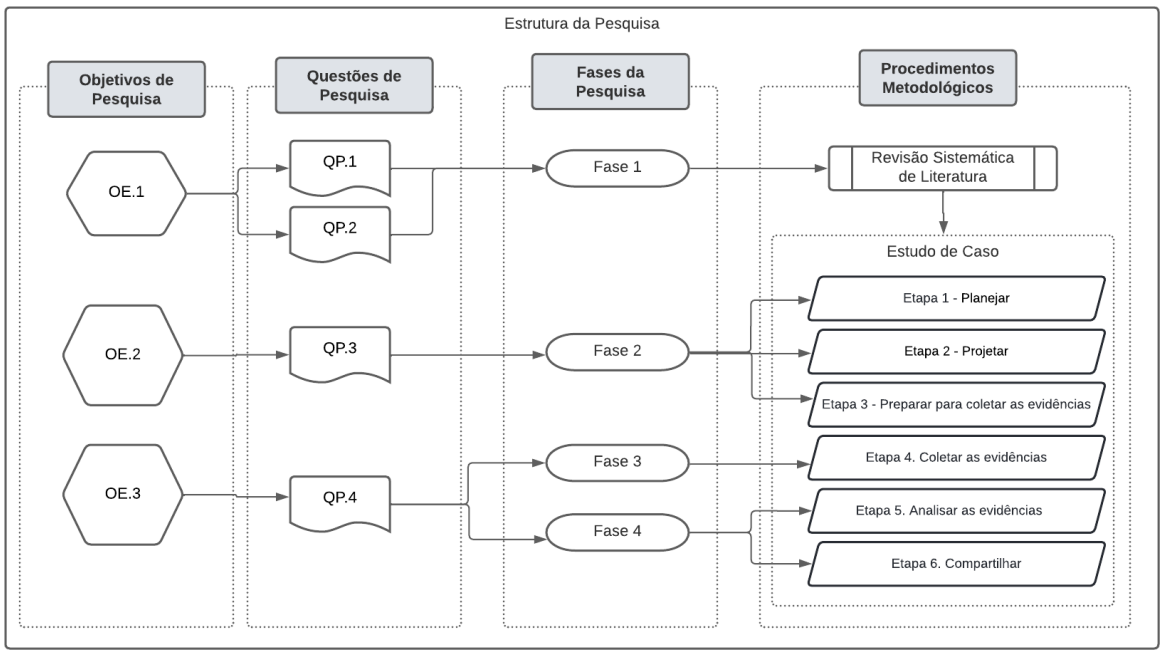

Figura 3.2: Metodologia de Pesquisa. Fonte: autor

Fase 1 - O objetivo principal dessa fase é realizar uma Revisão Sistemática de Literatura (RSL), por meio de palavras-chave em diferentes bases de dados, esse busca tem

o intuito de identificar fatores adicionais de segurança relevantes que possam contribuir e fortalecer a identificação e a autenticação na plataforma gov.br. Portanto, a análise foi focada em analisar se esses fatores adicionais que foram encontrados nos trabalhos candidatos possuem elementos passíveis de implementação no gov.br e coleta de resultados.

Fase 2 - Nesta fase se inicia a **aplicação do estudo de caso**, com a execução das 3 primeiras etapas. O **(1.) Planejar o estudo de caso** inclui a avaliação do cenário atual da plataforma gov.br para identificação dos critérios de fatores adicionais já existentes para compilar com os resultados da fase 1. Na etapa de **(2.) Projetar o estudo de caso** define-se critérios para seleção dos fatores adicionais identificados na Fase 1, identificando quais são os fatores de segurança já utilizados na plataforma e finaliza com a etapa **(3.) Preparar para coletar as evidências dos estudos de caso** que será realizada uma avaliação do gov.br acerca dos indicadores ou métricas relacionadas com a segurança atual. Essa observação contribui também para a fase 5 em que será possível realizar um comparativo do fatores adicionais implementados.

Fase 3 - Nesta fase, ocorre a implementação do fator adicional de autenticação na plataforma gov.br, dando início à **etapa (4.) coleta das evidências do estudo de caso**, conforme Yin[27]. A integração do fator adicional selecionado é realizada em alinhamento com a equipe responsável pela evolução da plataforma, garantindo sua inclusão no *roadmap* de desenvolvimento. Durante essa implementação, são monitoradas métricas para avaliação da implementação. A documentação dessas evidências é fundamental para permitir uma análise comparativa na fase seguinte e avaliar o impacto real da solução aplicada.

Fase 4 - A última fase tem como objetivo **analisar as evidências coletadas (etapa 5)** e **compartilhar os achados do estudo de caso (etapa 6),** conforme a metodologia de [27]. A análise é realizada por meio da comparação entre os dados antes e depois da implementação do fator adicional verificando impactos na segurança e na experiência do usuário. Além da interpretação dos resultados, esta fase contempla a comunicação dos achados por meio desta dissertação como método para registro dos achados, possibilitando que as descobertas possam contribuir para futuras pesquisas e aprimoramentos na autenticação digital. Os resultados obtidos servirão de insumos para subsidiar a conclusão do estudo e validar se o fator adicional proposto traz vantagens ou desvantagens relativas a seu uso no contexto da plataforma ID gov.br e no âmbito do Governo Federal.

3.4 Revisão Sistemática de Literatura

Uma Revisão Sistemática de Literatura (RSL) baseada no protocolo proposto por Kitchenham et al.[5] foi realizada com o intuito de identificar RNF de segurança em iden-

tidades digitais e mecanismos de mitigação. A RSL é um estudo que revisa todos os trabalhos primários relacionados a uma questão de pesquisa específica, contribuindo para integrar/sintetizar evidências sobre a questão de pesquisa, isto é, utiliza uma metodologia definida para identificar, analisar e interpretar todas as evidências disponíveis [32]. A ferramenta online Parsifal [33] foi utilizada para apoiar todo o processo de RSL.

Este Capítulo apresenta a metodologia de pesquisa cientifica utilizada para o desenvolvimento deste trabalho de dissertação.

Nesse trabalho foi empregada a técnica Revisão Sistemática de Literatura (RSL) baseada no protocolo proposto por Kitchenham et al. [34]. Esse protocolo é composto por três fases:

- **Planejamento** - objetivo de identificar a real necessidade da RSL e a motivação da pesquisa, nessa fase são executadas as atividades de definição de objetivo, preparação do protocolo para o RSL e a avaliação do protocolo de pesquisa, que neste trabalho foi testado quando aplicado a *string* nas bases de dados escolhidas.
- **Condução** - Estudos são identificados através da aplicação da *string* de busca e selecionados de acordo com o protocolo definido na fase de planejamento. Os dados são coletados e sintetizados para responder a questão de pesquisa e facilitar a análise e criação dos resultados.
- **Relatos** - A última fase da RSL é relacionado com a documentação e descrição dos resultados, preparação das respostas das questões de pesquisa e disseminação dos resultados para os interessados.

A seguir serão demonstrados os passos acima para execução da RSL.

3.4.1 Planejamento da Revisão

Uma Revisão Sistemática de Literatura (RSL) baseada no protocolo proposto por Kitchenham et al.[5] foi realizado com o intuito de identificar fatores adicionais de segurança em identidades digitais e mecanismos de mitigação. A RSL é um estudo que revisa todos os trabalhos primários relacionados a uma questão de pesquisa específica, contribuindo para integrar/sintetizar evidências sobre a questão de pesquisa, isto é, utiliza uma metodologia definida para identificar, analisar e interpretar todas as evidências disponíveis [32]. A ferramenta online Parsifal [33] foi utilizada para apoiar todo o processo de RSL.

3.4.2 Questões de Pesquisa

As questões de pesquisa foram previamente estabelecidas na Seção 3.1, dedicada à definição dos métodos.

3.4.3 Definição da String de Busca

A *string* de pesquisa de base foi criada usando o operador AND para relacionar às palavras-chave, com os respectivos sinônimos agrupados usando o operador OR. Esta string é apresentada a seguir:

```
("digital identity"
OR "digital authentication"
OR "digital identification")
AND ("two-factor authentication"
OR "second factor authentication"
OR "multi-factor authentication")
```

Para a construção da *string* de pesquisa, primariamente, foi feito uma busca manual pela base de dados Scopus com as palavras-chave *digital identity* e *two-factor authentication*, a partir dos resultados dos trabalhos retornados foram coletadas as palavras-chave desses, para serem utilizados como sinônimos, e compor a *string* de busca, conforme Tabela 3.1. Essa *string* foi executada, com o objetivo de refinamento da string, nas seguintes bases: Scopus e ACM Library. Após refinamento, a pesquisa foi executada nas bases Scopus e ACM Library, IEEE Xplore, ScienceDirect.

Tabela 3.1: Palavras-chave e Sinônimos

Palavras-chave	**Sinônimos**
Identity digital	digital authentication, digital identification
two-factor authentication	second factor authentication, multi-factor authentication

3.5 Condução

Essa etapa consiste na execução do protocolo proposto visando encontrar os estudos, selecionar os trabalhos, conforme os critérios de seleção e extrair os dados dos estudos primários para então gerar os resultados, insumo para que as questões de pesquisa serão respondidas.

3.5.1 Critérios de Inclusão

Para a RSL foram definidos os seguintes critérios de inclusão:

CI.1 O trabalho precisa conter as palavras: identidade digital, autenticação digital, segundo fator ou multi-fator autenticação;

CI.2 a partir de 2019;

CI.3 trabalhos escritos em língua inglesa.

3.5.2 Critérios de Exclusão

Como critério de exclusão dos estudos foram considerados:

CE.1 O trabalho não apresenta fatores adicionais de segurança a uma identidade digital;

CE.2 editoriais, revistas, resumos, tutoriais, relatórios *workshop*, opiniões, sumários de conferências, teses, dissertações, relatórios técnicos, livros, *shorts papers*;

CE.3 trabalhos com proposições de mecanismos de segurança físicos;

CE.4 trabalhos não acessíveis;

CE.5 duplicados entre as bases de pesquisas;

CE.6 trabalhos secundários e terciários.

3.5.3 Avaliação de Qualidade

A avaliação da qualidade de cada trabalho foi definida a partir da resposta dada pelas seguintes questões. Cada uma delas foi respondida com Sim (S, peso 1), Parcialmente (P, peso 0,5) ou Não (N, peso 0) seguindo os critérios definidos a seguir:

AQ.1 Resultados sobre a aplicabilidade do(s) fator(es) proposto(s) foi(ram) apresentado(s)?

AQ.2 Apresenta fator(es) adicional(ais) e/ou ferramenta(s) de segurança que pode(m) ser aplicada(s) a uma identidade digital?

AQ.3 Limitações do(s) trabalho(s) foi(ram) descrita(s)?

O *score* de qualidade de cada trabalho foi calculado pelo somatório das respostas de todas as questões.

3.5.4 Coleta de Dados

Os dados extraídos de cada estudo foram:

- Título;
- resumo;
- O(s) autor(es);
- fatores adicionais ou técnicas aplicadas para resolver o problema de requisitos de segurança.

3.5.5 Análise de Dados Coletados

Os trabalhos candidatos para condução dos próximos passos foram selecionados seguindo o score de qualidade encontrado para cada um deles. Os que não atingiram o *Score* conforme definido nos critérios de avaliação de qualidade foram considerados não aptos para essa RSL uma vez que poderiam apresentar pouca similaridade ao objeto desse estudo mitigando prejuízos aos resultados.

3.6 Estudo de Caso na Plataforma gov.br

O estudo de caso é um método composto geralmente por poucos ou apenas um objeto, que em sua aplicação fornecem conhecimentos profundos. Normalmente se utiliza esse método de pesquisa para dados qualitativos coletados a partir de eventos reais objetivando elucidar, pesquisar ou descrever características atuais inseridas em seu próprio contexto [35]. As abordagens quantitativas buscam a generalização dos resultados, conquanto, o estudo de caso busca uma entendimento aprofundado de uma ocorrência ou situação particular, uma companhia, um processo ou acontecimento singular [36].

O estudo de caso, pode ser aplicado em variadas situações, suas contribuições alcançam o conhecimento de fenômenos individuais, grupais, organizacionais, sociais, políticos e relacionados, por exemplo, quando o pesquisador não possui total gestão sobre os acontecimentos que estão sendo analisados, o estudo de caso se mostra como um relevante instrumento para entender importantes questões: como e o porquê [37]. Reforçando o entendimento, Merriam (2009) descreve o estudo de caso como uma pesquisa empírica que examina um fenômeno em seu ambiente natural, sendo particularmente útil quando as fronteiras entre o fenômeno e o contexto não estão claramente delineadas. Nesse sentido, o estudo de caso possibilita investigar sutilezas contextuais e captar pormenores que dificilmente seriam percebidos em estratégicas que empregam métodos quantitativos normatizados [38].

Além disso, o emprego do estudo de caso também se destaca em investigações que envolvem práticas profissionais e análises de implementação, em que os resultados podem servir como fundamento para práticas aplicadas e decisões [37]. Creswell (2007) reforça a capacidade do estudo de caso de propiciar novas percepções, sendo útil a sua utilização em contexto similares ou fornecendo base para estudos futuros [39]. Segundo Yin, a metodologia estudo de caso, permite que os pesquisadores observem características abrangentes e importantes dos eventos da vida real [40]. A versatilidade do estudo de caso permite que ele seja alinhado a diferentes objetivos e áreas do conhecimento. No entanto, isso exige que o pesquisador mantenha um rigor metodológico para garantir a validade e a confiabilidade dos resultados. Conforme descrito e sistematizado por Yin (2015), essa metodologia robusta possibilita uma análise aprofundada e contextualizada de fenômenos complexos [27].

A aplicação do estudo de caso será baseado no modelo proposto por Yin [41] composto por 6 etapas: 1. Planejar o estudo de caso; 2. Projetar o estudo de caso; 3. Preparar para coletar as evidências dos estudos de caso; 4. Coletar as evidências dos estudos de caso; 5. Analisar as evidências do estudo de caso; 6. Compartilhar os estudos de caso.

3.6.1 Justificativa da Escolha do Método

O método de estudo de caso foi escolhido para este trabalho devido à sua relevância e adequação em pesquisas que buscam compreender fenômenos complexos em contextos reais. De acordo com Yin [27], o estudo de caso é particularmente apropriado quando o pesquisador deseja explorar questões do tipo “como” e “por que” em situações em que não se pode separar o fenômeno de seu contexto.

No caso desta dissertação, o objetivo foi investigar o aprimoramento da segurança na plataforma gov.br, especialmente por meio da implementação e avaliação de um fator adicional de segurança. Essa situação envolve diversas variáveis, como usabilidade, experiência do usuário e segurança, tornando o método de estudo de caso a escolha mais apropriada para analisar a complexidade do tema.

3.6.2 Caracterização do Tipo de Estudo de Caso

Este trabalho é caracterizada como um estudo de caso único e exploratório, conforme os critérios de Yin[27]. O estudo de caso único se justifica por focar na plataforma gov.br, que representa uma solução única e crítica para os serviços públicos digitais no Brasil. A plataforma gov.br e sua relevância nacional tornam-na um objeto de estudo para analisar a implementação de um novo fator adicional de segurança, permitindo uma investigação aprofundada de suas características, desafios e implicações no contexto de segurança.

Além disso, o estudo é exploratório, pois busca compreender um fenômeno relativamente novo, o uso de um mecanismo adicional de segurança em plataformas de governo, e levantar hipóteses e discussões iniciais sobre suas limitações e benefícios. Diferentemente de estudos descritivos, a dissertação não se limita a explicar o funcionamento do sistema, mas explora questões técnicas e operacionais, como custos de infraestrutura e impactos na experiência do usuário. Essa abordagem reflete a necessidade de investigar o tema em um ambiente específico e gerar subsídios para pesquisas futuras na área de autenticação digital.

3.6.3 Unidade de Análise

A unidade de análise desta dissertação é o processo de autenticação na plataforma gov.br, com foco na implementação do mecanismo adicional no momento da autenticação.

O estudo investiga como esse mecanismo foi aplicado para aprimorar a segurança no acesso aos serviços públicos digitais, com base em padrões de risco, como mudanças de localização. Outrossim, avalia-se o impacto na experiência do usuário, avaliando possíveis dificuldades enfrentadas pelos cidadãos ao acessar suas contas e os desafios associados à adoção desse mecanismo.

3.7 Etapas do Estudo de Caso

Esta Seção apresenta as etapas do estudo de caso, segundo Yin [27], demonstrando a metodologia empregada em sua execução.

O detalhamento das etapas e seus protocolos é feito nas próximas seções apresentando as definições e o embasamento no método de Yin [27].

3.7.1 Etapa 1 - Planejamento do Estudo de Caso

A **Fase 2** desta dissertação marca o início da aplicação do **estudo de caso**, conforme a metodologia de Yin[27]. A **Etapa 1**, denominada **Planejar o estudo de caso**, é essencial para garantir que a investigação seja conduzida de forma estruturada, coerente e alinhada aos objetivos da pesquisa. O principal foco dessa etapa foi avaliar o cenário atual da plataforma gov.br para compreender como a RBA poderia ser integrada e quais fatores de segurança já estavam implementados no sistema.

A execução dessa etapa começou com a **identificação do cenário atual da plataforma de autenticação gov.br**, visando mapear os **fatores adicionais de segurança já existentes**. Para isso, foi realizada uma análise exploratória no processo de auten-

ticação da plataforma, a verificação do termo de uso e aviso de privacidade, buscando identificar as práticas adotadas para proteger o acesso dos usuários.

O objetivo era garantir que qualquer proposta de aprimoramento da segurança estivesse alinhada à arquitetura e requisitos já estabelecidos na plataforma.

Além disso, o planejamento do Estudo de Caso incluiu a **definição de critérios para a seleção dos fatores adicionais de autenticação** que seriam analisados nas próximas fases. Esses critérios foram estabelecidos com base nos achados da RSL realizada na Fase 1, permitindo uma correlação entre os fatores sugeridos pela literatura e aqueles já aplicáveis ao contexto do gov.br. Dessa forma, a etapa 1 serviu como base metodológica para garantir que a pesquisa seguisse um caminho lógico e fundamentado, preparando o estudo de caso para a fase de coleta de evidências e implementação do novo fator de autenticação.

3.7.1.1 Identificação de Fatores Adicionais no gov.br (Fase 2)

Durante a pesquisa desenvolvida no âmbito da dissertação, com o objetivo de identificar os fatores adicionais de segurança já implementados pela plataforma gov.br, constatou-se que **a única medida adicional vigente no processo de autenticação era o duplo fator de autenticação (2FA)**. Esse recurso, amplamente adotado em sistemas digitais, reforça a camada de proteção ao exigir dois elementos distintos de validação de identidade.

O duplo fator de autenticação é uma ferramenta essencial para adicionar uma camada de proteção relacionados ao acesso não autorizado e à proteção de informações sensíveis [19].

3.7.2 Etapa 2 - Projeção do Estudo de Caso

Na etapa de projeção do estudo de caso, são detalhados os procedimentos metodológicos que orientam a execução da pesquisa empírica. O estudo foi delineado como um estudo de caso único, conforme a classificação de Yin (2015), uma vez que a plataforma gov.br se apresenta com um representatividade singular e relevante para a autenticação digital em serviços públicos.

Sendo assim, o objetivo foi garantir que a coleta de dados de maneira estruturada, confiável e alinhada aos critérios definidos na **Etapa 1**. Segundo Yin [27], essa fase é essencial para a **integridade metodológica do estudo de caso**, pois envolve a definição de instrumentos, protocolos e indicadores que serão utilizados na análise das evidências.

Nesta dissertação, a preparação para a coleta de evidências consistiu, primeiramente, na **identificação dos dados e métricas que poderiam ser extraídos da plataforma gov.br** para avaliar a segurança da autenticação. Foram definidos indicadores-chave de

segurança, como **o percentual de logins que acionaram verificações adicionais**, **padrões de localização dos acessos**. Esses indicadores foram escolhidos com base nos fatores de autenticação analisados na RSL e na avaliação do cenário atual realizada na Etapa 1, vide Figura 4.4. Também é executada nesta etapa a **Comparação entre Fatores da RSL** e os Utilizados no gov.br, assim como a **Priorização dos Fatores Adicionais a Serem Avaliados.**

Além disso, a preparação para a coleta de dados envolveu a **seleção das fontes de evidência** que seriam utilizadas para validar a implementação do RBA. Isso **incluiu o levantamento de relatórios operacionais da plataforma gov.br**, **o acesso a logs de autenticação (respeitando as diretrizes da LGPD) e a análise de registros estatísticos sobre os acessos autenticados**, disponibilizados pela Diretoria Identidade digital, que serão apresentados na Seção 3.7.2.2. Para garantir a confiabilidade dos dados coletados, foram estabelecidos critérios de rastreabilidade e consistência das informações, buscando minimizar vieses na interpretação dos resultados.

Outro ponto fundamental da preparação foi a **definição do protocolo de coleta de evidências**, estabelecendo a forma como os dados seriam analisados e documentados. Esse protocolo foi essencial para garantir que as informações coletadas fossem organizadas de maneira sistemática, possibilitando comparações antes e depois da implementação do RBA, o que seria fundamental para as análises conduzidas nas fases seguintes da pesquisa.

3.7.2.1 Protocolo de Coleta de Evidências

Para garantir que a coleta de dados fosse realizada de maneira estruturada e confiável, foi estabelecido um protocolo de coleta de evidências baseado na metodologia de [27]. Esse protocolo definiu as etapas para obtenção, organização e análise dos dados coletados, conforme detalhado abaixo:

- **Fontes de evidência:** As informações foram obtidas a partir de relatórios operacionais da plataforma gov.br, logs de autenticação anonimizados e estatísticas fornecidas pelos responsáveis pela infraestrutura do sistema; [42, 43, 44]
- **Período de coleta:** A coleta de dados foi realizada em um intervalo de tempo predefinido, abrangendo períodos anteriores e posteriores à implementação do RBA para possibilitar comparações, segundo o período possibilitado pela Diretoria de identificação Digital;
- **Critérios de validação:** Para garantir a confiabilidade dos dados, foram utilizados critérios como a verificação de consistência entre diferentes fontes e a análise de padrões anômalos que pudessem indicar inconsistências ou erros nos registros;

- **Forma de registro:** Todos os dados coletados foram armazenados em planilhas estruturadas para posterior análise com intuito de identificar padrões e tendências;
- **Análise comparativa:** Os dados foram comparados antes e depois da implementação do RBA para avaliar seu impacto na segurança e na experiência do usuário. Além disso, foram analisadas possíveis variações de comportamento decorrentes de fatores externos, como mudanças sazonais no volume de acessos.

Com esse protocolo bem definido, a coleta de evidências foi realizada de forma organizada, permitindo que os resultados fossem interpretados de maneira fundamentada e alinhada com os objetivos da pesquisa.

3.7.2.2 Itens para a Coleta de Evidências

Análise estruturada e fundamentada da implementação do RBA na plataforma gov.br seguiu considerando os itens definidos para coleta na Seção 3.7.2. A Tabela 3.2 apresenta um resumo das métricas e informações selecionadas para a análise.

Tabela 3.2: Itens coletados para a avaliação do RBA

Item	Descrição	Objetivo da Coleta
Total de logins	Número total de acessos à plataforma gov.br em um período específico	Determinar a representatividade dos acessos analisados
Logins com verificação adicional	Total de logins que acionaram verificações extras baseadas em risco	Identificar a frequência de acionamento do RBA
Distribuição geográfica dos acessos	Localizações dos acessos autenticados	Avaliar padrões de comportamento do usuário e variações de localização
Recuperações de Conta no gov.br	Total de recuperações de conta por métodos de autenticação	Mensurar o impacto da segurança aprimorada na plataforma
Logins com vinculação	Total de acessos vinculados a uma identidade confirmada	Mensurar o impacto da segurança aprimorada na plataforma

Assim, a etapa 2 estruturou o estudo de caso para a coleta e interpretação dos dados, permitindo que a pesquisa avançasse para a implementação e avaliação do fator adicional de autenticação na plataforma gov.br.

3.7.3 Etapa 3 - Preparação para Coletar as Evidências do Estudo de Caso

Para garantir a efetividade da coleta de evidências, foram realizadas atividades preparatórias que incluíram a **definição de indicadores** de utilização do login, além de relatórios

operacionais e logs de autenticação. A equipe responsável pela gestão da ID gov.br foi envolvida no processo para viabilizar a coleta de dados e assegurar a **conformidade com as diretrizes de privacidade e segurança estabelecidas pela LGPD.**

A preparação também contemplou a definição de um **cronograma para a coleta das evidências** e validação dos instrumentos de análise.

A **Etapa 3** do estudo de caso consiste na **preparação para a coleta de evidências**, sendo um passo fundamental para garantir que os dados sejam obtidos de forma estruturada, confiável e alinhada aos objetivos da pesquisa. Segundo [27], essa etapa envolve a definição das fontes de evidência, dos critérios de validação dos dados e dos instrumentos que serão utilizados para garantir a rastreabilidade e a integridade das informações coletadas.

3.7.3.1 Definição das Fontes de Evidência

Nesta dissertação, foram estabelecidas diferentes fontes de evidência para embasar a análise da implantação do RBA na plataforma gov.br. A Tabela 3.3 apresenta um resumo das fontes utilizadas.

Tabela 3.3: Fontes de Evidência para a Coleta de Dados

Fonte de Evidência	Descrição	Objetivo
Relatórios Operacionais	Documentação técnica da plataforma gov.br, contendo estatísticas sobre logins e uso de fatores de autenticação adicionais.	Verificar os padrões de autenticação antes e após a implementação do RBA.
Logs de Autenticação	Registros anonimizados dos acessos dos usuários à plataforma gov.br, contendo informações sobre localização, dispositivo e acionamento de verificações adicionais.	Identificar padrões de risco e avaliar a frequência com que o RBA foi ativado.
Indicadores de utilização	Métricas estabelecidas para mensurar o impacto do RBA, incluindo percentual de logins e padrões geográficos dos acessos.	Avaliar o impacto da implementação do RBA na segurança da plataforma.

3.7.3.2 Critérios de Validação dos Dados

Para possibilitar que os dados coletados sejam confiáveis e representativos, foram definidos critérios de validação, conforme apresentado a seguir:

- **Consistência entre Fontes:** Os dados provenientes de diferentes fontes (relatórios operacionais, logs de autenticação e indicadores de segurança) foram comparados para garantir coerência e evitar distorções nos resultados;

- **Período de Coleta:** A análise considerou um intervalo de tempo suficientemente amplo para permitir a observação de padrões antes e depois da implementação do RBA, minimizando efeitos sazonais, segundo o período possibilitado pela Diretoria de identificação Digital;
- **Anonimização e Conformidade:** Os dados de autenticação foram tratados de forma a garantir o respeito às diretrizes da (LGPD), utilizando apenas métricas quantitativas sem quaisquer traços de identificação do usuário evitando qualquer exposição de informações sensíveis.

3.7.3.3 Protocolo para Coleta de Evidências

A coleta de evidências foi planejada de acordo com um protocolo estruturado, garantindo que os dados fossem coletados e analisados de maneira sistemática. O protocolo estabelecido seguiu as seguintes diretrizes:

- **Identificação dos Dados a Serem Coletados:** Foram definidos os indicadores-chave, incluindo total de logins, logins com verificação adicional, tempo de autenticação e distribuição geográfica dos acessos.
- **Processamento dos Dados:** Os dados coletados foram organizados em bases estruturadas e analisados estatisticamente para identificação de padrões e anomalias.
- **Análise Comparativa:** Os dados foram avaliados antes e depois da implementação do RBA para verificar se houve impactos positivos ou desafios na autenticação dos usuários.
- **Registro e Documentação:** Todas as análises foram documentadas de forma sistemática para garantir a rastreabilidade dos resultados e permitir a reprodução da pesquisa em estudos futuros.

Com a definição clara das fontes de evidência, critérios de validação e um protocolo estruturado para a coleta de dados, a pesquisa garantiu a confiabilidade das informações utilizadas na análise da implementação do *Risk-Based Authentication* na plataforma gov.br.

3.7.4 Etapa 4 - Coleta de Evidências do Estudo de Caso

A **Etapa 4 do estudo de caso corresponde à coleta das evidências do estudo de caso**, utilizando os procedimentos definidos na etapa anterior. Segundo Yin [27], essa fase tem como objetivo garantir que as informações sejam obtidas de forma rigorosa, documentada e representativa, permitindo que os achados do estudo sejam confiáveis.

3.7.4.1 Procedimentos de Coleta de Evidências

A coleta de evidências foi realizada com base nas fontes definidas na Etapa 3, utilizando métodos padronizados descritos na Seção 3.7.3.3 para garantir a rastreabilidade dos dados. A Tabela 3.4 apresenta um resumo dos principais procedimentos adotados.

Tabela 3.4: Procedimentos para Coleta de Evidências

Fonte de Evidência	Procedimento	Objetivo
Registros de autenticação	Extração de logs anonimizados da plataforma gov.br	Verificar padrões de acesso, acionamento do RBA e frequência de bloqueios.
Relatórios operacionais	Armazenamento e organização dos dados coletados	Comparar o desempenho antes e depois da implementação do RBA.
Indicadores de segurança	Monitoramento das verificações adicionais	Avaliar o impacto do RBA na proteção contra acessos não autorizados.

3.7.4.2 Definição da Coleta

Para garantir que os dados coletados fossem representativos e confiáveis, a execução da coleta seguiu as seguintes diretrizes:

- **Período de Coleta:** A coleta foi realizada em intervalos pré-definidos, abrangendo períodos antes e depois da implementação do RBA;
- **Anonimização e Conformidade:** Os dados de autenticação foram tratados de forma a garantir o respeito às diretrizes da (LGPD), utilizando apenas métricas quantitativas sem quaisquer traços de identificação do usuário evitando qualquer exposição de informações sensíveis, garantindo a privacidade dos usuários;
- **Validação dos Dados:** Foram realizados testes de consistência e cruzamento de informações entre diferentes fontes de evidência para garantir a integridade dos dados;
- **Armazenamento e Documentação:** Os dados coletados foram organizados de forma estruturada, permitindo análises futuras e garantindo a rastreabilidade da pesquisa.

Essa etapa foi essencial para consolidar a pesquisa empírica, garantindo que a análise dos impactos do RBA fosse realizada com base em dados concretos e confiáveis.

3.7.4.3 Execução da Coleta

Em seguida foram coletados os números para composição dos dados-base para avaliação da implantação do RBA da solução na plataforma gov.br. A **métrica de recuperação**

de senha foi a selecionada por ser uma funcionalidade comumente utilizada nas tentativas de sequestro de contas no gov.br.

A plataforma em sua recuperação de conta, guia o usuário por meio de sua experiência de tela para realizar a recuperação pelo método mais forte, isto é, manter o nível da sua conta ouro ou prata.

A análise dos dados referentes ao período de 06/07/2024 a 18/08/2024 revelou importantes informações sobre as recuperações de contas antes da implementação do mecanismo de RBA.

Durante o período analisado, o total de contas recuperadas foi de 9.426.544, com destaque para os métodos de recuperação via *e-mail* e SMS, que representaram, respectivamente, 37,56% e 9,66% do total. Esses números demonstram que esses meios são os mais utilizados especialmente entre os usuários que buscam um processo rápido.

Contudo, revelam uma possível fragilidade de agentes mal-intencionados por esses mesmos métodos, devido à possibilidade de exploração de vulnerabilidades por meio de técnicas de *phishing* e engenharia social.

Os métodos baseados em biometria também desempenharam um papel significativo na recuperação de contas. A biometria da ICN registrou 25.12% ou 2.367.645 recuperações, evidenciando sua relevância como uma solução segura e eficaz para verificação de identidade. Da mesma forma, a biometria da CNH contribuiu com 3.11% ou 293.618 recuperações, demonstrando seu potencial como um recurso complementar, ainda que menos abrangente. A robustez desses métodos torna-os menos atrativos para fraudadores, que encontram maiores barreiras para manipulações ou falsificações nesses métodos.

A tabela a seguir demonstram como está a distribuição de recuperação durante o período que será utilizado como fator de comparação pré implantação do mecanismo RBA na plataforma gov.br.

Tabela 3.5: Pré-RBA: Métodos utilizados para recuperação de senha na plataforma Gov.br

Método	**Quantidade**	**Percentual (%)**
Bancos	2.382.391	25,27%
Biometria ICN	2.367.645	25,11%
Biometria CNH	293.618	3,11%
SMS	910.943	9,66%
e-mail	3.543.925	37,56%
Total Geral	9.426.544	100,00%

Capítulo 4

Apresentação e Análise dos Resultados

4.1 Resultados da RSL (Fase 1)

O protocolo de condução da RSL resultou em 09 (nove) trabalhos. A aplicação da *string* de pesquisa e dos critérios de seleção são ilustradas na Figura 4.1.

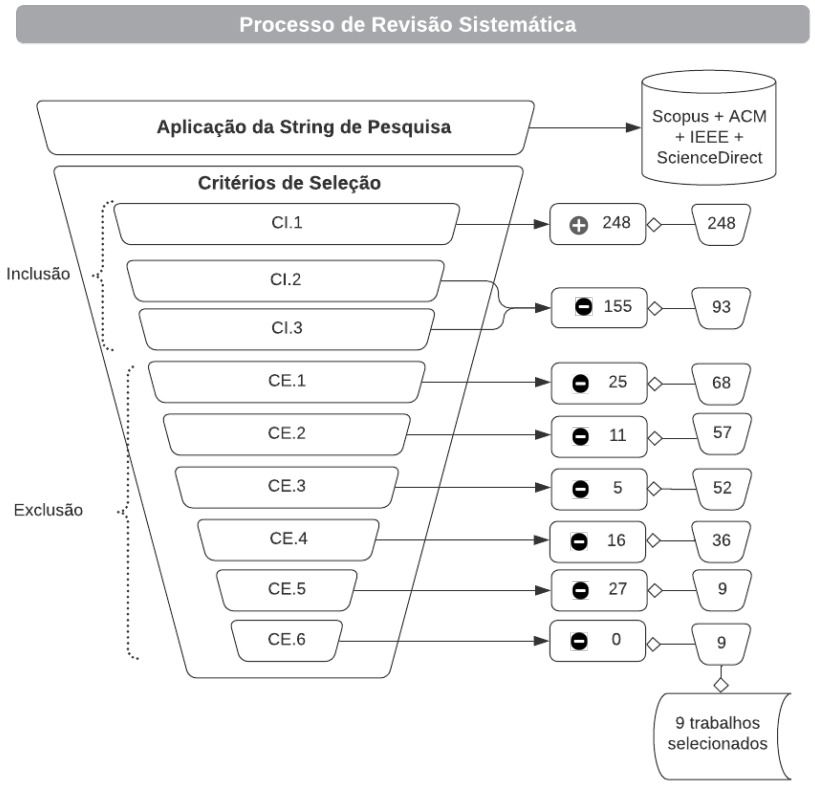

Figura 4.1: Processo RSL. Fonte: autor

A execução da *string* de busca na base de dados Scopus retornou 160 trabalhos enquanto na base de dados ACM Library 23 foram encontrados, IEEE Xplore a quantidade foi de 57 e por fim, na ScienceDirect apenas 8, totalizando 248 trabalhos.

Considerando a baixa quantidade de trabalhos identificados foi necessária a reavaliação da aplicação da *string* para garantir a mitigação de problemas relacionados a identificação de trabalhos primários. Foram consideradas as particularidades e a forma de pesquisa de cada base de dados, a *string* foi adaptada e validada de modo a garantir a correta aplicabilidade da *string* original em todas as bases de buscas, foi montada a tabela 4.1 para demonstração:

Tabela 4.1: Strings Adaptadas

Bases	**Strings**
Scopus	(((TITLE-ABS-KEY ("digital identity") OR TITLE-ABS-KEY ("digital authentication") OR TITLE-ABS-KEY ("digital identification")) OR (TITLE-ABS-KEY ("two-factor authentication") OR TITLE-ABS-KEY ("second factor authentication") OR TITLE-ABS-KEY ("multi-factor authentication")))
ACM	(Title: "digital identity") OR (Title: "digital authentication") OR (Title: "digital identification") OR (Abstract: "digital identity") OR (Abstract: "digital authentication") OR (Abstract: "digital identification") OR (Keyword: "digital identity") OR (Keyword: "digital authentication") OR (Keyword: "digital identification")) AND ((Title: "two-factor authentication") OR (Title: "second factor authentication") OR (Title: "multi-factor authentication") OR (Title: "Risk-based authentication") OR (Abstract: "two-factor authentication") OR (Abstract: "second factor authentication") OR (Abstract: "multi-factor authentication") OR (Abstract: "Risk-based authentication") OR (Keyword: "two-factor authentication") OR (Keyword: "second factor authentication") OR (Keyword: "multi-factor authentication") OR (Keyword: "Risk-based authentication"))
IEEE	(("Publication Title": "digital identity") OR ("Publication Title": "digital authentication") OR ("Publication Title": "digital identification") OR ("Abstract": "digital identity") OR ("Abstract": "digital authentication") OR ("Abstract": "digital identification") OR ("Author Keywords": "digital identity") OR ("Author Keywords": "digital authentication") OR ("Author Keywords": "digital identification")) AND (("Publication Title": "two-factor authentication") OR ("Publication Title": "second factor authentication") OR ("Publication Title": "multi-factor authentication") OR ("Abstract": "two-factor authentication") OR ("Abstract": "second factor authentication") OR ("Abstract": "multi-factor authentication") OR ("Author Keywords": "two-factor authentication") OR ("Author Keywords": "second factor authentication") OR ("Author Keywords": "multi-factor authentication"))
ScienceDirect	("digital identity"OR "digital authentication"OR "digital identification") AND ("two-factor authentication"OR "second factor authentication"OR "multi-factor authentication")

A execução da *string* na base de dados Scopus atende diretamente o critério de inclusão CI.1, logo, foram encontrados 160 trabalhos que com a aplicação dos critérios de inclusão CI.2 foram reduzidos para 63 trabalhos, aplicando o CI.3 o total de 63 foi mantido.

Na base de dados ACM, o total encontrado após o CI.1 foi de 23 trabalhos, aplicando os critérios de inclusão CI.2 restaram 11 trabalhos e aplicando o CI.3 o total de 11 foi mantido. Enquanto que na IEEE Xplore após a aplicação do CI.1 57 trabalhos foram encontrados, aplicando os critérios de inclusão CI.2 restaram 18 trabalhos e aplicando o CI.3 o total de 18 foi mantido.

Por fim, na base de dados ScienceDirect o total encontrado após o CI.1 foi de 08 trabalhos, aplicando os critérios de inclusão CI.2, restou 01 trabalho. Tem-se portanto um total de 93 trabalhos, considerando o somatório das bases que foram submetidos aos critérios de inclusão.

Com a aplicação do critério de exclusão para se considerar apenas os trabalhos que atendam ao critério CE.1, foram excluídos 25 trabalhos. Seguindo com a aplicação dos critérios de exclusão, foi aplicado o critério CE.2, foram excluídos 11 trabalhos, com a aplicação do critério de exclusão CE.3, foram excluídos 05 trabalhos, aplicando-se o critério de exclusão CE.4, foram excluídos 16 trabalhos, por fim, foram excluídos 27 trabalhos com o critério CE.5. Não houve trabalhos identificados como secundários ou terciários, conforme o critério CE.6.

Dessa forma, restaram 09 trabalhos para análise e submissão ao processo de Avaliação de Qualidade. Os trabalhos são apresentados na Tabela 4.2 para melhor visualização dos achados e de suas informações.

Tabela 4.2: Fontes Primárias de Estudo

ID	**Título**	**Autoria**	**Ref**
S1	SecuriCast: Zero-touch two-factor authentication using WebBluetooth	Dressel, T. and List, E. and Echtler, F.	[15]
S2	Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication	Seta, H. and Wati, T. and Kusuma, I.C.	[45]
S3	A Proposed Unified Digital Id Framework for Access to Electronic Government Services	Geteloma, V. and Ayo, C.K. and Goddy-Wurlu, R.N.	[17]
S4	A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing	Kumar, S. and Jafri, S.A.A. and Nigam, N. and Gupta, N. and Gupta, G. and Singh, S.K.	[46]
Continua na próxima página			

Tabela 4.2 – Continuação da página anterior

ID	Título	Autoria	Ref
S5	Click This, Not That: Extending Web Authentication with Deception	Barron, T. and So, J. and Nikiforakis, N.	[47]
S6	Securing remote access to information systems of critical infrastructure using two-factor authentication	Bruzgiene, R. and Jurgilas, K.	[48]
S7	TrustedID: An Identity Management System based on OpenID Connect Protocol	KOSE, Busra OZDENIZCI and BUK, Onur and MANTAR, Haci Ali and COSKUN, Vedat	[25]
S8	More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication	Wiefling, Stephan and Dürmuth, Markus and Lo Iacono, Luigi	[49]
S9	2D-2FA: A New Dimension in Two-Factor Authentication	Shirvanian, Maliheh and Agrawal, Shashank	[19]

4.1.1 Avaliação de Qualidade de RSLs

Segundo a avaliação de qualidade definida, os trabalhos selecionados foram devidamente analisados e pontuados, conforme apresentado na Tabela (4.3). Como parte do processo de avaliação de qualidade, foi estabelecida a métrica de taxa média demonstrado na fórmula apresentada (4.1) para que fossem calculadas as linhas de base para adequação às avaliações de qualidade (QA). Dessa maneira, a linha de base utilizada para o corte é o valor superior ao obtido na aplicação da fórmula em que é divido o valor total das notas pela quantidade de trabalhos avaliados.

$$s = \frac{(\sum \beta)}{\omega}, \tag{4.1}$$

Onde: s = média entre os trabalhos, β = notas atribuídas aos trabalhos na QA, ω = quantidade total de trabalhos avaliados.

Dessa forma, tendo o $\sum \beta$ = a 17 e a $\omega = 9$, tem-se $s = 1.88$ como linha de base para o corte desta avaliação de qualidade, sendo assim 4 trabalhos foram excluídos por possuírem nota inferior a s, restando 05 para a análise pelo autor.

Tabela 4.3: Avaliação de Qualidade

ID	AQ1	AQ2	AQ3	Score
S8	S	S	S	3.0
S5	S	S	S	3.0
S9	S	P	S	2.5
S1	P	S	S	2.5
S2	S	S	N	2.0
S6	S	P	N	1.5
S4	P	P	N	1.0
S3	N	S	P	1.0
S7	N	P	N	0.5

No contexto dos 05 (cinco) trabalhos primários analisados foram identificados 06 (seis) fatores adicionais de autenticação de segurança, conforme demonstrado na Tabela 4.4. O OTP, *one-time password*, é o fator adicional que mais se repete entre os trabalhos primários, aparecendo em três trabalhos, em dois deles combinado com outros mecanismos.

Tabela 4.4: Artigos e Fatores Adicionais

ID	**RBA**	**Tripwire**	***Login rituals***	**OTP**	**Bluetooth**	**SHA 1**
S8	x					
S5		x	x			
S9				x		
S1				x	x	
S2				x		x

Tendo findado o protocolo de execução da RSL e seus resultados, as questões de pesquisa QP.1 e QP.2 já podem ser respondidas. A seguir são apresentadas as respostas para

essas questões.

QP1. Quais fatores de dupla autenticação identificados na literatura estão relacionados a uma Identidade Digital?

O trabalho **S8** [49] aborda a autenticação Baseada em Riscos, em inglês *Risk Based Authentication* (RBA). Caso seja identificado comportamento significativamente diferente do rotineiro do usuário, são solicitados fatores adicionais de autenticação. Os autores destacam que o RBA tem o potencial de oferecer autenticação mais usual, porém as percepções de segurança do RBA e a usabilidade não são bem estudadas pela literatura. A proposta do trabalho é um estudo entre grupos em ambiente controlado com 65 participantes para avaliação de dois tipos diferentes de decisão RBA (quando ocorre uma mudança de dispositivo ou quando ocorre uma mudança de localização os dois tipos utilizam a re-autenticação via e-mail para confirmação), um tipo de 2FA (via e-mail) e autenticação somente por senha. Os quatro métodos escolhidos se basearam nas próprias observações dos autores sobre as implantações de última geração sobre RBA e outros métodos de autenticação populares. Os resultados apresentados pelo trabalho indicaram que o RBA é considerado mais utilizável do que os tipos de 2FA estudados. Também é percebido como mais seguro do que a autenticação somente por senha além de ser considerado comparativamente seguro em relação aos 2FA dos tipos de aplicativos avaliados.

O trabalho **S9** [19], propõe um mecanismo de dupla autenticação denominado pelos autores de 2D-FDA (*Two Dimensions - Secound Factor authentication*). De acordo com os autores, o 2D-2FA pois três principais características: Primeiro, após o o preenchimento do nome de usuário e senha em um terminal de login, um identificador exclusivo é exibido para ele. O usuário insere este identificador em seu dispositivo 2FA previamente registrado de acordo com os critérios de identificação. Depois, um PIN de uso único é calculado no dispositivo e transferido automaticamente para o servidor, o que é indicado pelos autores como um diferencial na proposta do 2D-FDA, sendo as duas dimensões que propõe o nome do mecanismo, pois o PIN pode ter um alto nível de uma entropia, inviabilizando ataques de adivinhação. Por último, o identificador também é incorporado ao cálculo do PIN, o que torna os ataques simultâneos ineficazes. Destaca-se que estudos de usabilidade e segurança foram executados para avaliar a aplicabilidade do 2D-2FA que demonstra que o sistema proposto oferece uma taxa de erro quase 50% menor e 2/3 melhor eficiência com a performance de 2 a 3 vezes mais rápida em comparação com o PIN-2FA comumente usado.

QP.2 Quais fatores de multi-autenticação identificados na literatura estão relacionados a uma Identidade Digital?

O trabalho **S5** [47] apresenta dois mecanismos relacionados a uma parametrização realizada pelo usuário, sendo eles: *tripwire* e *rituals logins*. No mecanismo *tripwire* é possível que o usuário personalize sua página web ou aplicativo criando uma armadilha que poderá ser evitada pelo legítimo proprietário, logo, se um *tripwire* é detectado, assume-me tratar de uma intrusão e ações de segurança são acionadas. Cabe destacar que essas armadilhas poderão ser acionadas pelo legítimo proprietário, ocasionalmente, em caso de esquecimento. No mecanismo *Ritual Logins* o usuário realiza uma configuração de acesso, isto é, ele determina uma sequência de cliques/acessos (um ritual) que serão feitos imediatamente após a autenticação na plataforma. Caso a pessoa que acesso não execute exatamente a sequência, contramedidas são adotadas e o usuário é automaticamente deslogado da plataforma. A combinação desses mecanismos gera a aplicação múltipla de fatores proposta pelos autores que foi avaliada a partir de um estudo de usuários que avaliou a taxa de detecção de *tripwires* contra invasores simulados, 88% dos quais clicaram em pelo menos um *tripwire*. A criação de rituais de login personalizados pelos usuários da web foi avaliada na perspectiva de praticidade e de memorização desses rituais ao longo do tempo. Dos rituais criados por usuários, todos foram únicos e 79% dos usuários conseguiram reproduzir seus rituais. Os autores destacam que o trabalho não pretende substituir as práticas de autenticação padrão, mas que seus resultados mostraram que os mecanismos baseados em engano podem fornecer camadas efetivas de segurança adicional.

O trabalho **S1** [15] criou um fator adicional chamado: *SecuriCast*, esse fator utiliza o OTP associado ao *bluetooth* do *smartphone* do usuário, por meio de uma conexão estabelecida entre navegador e dispositivo móvel. O processo do SecuriCast consiste em três componentes principais: o serviço provedor que deseja autenticar o usuário, um navegador com Suporte *WebBluetooth* para o processo de login, e o *smartphone* do usuário com o aplicativo *SecuriCast* que fornecerá o segundo fator. O *SecuriCast* apresenta duas formas: *zero-touch e notify*, na primeira o usuário recebe quatro palavras-chave para verificar e confirmar a tentativa de autenticação. Enquanto na segunda o usuário recebe um código de seis dígitos para ser inserido manualmente. Os autores realizaram um estudo de caso em laboratório com participação de um grupo de 30 pessoas voluntárias entre funcionários e alunos da universidade, a análise demonstrou que que o *SecuriCast* (*zero-touch*) oferece um desempenho um pouco melhor que o *GoogleAuthenticator*, porém o desempenho não alcançou um nível estatisticamente significativo. Os autores registram que essa pequena diferença pode estar provavelmente relacionada à interação adicional atualmente necessária para configurar a conexão *Bluetooth* e que essa necessidade pode desaparecer em versões futuras do *WebBluetooth*. o SecuriCast (*notify*) leva mais tempo do que os outros modos, entretanto os autores destacam que essa diferença provavelmente está

relacionada ao processo relativamente desconhecido de comparação de quatro palavras-chave e diminuiria com a prática.

O trabalho **S2** [45] propõe uma solução de utilização do método de autenticação TOTP e o algoritmo de *hash* de algoritmo seguro 1 (SHA1). O método permite que sistemas não dependam apenas do nome de usuário e senha para entrar na conta do usuário, mas que além disso o usuário deve receber um *token* ou código que é usado para fazer login na conta do usuário. Os autores destacam a fragilidade de utilizar o OTP junto ao SHA1 para gerar um código que não pode ser o mesmo pois este código só pode ser usado uma vez com um limite de tempo certo. A utilização do SHA1 com strings diferentes de entrada longa produziu uma saída com uma *string* de comprimento fixo de 160 bits. Os resultados dos testes demonstraram que 30 segundos é suficiente para evitar que os hackers façam login e assumam a conta sem permissão e também provam que esta autenticação pode aumentar bem a segurança do processo de autenticação. Com base nos resultados dos testes de segurança executados pelos autores, o processo de autenticação usando TOTP e SHA 1 ainda precisa de algumas melhorias.

4.2 Resultados da Fase 2

A Fase 2 tem como objetivo identificar quais são os fatores de segurança já são utilizados na plataforma ID gov.br e responder a pergunta QP.3.

QP.3 Quais fatores adicionais se diferem dos já implementados e atendem aos critérios para o estudo de aplicabilidade a uma Identidade Digital?

Em levantamento realizado junto a plataforma ID gov.br foram identificados dois fatores adicionais de segurança em utilização, esses fatores são utilizados seja no processo de criação ou recuperação da Identidade Digital (ID) gov.br. Os fatores adicionais identificados são o One-Time Password (OTP) e a Biometria Facial.

A biometria facial é utilizada no aplicativo gov.br pelo processo de *onboarding*, nesse momento é realizado uma comparação entre a foto coletada pelo aplicativo com a base de dados da Identidade Civil Nacional (ICN), quando o usuário possuir cadastro no ICN, o que lhe atribui a ID ouro ou na base de dados do Registro Nacional de Carteira de Habilitação (Renach) o que lhe atribui a categoria ID Prata, respectivamente.

Após a criação da ID é possível habilitar o segundo fator de autenticação (2FA) para o usuário. Esse procedimento pode ser feito na plataforma online ID gov.br. Uma vez habilitado o segundo fator, qualquer tentativa de login, seja na web ou via aplicativo, será

necessário informar o código gerado via OTP. O Código é informado pelo cidadão e a ID gov.br efetua a validação permitindo ou não a conclusão do processo de login.

Considerando a levantamento realizado e os achados de fatores adicionais decorrentes dos trabalhos primários, foi realizado um quadro comparativo para validar os fatores adicionais existentes e os atualmente implementados na plataforma ID gov.br em contrapartida com os que foram identificados na literatura como potenciais candidatos, conforme apresentado na tabela 4.5.

Tabela 4.5: Comparação entre os Fatores Adicionais gov.br x Achados da RSL

Fatores adicionais da ID gov.br	**RBA**	**Tripwire**	***Login rituals***	**OTP**	***Bluetooth***	**SHA 1**
OTP				x		
Biometria Facial						

Dos fatores identificados na literatura a ID gov.br atualmente já implementa o fator de autenticação adicional por meio de OTP conforme descrito acima. Os fatores RBA, *Tripwire*, *Login Rituals* OTP+*Bluetooth* e OTP+SHA1 são os fatores que foram identificados como os que se diferem dos atualmente implantados na plataforma ID gov.br.

4.2.1 Definição de Critérios para Seleção dos Fatores Adicionais

Os fatores selecionados em resposta à QP.3 foram analisados e discorridos a seguir, além disso uma análise foi realizada para avaliar se os fatores adicionais apresentados nos trabalhos primários selecionados são factíveis de serem utilizados no sistema de identificação digital do Governo Federal.

Nesse contexto, tornou-se necessário definir um método que equilibrasse três aspectos fundamentais: segurança, experiência do usuário e viabilidade técnica de implementação. Esses aspectos foram definidos, juntamente com a tipificação da classificação, pelos gestores da Diretoria de Identidade Digital.

Para avaliar cada fator de autenticação, foi utilizado um modelo de categorização com três níveis:

- **Alta**: O fator apresenta desempenho consistente e vantagem significativa sobre métodos convencionais.

- **Média**: O fator oferece melhorias, mas tem desafios que impactam sua adoção.
- **Baixa**: O fator apresenta limitações que comprometem sua eficácia ou usabilidade.

Essa categorização foi baseada na literatura acadêmica sobre autenticação e em análises empíricas de implementação em plataformas digitais, considerando as três dimensões:

- **Segurança**: Avaliação da resistência do fator contra ataques de força bruta, phishing e comprometimento de credenciais.
- **Experiência do Usuário**: Impacto do fator na usabilidade e conveniência para diferentes perfis de usuários.
- **Viabilidade Técnica**: Possibilidade de implementação na infraestrutura existente, considerando desafios de conformidade regulatória, custo e compatibilidade.

O *tripwire* e *rituals logins* trazem uma abordagem atrativa para a solução, considera-se um fator adicional voltado para a responder a pergunta: O que o usuário sabe? Uma vez que tanto a armadilha quanto o sequenciamento inicial de acesso foram definidos por ele. Sendo assim, ainda que o atacante consiga as credenciais de login e senha seria necessário superar esses fatores adicionais. Partindo do pressuposto que o atacante não faz ideia da existência desses fatores adicionais e que eles poderiam, inclusive, ser reconfigurados de acordo com um periodicidade definida, torna-se ainda mais complexo superar esses obstáculos. No entanto, o *Tripwire* apesar de proteger contra ataques de credenciais comprometidas, é vulnerável a engenharia social [50], tornando o pilar de segurança médio, conforme demonstrado na tabela 4.6. Já o *Login Rituals* é sucetível à observação de terceiros que podem ser fraudadores, também tornando sua classificação média. Por requerer configurações prévias e memorização do ritual de login, respectivamente, esses dois métodos tem baixa classificação na experiência do usuário, conforme demonstrado na tabela 4.7 e, por fim, na viabilidade técnica, os dois mecanismos são classificados como inviáveis, vide tabela 4.8, tendo em vista que o tripwire pois alta complexidade de implementação e é pouco compatível com sistemas de larga escala [51] como o gov.br. O *Login Rituals*, por sua vez, requer grande capacidade de armazenamento e processamento também inviabilizando sua adoção no contexto govr.br.

Em relação ao fator adicional de segurança OTP, a combinação deste fator com o SHA1 não trouxe resultados significativos no estudo de [45], assim como outros estudos não apresentaram melhoria siginificativa com sua implementação [52], o que inviabiliza sua consideração nos processos de melhoria da plataforma ID gov.br e o classifica no fator de segurança como baixo, evidenciado na tabela 4.6. Sob a perspectiva de experiência do usuário, o método se mostrou de categorização média, conforme tabela 4.7, por ser familiar aos usuários mas pode se tornar inconveniente considerando a necessidade recorrente de

digitação do código [53]. No aspecto de viabilidade técnica, demonstrado na tabela 4.8, ele se demonstrou inviável por não apresentar melhoras relevantes e conter vulnerabilidades [54].

A utilização da combinação do OTP + *bluetooth* foi categorizado como fator de alta aderência ao critério de segurança, vide tabela 4.6, por utilizar a proximidade, reduzindo risco de *phising* [50]. Na experiência do usuário, conforme tabela 4.7, sua classificação foi considerada média dado que é conveniente sua utilização quando compatível com o dispositivo do usuário [55] mas possui inviabilidade técnica, demonstrado em 4.8 por requerer compatibilidade de múltiplos dispositivos, pois a exigência do mecanismo de autenticação OTP+Bluetooth na plataforma gov.br pode representar uma barreira de acesso para usuários que não possuem dispositivos móveis com suporte a *Bluetooth*. Esse critério de autenticação pode excluir parte da população em situação de vulnerabilidade socioeconômica, que muitas vezes não dispõe de *smartphones* com essa funcionalidade.

Os fatores adicionais propostos, conforme verificado durante esse trabalho, referem-se em sua maioria a uma maneira de se implementar um MFA, seja utilizando OTP ou sua combinação com outros fatores. A ID gov.br atualmente já implementa o fator de autenticação adicional via OTP para oferecer ao cidadão a opção de receber um código por meio do aplicativo ID gov.br.

O RBA se mostra um fator adicional interessante quando o sistema no qual é aplicado possui uma boa infraestrutura de análise comportamental. Isto é, o sistema coleta dados de localização do usuário e monitora os acessos controlando quando dispositivos diferentes do que o dispositivo inicialmente vinculado efetuam acesso. Para cenários que se diferem do comportamento padrão do usuário, um segundo fator de autenticação é exigido para garantir a autorização de acesso. Na perspectiva de segurança, o RBA foi considerado como Alto, conforme tabela 4.6 por detectar padrões de riscos e acionar autenticações extras apenas a partir dessas situações suspeitas [56]. Sob a ótica da experiência do usuário o RBA também foi categorizado como alto, considerando o impacto mínimo para o usuário [54], conforme tabela 4.7. E por fim, na avaliação técnica, o RBA se demonstrou viável por ter a possibilidade de ser integrado à infraestrutura atual porém requer atenção à conformidade com a LGPD.

Tabela 4.6: Avaliação dos Fatores Adicionais de Segurança

Fator Analisado	Segurança	Justificativa
Tripwire	Média	Protege contra ataques de credenciais comprometidas, mas vulnerável a engenharia social [51].
Login Rituals	Média	Melhora segurança contra ataques de credenciais roubadas, mas suscetível a observação [52].
OTP + SHA1	Baixa	Estudos apontam que não melhora significativamente a segurança em relação ao OTP convencional [54].
OTP + Bluetooth	Alta	Usa autenticação baseada em proximidade, reduzindo riscos de phishing [50].
RBA	Alta	Detecta padrões de risco e aciona autenticações extras apenas em situações suspeitas [57, 56].

Tabela 4.7: Avaliação da Experiência do Usuário

Fator Analisado	Experiência do Usuário	Justificativa
Tripwire	Baixa	Requer configuração prévia e pode ser esquecida pelo usuário [55].
Login Rituals	Baixa	Usuário precisa lembrar o ritual, dificultando a usabilidade [52].
OTP + SHA1	Média	Familiar para usuários, mas pode ser inconveniente devido à necessidade frequente de digitação [53].
OTP + Bluetooth	Média	Conveniente quando compatível, mas pode falhar em dispositivos sem Bluetooth [54].
RBA	Alta	Pouco impacto no usuário legítimo, pois solicita autenticação extra apenas em situações suspeitas [54].

Tabela 4.8: Avaliação da Viabilidade Técnica

Fator Analisado	Viabilidade Técnica	Justificativa
Tripwire	Inviável	Implementação complexa e pouco compatível com sistemas de larga escala [51].
Login Rituals	Inviável	Requer armazenamento e processamento de padrões individuais, dificultando a adoção [52].
OTP + SHA1	Inviável	Estudos indicam que não apresenta melhorias relevantes e tem vulnerabilidades [54].
OTP + Bluetooth	Inviável	Requer compatibilidade com múltiplos dispositivos e pode ser vulnerável a ataques de relay [50].
RBA	Viável	Pode ser integrado à infraestrutura existente, mas requer conformidade com a LGPD e processamento em tempo real [56].

Diante do exposto, **o RBA foi o mecanismo que mais demonstrou potencial, conforme resumo da avaliação apresentado na tabela 4.9, para ser aplicado à ID gov.br**, pois a escolha do RBA como mecanismo de autenticação adicional na plataforma gov.br foi fundamentada em uma análise dos fatores identificados ao longo desta pesquisa, bem como o alinhamento das necessidades junto aos gestores da plataforma.

Tabela 4.9: Classificação Consolidada dos Fatores Adicionais de Autenticação

Fator Analisado	Segurança	Experiência do Usuário	Viabilidade Técnica
RBA	Alta	Alta	Viável
Tripwire	Média	Baixa	Inviável
Login Rituals	Média	Baixa	Inviável
OTP + SHA1	Baixa	Média	Inviável
OTP + Bluetooth	Alta	Média	Inviável

Dentre os fatores analisados, a proteção contra ataques baseados em roubo de credenciais foi um dos aspectos determinantes para a escolha do RBA. Esse mecanismo possui um diferencial importante em relação a métodos tradicionais, pois realiza uma avaliação da tentativa de login, identificando padrões suspeitos antes de aplicar um fator adicional de autenticação. Ao contrário de abordagens estáticas, como o duplo fator de autenticação (2FA), que exige uma validação extra em todas as tentativas de acesso, o RBA só é acionado em situações de risco, reduzindo as chances de fraudes e acessos não autorizados. Dessa forma, o sistema agrega uma camada extra de proteção sem comprometer a fluidez do processo de autenticação.

Outro critério que influenciou a decisão foi a experiência do usuário, uma vez que métodos de autenticação que exigem verificações adicionais a cada tentativa de login podem ser considerados intrusivos e gerar atrito no acesso aos serviços digitais, especialmente em plataformas governamentais de grande escala. O RBA se destaca por oferecer uma solução mais eficiente nesse aspecto, pois minimiza interrupções desnecessárias e mantém a usabilidade da plataforma, acionando desafios adicionais apenas quando há indícios de atividade suspeita. Dessa forma, a solução equilibra segurança e praticidade, garantindo uma proteção sem afetar negativamente a jornada do usuário.

A viabilidade técnica e a integração com a plataforma gov.br também foram aspectos determinantes para a adoção do RBA. As demais abordagens, como Tripwire e Login Rituals, apesar de apresentarem potencial em determinados cenários, demandariam modificações significativas na interface do sistema e no comportamento dos usuários, o que poderia comprometer a adoção da solução em larga escala.

Diante dessa análise, o RBA demonstrou ser o mecanismo mais adequado para reforçar a segurança da identidade digital na plataforma gov.br, ao oferecer proteção dinâmica contra ameaças, melhor experiência do usuário e viabilidade técnica de implementação.

4.3 Resultados da Fase 3

A Fase 3, tem como objetivo a implementação do fator adicional de autenticação, dando início a coleta das evidências do estudo de caso.

Nesse sentido, o RBA esteve ativo na plataforma gov.br durante 74 dias, entre 19/08/2024 até 1º/11/2024. Dois conjuntos de dados relativos a esse período foram disponibilizados para análise da implementação do RBA na plataforma ID gov.br, os quais são: **relatórios diários de logins** e **informações detalhadas por estado**. O primeiro arquivo[42] relacionado aos logins diários (LD) é composto por:

LD.A **Data**: Data em que os logins foram efetuados;

LD.B **Total Geral de Logins:** Quantidade total de logins naquela data;

LD.C **Total com Localização:** Quantidade total de logins para usuários com localização compartilhada naquela data;

LD.D **% de Localização em relação ao Total Geral:** Percentual de logins com localização compartilhada em relação ao total geral de logins naquela data, fórmula:

$$LD.D = (\frac{LD.C}{LD.B}) \tag{4.2}$$

LD.E **Total com Vinculação:** Quantidade total de logins que possuem vinculação de dispositivo naquela data ;

LD.F **% de Vínculo em relação ao Total Geral:** Percentual de logins para dispositivos vinculados em relação ao total geral de logins naquela data, fórmula:

$$LD.F = (\frac{LD.E}{LD.B}) \tag{4.3}$$

LD.G **% de Vínculo em relação à Localização**: Percentual de logins para dispositivos vinculados em relação ao total de logins com localização naquela data, fórmula:

$$LD.G = (\frac{LD.E}{LD.C}) \tag{4.4}$$

LD.H **Total Estado Diferente**: Quantidade total de logins que foram efetuados em estados diferentes do estado em que foi efetuada a vinculação naquela data;

LD.I **% em Estado Diferente em relação ao Total Geral**: Percentual de logins efetuados em estado diferente do estado em que foi efetuada a vinculação em relação ao total geral de logins naquela data, fórmula:

$$LD.I = (\frac{LD.H}{LD.B}) \tag{4.5}$$

LD.J **% em Estado Diferente em relação Total com Vinculação**: Percentual de logins efetuados em estado diferente do estado em que foi efetuada a vinculação em relação ao total logins com vinculação de dispositivos naquela data, fórmula:

$$LD.J = (\frac{LD.H}{LD.E}) \tag{4.6}$$

LD.K **Total Mesmo Estado**: Quantidade total de logins que foram efetuados em estados iguais ao estado em que foi efetuada a vinculação naquela data;

LD.L **% de Total mesmo Estado em relação ao Total Geral**: Percentual de logins efetuados no mesmo estado em que foi efetuada a vinculação em relação ao total geral de logins naquela data, fórmula:

$$LD.L = (\frac{LD.K}{LD.B}) \tag{4.7}$$

LD.M **% de Total Mesmo Estado em relação ao Total com Vinculação**: Percentual de logins efetuados no mesmo estado em que foi efetuada a vinculação em

relação ao total logins com vinculação de dispositivos naquela data, fórmula:

$$LD.M = (\frac{LD.K}{LD.E}) \tag{4.8}$$

O segundo arquivo [43] com os dados a serem analisados, corresponde às **informações de logins detalhadas por estado** (LE), que contém 32.640 registros do período em que o RBA esteve ativo em ambiente produtivo (19/08/2024 a 1º/11/2024), por isso uma amostra desses dados é apresentada no Anexo I e uma versão total é disponibilizada em [43] . A estrutura do arquivo contém as seguintes colunas:

LE.A **Data:** Data em que os logins foram efetuados;

LE.B **Estado do Dispositivo:** Estado em que foi efetuado o login no Aplicativo gov.br;

LE.C **Estado no Aplicativo:** Estado em que o Dispositivo foi primariamente vinculado;

LE.D **Total Mesmo Estado:** Quantidade total de logins que ocorreram no mesmo estado em que o dispositivo foi previamente vinculado naquela data;

LE.E **Total Estado Diferente:** Quantidade total de logins que ocorreram estado diferente do estado em que dispositivo foi previamente vinculado naquela data;

LE.F **Total com Localização:** Quantidade total de logins para usuários que autorizaram o compartilhamento de localização.

4.3.1 Implementação do RBA

Com a escolha do fator adicional descrito nos capítulos anteriores, serão apresentados a seguir os passos para implementação do RBA como fator adicional no gov.br. O processo de desenvolvimento do gov.br, envolve um time multidisciplinar com conhecimentos sólidos das regras de negócios já existentes na plataforma. Assim, o surgimento de uma nova funcionalidade é primeiramente avaliado do ponto de vista funcional, questionando-se: "Espera-se agregar significativo valor para a plataforma e, consequentemente, para o cidadão que a utiliza?" Se essa premissa for respondida de maneira positiva, o próximo passo é avaliar as diretrizes de segurança e a necessidade de revisão dos normativos, como o Termo de Uso (TU) e o Aviso de Privacidade (AP).

A partir disso, a funcionalidade é movida para o *backlog* e aguarda a priorização dos gestores e entrada na *sprintbacklog* para implementação. Uma vez priorizado, acontece a reunião com o fornecedor responsável pelo desenvolvimento de software para explicação da necessidade bem como o que se espera com a implementação daquela funcionalidade.

A partir desse primeiro contato, o fornecedor estimará o esforço necessário para o desenvolvimento, e quais requisitos não funcionais e ajustes de arquitetura serão envolvidos e/ou necessários nesta demanda.

Do outro lado, o time do gov.br se encarrega de detalhar e escrever os requisitos da funcionalidade a ser desenvolvida, mapear seus fluxos, a prototipação das telas e mensagens que serão exibidas para o cidadão. O processo descrito acima ocorre conforme fluxo abaixo 4.2.

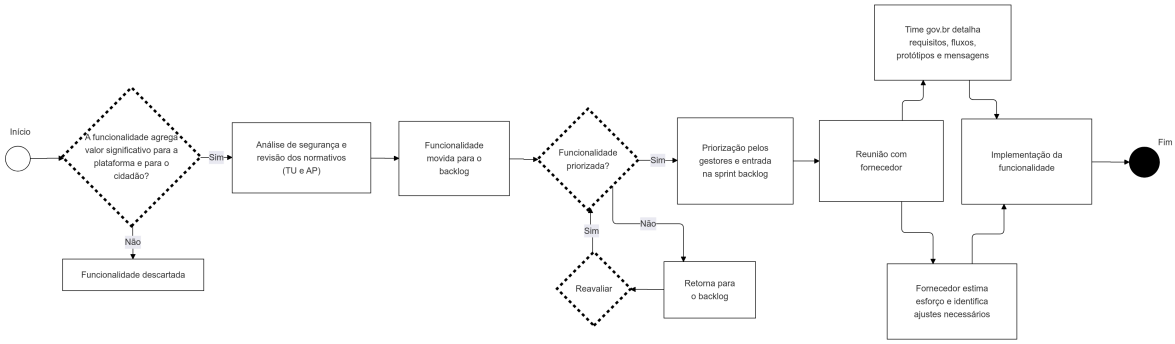

Figura 4.2: Processo de Prioização de demandas no Gov.br. Fonte: autor

O RBA será utilizado para alertar o cidadão sobre a tentativa de login em uma localidade diferente da localidade padrão comumente utilizada e não quando o cidadão não possuir a funcionalidade de gestão de dispositivos habilitada no aplicativo gov.br, permitindo dupla checagem no momento na autenticação.

4.3.2 Implementação da Gestão de Dispositivos

Durante a implantação do RBA percebeu-se a necessidade de ter a funcionalidade de gestão de dispositivos já disponibilizada na plataforma gov.br, como uma premissa. Isso se fez necessário, devido a necessidade de controlar quais os dispositivos estão sendo utilizados no processo de autenticação, sejam eles dispositivos móveis (celular ou tablet) ou desktops/notebooks.

Para implantação da funcionalidade de Gestão de Dispositivos, foram definidos alguns conceitos no âmbito do gov.br relativos aos dispositivos a serem utilizados pelos usuários, a saber:

Dispositivo autorizador: Trata-se do único dispositivo móvel com o aplicativo gov.br instalado e vinculado à conta do usuário, capacitado a realizar ações relacionadas à autorização de novos dispositivos. Este dispositivo pode receber ou gerar tokens de autorização, realizar autorizações diretas ou transferir a função de Dispositivo Autorizador para outro dispositivo móvel com o aplicativo gov.br devidamente instalado e

vinculado. De modo geral, o Dispositivo Autorizador é definido como o primeiro dispositivo vinculado pelo usuário. Para usuários que já possuíam um aplicativo vinculado antes da implementação desta regra, o aplicativo previamente associado será automaticamente convertido em Dispositivo Autorizador.

Dispositivo autorizado: Representa qualquer dispositivo que receba autorização por um dos meios oferecidos:

1. Login com autorização por token enviado/gerado no dispositivo autorizador (2FA atual);
2. Autorização por funcionalidade "Autorizar dispositivo" no dispositivo autorizador (aplicativo gov.br);
3. Autorização automática nos casos a seguir:
   - 3.1 Login com certificado digital;
   - 3.2 Login com banco;
   - 3.3 Login com QR Code/ Login com aplicativo (usando o dispositivo autorizador);
   - 3.4 Criação de conta por método que envolva validação biométrica (facial);
   - 3.5 Criação de conta por método que envolva validação em bancos credenciados;
   - 3.6 Recuperação de conta por método que envolva validação biométrica (facial);
   - 3.7 Recuperação de conta por método que envolva validação em bancos credenciados.

Dispositivo Vinculado: Para esse conceito, a regra atual é aplicada somente ao dispositivo com aplicativo gov.br:

- ID Bronze - logará no app sem necessidade de vinculação, mas com acesso restrito;
- ID Prata - pode vincular: por biometria (CNH) ou Login com banco;
- ID Ouro - pode vincular: somente com biometria (ICN ou CIN).

Pós definição desses conceitos, foram estabelecidas as regras relativas que relacionam a gestão de dispositivo ao nível da conta do cidadão, vide 2.2 na Seção 2.2 do Capítulo 2. O login na conta gov.br somente será liberado com amplo acesso (correspondente a nível prata e ouro) se realizado a partir de um dispositivo autorizado. Quando um novo acesso for realizado a partir de um dispositivo não autorizado, e não for realizado pelos métodos que já garantem autorização automática, a plataforma deverá informar que o acesso dependerá de uma autorização do dispositivo e:

1. Identificar se o usuário possui um dispositivo autorizador ativo. Se sim, usar esta opção de autorização;

2. Não possuindo um dispositivo autorizador ativo, ou o usuário pular a etapa anterior, orientar as demais formas de autorização automática;

3. Se o usuário não desejar realizar a etapa anterior, informar que o login poderá ser realizado mas com acesso limitado, e por isso não terá acesso a serviços que exigem nível prata ou ouro. O dispositivo irá para lista de pendentes de autorização e poderá ser autorizado mais tarde.

Por fim, cabe destacar que as regras foram definidas considerando o nível da conta do cidadão no momento do acesso, e não o potencial nível de acesso que o usuário pode obter. Dessa forma, em um cenário em que um CPF, mesmo possuindo biometria na base de dados da ICN, não tenha realizado acesso via web e não tenha aumentado o nível, permanecendo como bronze, nível inicial, esse cidadão estará sujeito à aplicabilidade da regra de ID bronze. Se o cenário for para ID prata (Sigepe ou banco), aplicar-se-á a regra prata com biometria.

Esse fluxo é apresentado na imagem a seguir 4.3:

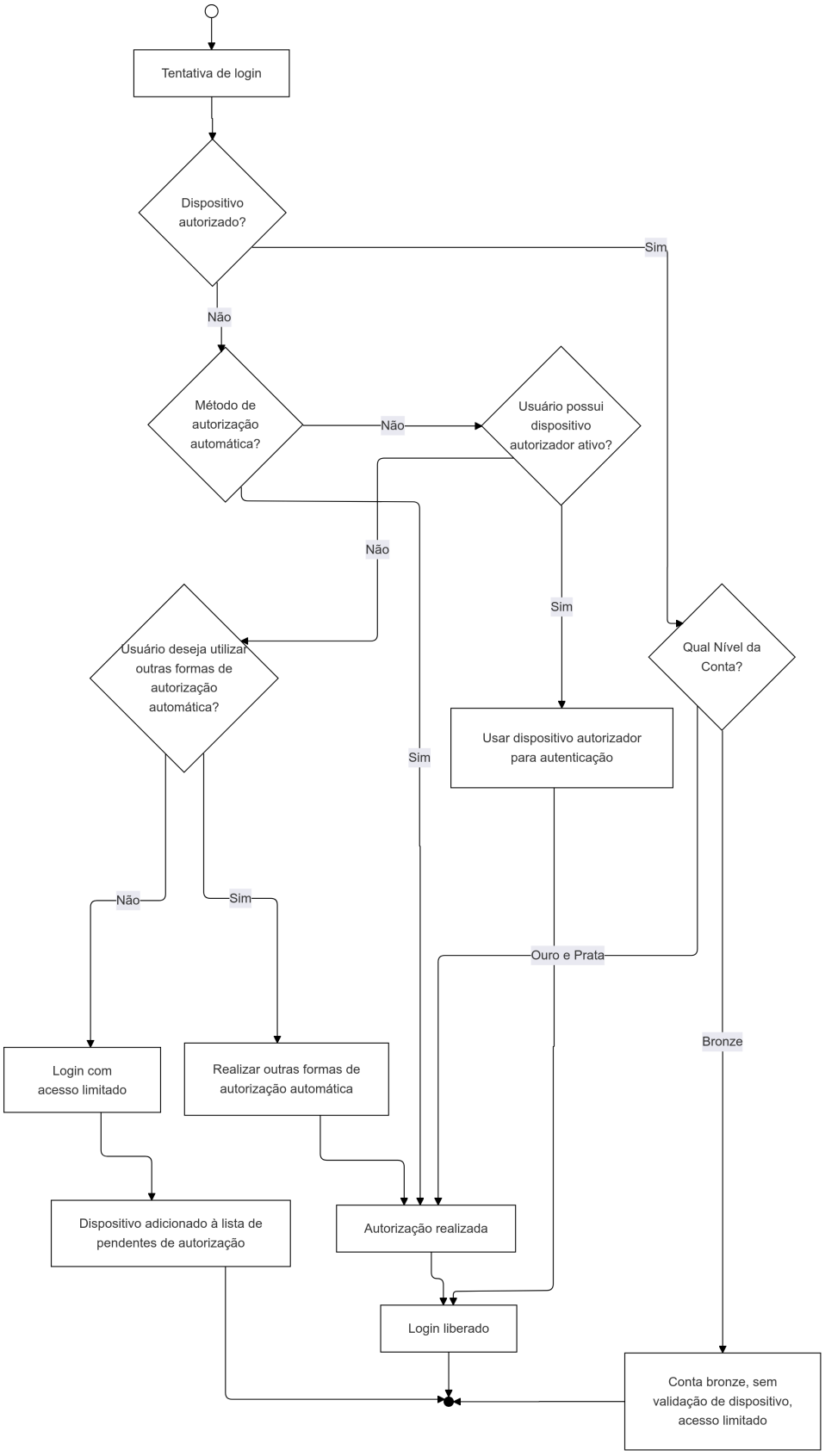

Figura 4.3: Processo de Autorização de Dispositivos de acordo com nível de conta gov.br. Fonte: autor

4.3.2.1 Desafios para Implantação da Gestão de Dispositivos

Durante o processo de priorização da demanda do RBA, para a implantação da funcionalidade de gestão de dispositivos, foi constatado que desenvolver esse controle internamente demandaria um esforço significativo da equipe, enquanto soluções pré-existentes no mercado poderiam atender às necessidades de demandando menos esforço de codificação e consequentemente menos comprometimento dos recursos.

O fornecedor do time gov.br havia previamente avaliado e planejou uma migração tecnológica, especificamente a transição do motor de autenticação MitreID para o RHSSO (RedHat Single Sign-On), que possui controle de dispositivos nativo. Diante disso, os gestores do projeto login gov.br decidiram aguardar essa migração e pausar a priorização do fluxo de gestão de dispositivos previamente apresentado.

O time gov.br acompanhou e participou da migração que apresentou diversos desafios, exigindo múltiplos testes de performance com a nova tecnologia para assegurar que os requisitos não funcionais fossem mantidos e que os serviços públicos digitais oferecidos aos cidadãos não sofressem impactos negativos. Além disso, a migração envolveria a transição da solução de hospedagem para uma nuvem privada, o que adicionou um nível maior de complexidade ao processo.

É importante destacar que, para realizar essa migração, era crucial que não houvesse eventos sazonais de grande volume de utilização de serviço público em andamento, como o ENEM, SISU ou a Declaração de Imposto de Renda. Esses eventos poderiam afetar a disponibilidade de acesso à plataforma, uma vez que seria necessário deixá-la offline durante a migração. A decisão de adotar uma solução pronta, como o RHSSO, foi estratégica, pois permitiria à equipe focar em outras áreas críticas do projeto, enquanto se beneficiava de uma tecnologia robusta e já testada no mercado.

Para o processo de migração, a equipe realizou uma série de testes rigorosos no intuito de garantir que a nova solução atendesse a todos os requisitos de desempenho e segurança. Esses testes incluíram simulações de carga para verificar a capacidade do sistema de lidar com um grande número de usuários simultâneos, bem como avaliações de segurança para identificar e mitigar possíveis vulnerabilidades.

A mudança para uma nuvem privada também foi uma decisão estratégica, visando aumentar a segurança e o controle sobre os dados sensíveis gerenciados pelo sistema gov.br. A nuvem privada oferece vantagens significativas em termos de personalização e segurança, permitindo que as equipes configurem o ambiente de acordo com as necessidades específicas do projeto. Essa abordagem possibilita maior controle sobre dados e infraestrutura, atendendo a requisitos rigorosos de privacidade e conformidade, o que a torna ideal para ambientes sensíveis, como os projetos desenvolvidos em departamentos de sistemas de

informação. Estudos recentes reforçam esses benefícios, destacando como as organizações podem explorar as vantagens da nuvem privada para otimizar suas operações [58, 59].

Houve um planejamento meticuloso com intuito de minimizar o impacto nos usuários finais. Para isso, a equipe estabeleceu um cronograma detalhado, coordenando com outros órgãos para garantir que a transição ocorresse de maneira fluida, sem interrupções significativas na prestação dos serviços públicos digitais.

A migração foi realizada, mas após dois dias de instabilidade na plataforma, foi necessário um rollback para a tecnologia anterior. Durante as semanas seguintes, a equipe junto aos especialistas dos fabricantes avaliaram a viabilidade de tentar uma nova migração. No entanto, os testes de performance foram insatisfatórios, levando os gestores do gov.br a decidirem não realizar uma nova tentativa de migração.

Consequentemente, os recursos inicialmente previstos para serem aproveitados a partir da solução pré-existente do RHSSO precisaram ser desenvolvidos integralmente do zero pela equipe técnica em colaboração com o fornecedor. Isso fez com que o backlog da plataforma aumentasse significativamente, uma vez que, durante o período que antecedeu a migração e durante a própria migração, houve um congelamento do ambiente. Esse período, comumente chamado de "congelamento", pode ser definido como quando novas funcionalidades são temporariamente impedidas de disponibilização no ambiente produtivo para garantir a estabilidade e evitar a introdução de erros ou problemas nesse ambiente.

Superado esse momento, as demandas do backlog começaram a ser atendidas à medida que o time definidor avançava com os requisitos. Considerando a necessidade da gestão de dispositivos como condição para a implementação do RBA, os gestores precisaram conciliar a resolução das funcionalidades pendentes no backlog com a definição e implementação da gestão de dispositivos.

É importante destacar que, ao longo da execução desta implementação, diversas políticas públicas governamentais foram priorizadas, incluindo o Programa Desenrola, o que resultou em repetidos adiamentos na inclusão do escopo na sprint backlog. Essas políticas públicas geraram um volume significativo de demandas para a equipe do gov.br, acarretando sucessivos replanejamentos na gestão de dispositivos e, por conseguinte, na implementação e operação do RBA. A priorização de políticas públicas no desenvolvimento de sistemas tecnológicos é frequentemente citada na literatura como um fator de impacto na gestão de projetos, especialmente em ambientes governamentais, onde a flexibilidade é essencial para atender a iniciativas de interesse público [60, 61].

4.3.2.2 Gestão de Dispositivos no Aplicativo

O Fluxo 1 - Gestão de Dispositivos no aplicativo, representa o processo de gestão dos dispositivos associados a um usuário dentro de um aplicativo, conforme imagem 4.4. O fluxo é estruturado em etapas distintas que envolvem o login gov.br, a confirmação de identidade, a visualização de dispositivos ativos e as ações subsequentes de autorização ou bloqueio de dispositivos. Esse processo foi modelado de forma a garantir a segurança, a eficiência e a transparência no gerenciamento dos dispositivos cadastrados.

O fluxo inicia-se com a tela de acesso ao aplicativo, onde o usuário realiza o login gov.br inserindo suas credenciais. Alternativamente, o sistema também permite o acesso via login com bancos e QRCode ou certificado digital. Após a conclusão desta etapa, o usuário é direcionado para a área de gestão de dispositivos, na qual é possível visualizar a lista de dispositivos atualmente registrados.

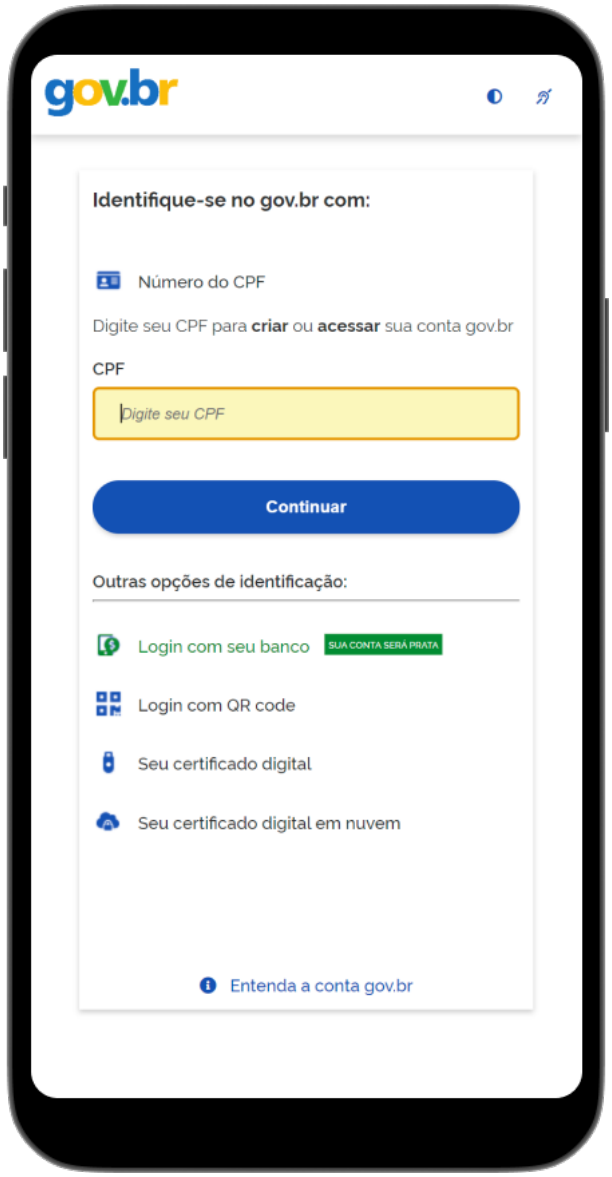

Figura 4.4: Tela de Login do App gov.br. Fonte: gov.br

Um aspecto relevante deste fluxo é a etapa intermediária de segurança adicional, onde o usuário deve validar sua identidade ou realizar alguma confirmação para prosseguir. Essa etapa é crítica para a integridade do sistema e está destacada no diagrama como uma tela de segurança extra. A validação pode envolver múltiplas técnicas, como a confirmação de senha, códigos de autenticação enviados ao usuário ou métodos biométricos.

Após a validação, a lista de dispositivos associados ao usuário é apresentada. A partir desta visualização, as principais ações possíveis estão relacionadas às decisões de autorização ou bloqueio de dispositivos. O processo de tomada de decisão segue regras predefinidas e possui implicações específicas, conforme descrito a seguir:

- **Autorização de Dispositivo:** Quando o dispositivo é autorizado, ele é marcado

como ativo, permitindo o seu uso normal dentro do sistema. O fluxo de autorização está representado no modelo por setas azuis e inclui uma tela de confirmação para garantir que o usuário tenha ciência do sucesso da operação. A autorização pressupõe a validação prévia do dispositivo e a conformidade com os critérios de segurança do sistema.

- **Bloqueio de Dispositivo:** Caso o dispositivo seja bloqueado, ele passa a ser marcado como restrito, o que impede sua utilização no aplicativo. Esse processo é representado por setas vermelhas no modelo, levando a uma tela específica que informa o usuário sobre o bloqueio. Além disso, o sistema emite alertas para garantir que o usuário tenha ciência da ação realizada.

Outro aspecto relevante é a presença de avisos automáticos, que atuam como notificações emitidas pelo sistema em situações críticas, como a autorização ou o bloqueio de dispositivos. Esses alertas, destacados no modelo por setas amarelas, contribuem para a transparência do processo e aumentam a percepção de segurança por parte do usuário.

Portanto, o fluxo de Gestão de Dispositivos no aplicativo apresenta uma estrutura robusta e organizada, composta por etapas sequenciais que visam atender às exigências de segurança e experiência do usuário. As tomadas de decisão entre autorização e bloqueio são claramente definidas, com caminhos e interfaces específicas que garantem a efetividade das operações. Dessa forma, o modelo reforça a importância de procedimentos de validação e notificação, alinhados às melhores práticas de governança e gestão de dispositivos digitais em ambientes seguros.

4.3.2.3 Fluxo de acesso com a função habilitada apenas para dispositivos autorizados

O presente fluxo tem como objetivo permitir que um usuário acesse um serviço utilizando um dispositivo que não esteja previamente autorizado, observando as regras de negócio previamente definidas. Este processo está dividido em três principais etapas: o acesso ao serviço, o login e as interações realizadas no aplicativo vinculado ao aplicativo gov.br.

Inicialmente, o usuário tenta acessar o serviço por meio de um dispositivo novo. Nesse momento, o sistema apresenta uma interface solicitando as credenciais de login, marcando o início do fluxo. Após a inserção do login e da senha na página de autenticação, os dados são enviados para verificação. Caso a chave acesso apenas para dispositivos autorizados esteja habilitada e o dispositivo utilizado não tenha sido previamente autorizado, o acesso será negado temporariamente. Tal medida caracteriza uma importante restrição de segurança, direcionando o usuário para um procedimento específico no aplicativo vinculado, com o intuito de autorizar o dispositivo em questão.

Na sequência, o usuário recebe uma notificação no aplicativo informando a tentativa de acesso realizada por um dispositivo não autorizado. Essa notificação solicita a autorização manual do novo dispositivo. Para tanto, o usuário deve acessar o aplicativo gov.br e navegar até a Seção de gerenciamento de dispositivos, onde o dispositivo pendente aparece destacado. Nesta aba, é possível realizar a confirmação da autorização, concedendo ao dispositivo permissão para acessar o serviço.

Após a autorização, o dispositivo é liberado, permitindo ao usuário retornar ao serviço e concluir o processo de login com sucesso. Dessa forma, o fluxo contempla uma transição entre a etapa inicial de tentativa de login e a interação necessária no aplicativo gov.br para a liberação do dispositivo, reforçando as políticas de segurança da organização.

Em suma, o mecanismo implementado busca garantir maior controle e segurança nos acessos realizados por dispositivos novos. Caso o login seja realizado a partir de um dispositivo não autorizado, o acesso será bloqueado temporariamente, e o usuário será notificado para proceder com a validação manual por meio do aplicativo. Essa validação manual tem como finalidade central assegurar que somente dispositivos previamente autorizados tenham acesso aos serviços, mitigando riscos e fortalecendo o controle de acessos.

A regra principal desse fluxo é clara: a chave "Acesso Apenas para Dispositivos Autorizados"impede que dispositivos não autorizados acessem os serviços, sendo indispensável que a autorização ocorra pelo aplicativo gov.br antes que o login seja concluído. Assim, o processo implementado não apenas notifica o usuário, mas também exige a sua validação ativa, garantindo uma camada adicional de proteção e controle. Essa abordagem, portanto, reforça as políticas de segurança adotadas, exigindo que todo novo dispositivo seja validado de forma manual e consciente pelo usuário antes de obter acesso ao serviço.

4.3.2.4 Fluxo de acesso com a função desabilitada apenas para dispositivos autorizados

O fluxo aborda o processo de autenticação de um usuário ao tentar acessar um serviço a partir de um dispositivo novo, com a configuração chave de acesso apenas para dispositivos autorizados desabilitada. Esse cenário está estruturado em três camadas principais: **Serviço**, **Login** e **Aplicativo**, cada uma desempenhando um papel específico no processo.

Inicialmente, o usuário acessa o site do serviço desejado, navegando até a opção de login para iniciar a autenticação. Em seguida, ele é redirecionado para a página de autenticação do gov.br, onde insere suas credenciais, como CPF e senha, para prosseguir. Uma vez autenticado, o sistema realiza uma análise para verificar se o dispositivo utilizado já foi previamente registrado. Como se trata de um dispositivo novo, e a chave de acesso para

dispositivos autorizados está desabilitada, o processo requer uma validação adicional para garantir a segurança.

Nesse momento, o sistema dispara notificações para o usuário por meio de diferentes canais previamente cadastrados. Essas notificações podem ser enviadas via e-mail, SMS ou pelo aplicativo vinculado à conta. O objetivo desta etapa é informar ao usuário sobre a tentativa de acesso e solicitar a validação do novo dispositivo. Cabe ao usuário confirmar a legitimidade do acesso respondendo à notificação recebida. Sem essa confirmação, o dispositivo permanece não autorizado, e o acesso ao serviço é bloqueado.

Uma vez que o usuário valida o novo dispositivo por um dos canais disponíveis, o sistema concede a autorização temporária, permitindo que o acesso ao serviço seja concluído com sucesso. Esse processo assegura que apenas o usuário legítimo possa realizar ações em dispositivos novos, mesmo com a configuração de dispositivos autorizados desabilitada.

As regras de negócio que regem esse fluxo reforçam a segurança e flexibilidade do sistema. A autenticação no gov.br é obrigatória para todos os acessos, e as credenciais inseridas devem corresponder aos dados previamente registrados. O sistema identifica automaticamente dispositivos novos e aciona notificações para validação, garantindo que o usuário seja o responsável por autorizar ou negar o acesso. Assim, mesmo com a chave de restrição desabilitada, é mantido um controle sobre quem pode acessar o serviço e a partir de quais dispositivos.

Portanto, esse fluxo equilibra segurança e acessibilidade, permitindo o uso de dispositivos novos mediante validação, ao mesmo tempo que protege os dados do usuário contra acessos não autorizados.

4.3.2.5 Fluxo de acesso com dispositivo bloqueado

O fluxo descreve o processo de autenticação de um usuário em um serviço quando o dispositivo utilizado está bloqueado. Esse fluxo está organizado em três camadas principais: Serviço, Login e App, que estruturam o caminho seguido pelo usuário para acessar o sistema e validar o dispositivo.

O processo inicia na camada de serviço, onde o usuário acessa o site do serviço desejado e seleciona a opção de login. A partir daí, ele é redirecionado para a página de autenticação do gov.br, na qual insere suas credenciais, como CPF e senha. Após a validação destas informações, o sistema verifica o status do dispositivo utilizado. Nesse caso, o dispositivo é identificado como bloqueado, o que impede a continuidade do acesso direto ao serviço.

Ao identificar um dispositivo bloqueado, o sistema dispara notificações para os canais previamente cadastrados pelo usuário. Essas notificações são enviadas por meio de e-mail, SMS e aplicativo, contendo as instruções necessárias para a validação do dispositivo. Por

exemplo, o e-mail pode trazer um link ou código de autorização, enquanto a mensagem de SMS e o aplicativo fornecem métodos alternativos para desbloqueio.

A validação do dispositivo é obrigatória para prosseguir no fluxo. O usuário deve acessar um dos canais de notificação e seguir as instruções para confirmar a legitimidade do dispositivo. Somente após a validação bem-sucedida, o dispositivo é temporariamente autorizado, permitindo que o usuário retorne ao fluxo e conclua o acesso ao serviço.

As regras de negócio que sustentam esse fluxo priorizam a segurança do sistema. A autenticação no gov.br é obrigatória, garantindo que apenas usuários com credenciais válidas avancem no processo. O sistema realiza uma análise automática do dispositivo para verificar seu status. Caso esteja bloqueado, ele não permite o acesso até que seja validado pelo usuário. A validação é um pré-requisito fundamental, que assegura que apenas dispositivos reconhecidos sejam utilizados, protegendo as informações e serviços acessados.

Além disso, o envio de notificações por múltiplos canais – e-mail, SMS e app – oferece flexibilidade ao usuário para desbloquear o dispositivo, mantendo um alto nível de segurança e conveniência. Dispositivos que não passam por essa etapa permanecem bloqueados, garantindo que acessos indevidos sejam evitados.

Portanto, o fluxo apresenta um processo claro e seguro para lidar com dispositivos bloqueados. Ele combina autenticação, notificação e validação, reforçando a segurança do sistema e oferecendo ao usuário controle sobre os dispositivos que podem acessar os serviços. Esse equilíbrio entre segurança e flexibilidade é essencial para proteger os dados e garantir uma experiência confiável para o usuário.

4.3.3 Definição de Requisitos do RBA

A administração de dispositivos, no âmbito do controle RBA, tem como foco central reforçar a segurança durante o processo de autenticação dos usuários no gov.br. Esse mecanismo considera o dispositivo utilizado para o login como uma camada adicional de proteção, bloqueando acessos provenientes de dispositivos diferentes daqueles previamente autorizados e registrados pelo próprio usuário. Esse mecanismo é ativado em condições específicas, gerando notificações ou impedindo o acesso caso sejam detectadas atividades suspeitas.

Por outro lado, o monitoramento da localização geográfica desempenha um papel igualmente relevante dentro do contexto do RBA. Essa funcionalidade utiliza a posição geográfica como um elemento complementar de segurança, restringindo tentativas de acesso realizadas fora da área em que o dispositivo foi vinculado pelo usuário. O conceito de localidade padrão refere-se ao estado informado pelo usuário no momento da vinculação do aplicativo gov.br à sua conta. Essa vinculação, por sua vez, só ocorre caso o cidadão

autorize o aplicativo a capturar sua localização geográfica. A ausência dessa permissão impede o processo. Além disso, o controle RBA só será ativado caso essas condições sejam atendidas.

4.3.3.1 Adaptação na Implantação do RBA e Gestão de dispositivos

Durante a fase de implantação da funcionalidade de gestão de dispositivos no contexto do RBA para a identidade digital gov.br, surgiram solicitações importantes por parte dos principais órgãos públicos. **Essas instituições destacaram a necessidade de um modelo mais transparente de gestão de dispositivos, sugerindo que o mecanismo não se restringisse ao funcionamento em segundo plano**, mas que fosse oferecida ao cidadão uma interface ativa para habilitação e gerenciamento de seus dispositivos. Essa funcionalidade permitiria que o usuário visualizasse os dispositivos autorizados, identificasse aqueles que não reconhecesse e revogasse de forma fácil e rápida o acesso desses equipamentos à sua conta.

Essa solicitação, que inicialmente não fazia parte das regras de negócio para o RBA, trouxe implicações significativas para a equipe de desenvolvimento e análise do gov.br. O planejamento inicial previa que a gestão de dispositivos atuaria silenciosamente, apenas fornecendo suporte ao algoritmo do RBA para análise de riscos. Nesse modelo original, as interações do usuário seriam mínimas, limitadas à execução de verificações adicionais apenas em situações identificadas pelo mecanismo. Contudo, o pedido dos órgãos públicos, respaldado pela relevância forçou uma reconsideração do plano.

A mudança exigiu uma reformulação substancial na abordagem do projeto. A equipe de analistas do gov.br se viu obrigada a revisar os objetivos e prioridades do RBA. O planejamento precisou ser adaptado para incorporar a criação de uma interface interativa, que equilibrasse a usabilidade e a segurança, sem comprometer o desempenho do sistema. Essa interface deveria ser intuitiva e acessível, proporcionando ao cidadão uma experiência de uso que reforçasse sua confiança na plataforma ao mesmo tempo em que mantivesse os altos padrões de segurança exigidos por uma solução crítica como o gov.br.

Essa reformulação não foi isenta de desafios. Além da necessidade de redesenhar o fluxo de desenvolvimento, a mudança de curso também implicou no replanejamento de recursos e na adequação dos cenários de decisão.

A modificação promovida pela solicitação dos órgãos públicos, resultou em uma reconfiguração significativa do escopo inicial do mecanismo de RBA. Concebido como um sistema integrado que utilizaria informações provenientes de múltiplas fontes, incluindo a gestão de dispositivos, a reformulação transformou a gestão de dispositivos em uma ferramenta independente e autônoma de segurança. Como consequência direta, o RBA

passou a operar de forma mais restrita, concentrando-se predominantemente na análise de mudanças de localidade geográfica durante tentativas de acesso à plataforma.

Esse redesenho impactou profundamente o funcionamento do RBA. Com a gestão de dispositivos sendo implementada como uma solução separada e diretamente gerenciada pelo usuário, o RBA foi ajustado para verificar se os outros mecanismos de segurança, como o duplo fator de autenticação (2FA) e a própria gestão de dispositivos, estavam ativos. Caso ambos os mecanismos estivessem habilitados, o sistema considerava que os níveis de proteção já eram suficientemente elevados e, portanto, suspendia a aplicação do RBA como camada adicional de análise. Esse ajuste operacional foi justificado pela necessidade de evitar redundâncias e sobrecarregar desnecessariamente os processos de autenticação para os usuários finais.

A decisão de ajustar o RBA para operar em conjunto com o 2FA e a gestão de dispositivos, mas de forma complementar, reflete uma abordagem estratégica que prioriza a experiência do usuário sem comprometer a segurança. A mudança no escopo do RBA e sua integração com outros mecanismos de segurança exemplificam a flexibilidade necessária para atender às demandas práticas e estratégicas da plataforma gov.br e sua grande volumetria.

4.3.3.2 Regras e Fluxos do RBA

Com o ajuste na implementação, o funcionamento do RBA no contexto da plataforma gov.br foi estruturado com base em uma lógica condicional que se adapta às configurações de segurança habilitadas pelo usuário. Esse fluxo visa garantir a proteção ao mesmo tempo que otimiza a experiência do cidadão para não gerar excessos de atritos para realização do login. O processo começa com a autenticação, em que o sistema avalia, primeiramente, se o mecanismo de autenticação de dois fatores (2FA) está ativo, caso o 2FA esteja habilitado, o sistema avança para a próxima etapa de verificação. Na sequência, o mecanismo verifica se a funcionalidade de Gestão de Dispositivos está configurada e em operação, se essa funcionalidade estiver ativa, o RBA é desconsiderado, entendendo que o nível de proteção já é satisfatório. Entretanto, se a gestão de dispositivos estiver desativada, o RBA é acionado para suprir essa lacuna de segurança.

Uma vez ativado, o RBA realiza uma análise do comportamento do acesso, considerando o fator localidade geográfica, Essa análise comportamental tem como objetivo identificar qualquer acesso suspeito em localidade distinta do momento em que houve a vinculação, que possa indicar uma tentativa de acesso não autorizada.

O fluxo do RBA demonstra a capacidade de se adaptar às configurações de segurança do usuário. Essa estrutura não apenas eleva o nível de proteção da plataforma e reforça a

confiança dos cidadãos na plataforma gov.br, oferecendo uma experiência personalizada e segura.

O processo inicia-se com a tentativa de login padrão, na qual o usuário insere suas credenciais (nome de usuário e senha). Nesse momento, a plataforma gov.br realiza uma análise baseada na localização atual em relação aos últimos três acessos anteriores, caso nenhuma irregularidade seja detectada, o acesso é liberado. Entretanto, se houver um risco identificado, o fluxo segue para uma validação adicional. Nessa etapa, o usuário precisa confirmar sua identidade por meio de um código que deve ser gerado no aplicativo gov.br. Se a validação for bem-sucedida, o acesso é concedido, e os dados do dispositivo ou localização são registrados como confiáveis para futuras tentativas. Caso contrário, o sistema bloqueia o acesso.

Por fim, o sistema de gestão de dispositivos e o controle RBA representam um avanço significativo na segurança da autenticação, utilizando a geolocalização como uma ferramenta poderosa para evitar acessos não autorizados. No entanto, aspectos operacionais, como mensagens exibidas ao usuário e prazos de validade, ainda demandam validação junto à SGD para garantir alinhamento às normas e uma experiência segura e clara para os usuários.

4.4 Resultados da Fase 4

A Fase 4 tem como objetivo realizar a análise das evidências coletadas e compartilhar os achados do estudo de caso e responder a QP.4 no que se refere a quais os benefícios e/ou problemas identificados após a aplicação dos fatores adicionais a uma Identidade Digital.

4.4.1 Etapa 5 - Analise das Evidências do Estudo de Caso

A **Etapa 5 do estudo de caso consiste na análise das evidências coletadas**, buscando identificar padrões, relações e impactos da implementação do RBA na plataforma gov.br. Segundo Yin [27], a análise dos dados em um estudo de caso deve ser conduzida de forma sistemática, utilizando diferentes técnicas para garantir uma interpretação rigorosa e a extração de conclusões significativas.

Dessa forma, foram executadas nesta etapa as atividades de **Comparação Estatística do Antes e Depois da aplicação do RBA**, em seguida foi efetuada a **aplicação da Triangulação de Evidências** e a **Identificação de Padrões nos Acessos** para análise e geração de hipóteses sobre os dados levantados.

4.4.1.1 Métodos de Análise dos Dados

A análise das evidências coletadas foi realizada por meio de **abordagens quantitativas e qualitativas**, permitindo a avaliação dos impactos do RBA a partir de diferentes perspectivas. A Tabela 4.10 apresenta um resumo das métricas analisadas e os métodos aplicados.

Tabela 4.10: Métodos de Análise das Evidências

Métrica	Descrição	Método de Análise
Taxa de logins com verificação adicional	Percentual de acessos que acionaram verificações extras	Comparação estatística entre períodos pré e pós-implementação do RBA
Distribuição geográfica dos acessos	Localização dos acessos antes e depois da implementação	Análise exploratória de padrões de deslocamento dos usuários

As métricas foram analisadas por meio de técnicas estatísticas descritivas e inferenciais, garantindo uma avaliação do impacto do RBA. Além disso, foi realizada **uma análise comparativa entre períodos anteriores e posteriores à implementação**, permitindo a identificação de mudanças na autenticação dos usuários.

4.4.1.2 Triangulação de Evidências e Validação dos Resultados

Para garantir a a abordagem correta da análise, foi aplicada a técnica de **triangulação de evidências** [27], que consiste na comparação de diferentes fontes de dados para validar os achados da pesquisa. Essa abordagem possibilitou uma interpretação mais confiável dos impactos da implementação do RBA, reduzindo vieses na análise dos resultados. Os seguintes procedimentos foram adotados:

- **Correlação entre métricas quantitativas e qualitativas:** Os dados numéricos foram analisados em conjunto com relatos qualitativos para garantir que os achados estatísticos estivessem alinhados;
- **Validação cruzada entre fontes de evidência:** As informações extraídas dos registros de autenticação foram comparadas com os relatórios operacionais da equipe de segurança do gov.br, garantindo coerência nos resultados;
- **Identificação de padrões recorrentes:** Foram analisadas tendências de comportamento nos acessos à plataforma antes e depois da implementação do RBA, avaliando possíveis impactos positivos e desafios operacionais.

4.4.2 Etapa 6 - Compartilhamento dos achados do Estudo de Caso

A **Etapa 6 do estudo de caso consiste na comunicação e disseminação dos resultados obtidos**, garantindo que as descobertas geradas pela pesquisa sejam documentadas de forma sistemática e possam contribuir para futuras investigações na área de segurança digital e autenticação baseada em risco. Segundo Yin [27], última etapa do estudo de caso deve assegurar que as descobertas sejam compartilhadas de forma estruturada, permitindo que futuras pesquisas possam se basear nesses achados para aprofundamento e evolução da área investigada.

Os achados da pesquisa foram documentados e analisados para subsidiar futuras melhorias na segurança da ID gov.br e contribuir com a literatura acadêmica sobre autenticação digital. Os resultados foram compartilhados com os responsáveis pela gestão da plataforma para avaliação da viabilidade de adoção definitiva dos mecanismos analisados. Além disso, o estudo será disseminado por meio de publicações científicas, apresentações em eventos acadêmicos e relatórios técnicos, possibilitando que outros pesquisadores e profissionais da área de segurança digital possam se beneficiar dos insights gerados pela investigação.

4.4.3 Publicações

Como resultado parcial desta dissertação, o artigo **Identification And Aplicability of Addtional Security Factor on the gov.br Digital Identity Plataform** publicado no CONTECSI USP - International Conference on Information Systems and Technology Management - ISSN 2448-1041, em 19-21 Dezembro 2022 [62], em que foi demonstrado o resultado da RSL.

4.4.4 A dissertação como Principal Meio de Compartilhamento

Neste estudo, a dissertação foi concebida como o principal meio de compartilhamento das evidências e análises realizadas, funcionando como um registro sistemático dos achados. Ao longo dos capítulos, foram apresentados:

- O contexto e a relevância do problema de pesquisa, destacando a necessidade de aprimoramento dos mecanismos de autenticação digital;
- A fundamentação teórica, baseada em uma Revisão Sistemática da Literatura (RSL), que subsidiou a escolha dos fatores adicionais de segurança analisados;

- A metodologia aplicada, detalhando a condução do estudo de caso segundo a abordagem de Yin [27];
- Os resultados obtidos, apresentando a análise das evidências coletadas e os impactos do *Risk-Based Authentication* na plataforma gov.br;
- As conclusões e recomendações para aprimoramento do RBA na plataforma gov.br.

Dessa forma, a dissertação consolida as informações geradas ao longo da pesquisa, permitindo que os leitores compreendam o processo de investigação e análise, além de oferecer um referencial para futuras pesquisas na área de autenticação baseada em risco.

A Etapa 6 assegura que os achados da pesquisa sejam documentados e disseminados de maneira estratégica, permitindo que os resultados gerados possam impactar tanto a prática quanto a pesquisa acadêmica, servindo como base para o aprimoramento contínuo dos mecanismos de segurança digital.

QP.4 Quais os benefícios e/ou problemas identificados após a aplicação dos fatores adicionais a uma Identidade Digital?

A questão de pesquisa QP.4 busca entender os impactos práticos da implementação do RBA no contexto do gov.br, avaliando os benefícios alcançados e os desafios enfrentados. Com base na análise dos dados apresentados e na fundamentação teórica da dissertação, o RBA se implementado na sua totalidade se mostra como uma solução vantajosa para mitigar riscos relacionados a acessos não autorizados e melhorar a experiência do usuário. Os resultados indicam que a aplicação do RBA, ainda que parcialmente, agregou camadas adicionais de segurança a plataforma gov.br, corroborando com estudos prévios que apontam a eficácia desse método em plataformas críticas [49].

Um dos principais benefícios constatados foi a capacidade do RBA de detectar e bloquear comportamentos atípicos.

Para compreender a ação do RBA na plataforma gov.br, foi necessário calcular a métrica que representa a porcentagem de acessos nos quais informações de localização estavam disponíveis em relação ao total de acessos realizados. Essa métrica foi utilizada para avaliar a efetividade da coleta de dados de geolocalização como fator adicional de segurança na autenticação dos usuários.

A métrica [42] *"% de Localização em relação ao Total Geral"* foi obtida por meio da seguinte equação:

$$\%Localização = (\frac{totalAcessosComLocalização}{totalGeralAcessos}) \times 100 \tag{4.9}$$

- **Total de acessos com Localização:** Representa o número de acessos na plataforma em que foi possível identificar a geolocalização do usuário.
- **Total Geral de acessos:** Refere-se ao número total de tentativas de autenticação na plataforma, independentemente da disponibilidade da localização.

Os dados demonstraram que cerca de 1,45% (132.272) dos logins diários acionaram a autenticação baseada em risco (RBA), ou seja, foram acessos em que o sistema identificou um risco potencial e exigiu um fator adicional de autenticação, indicando que o mecanismo foi capaz de identificar padrões de risco, como mudanças de localização.

Esses achados são consistentes com a literatura que ressalta a capacidade do RBA [49] de combinar usabilidade com segurança, permitindo intervenções personalizadas sem sobrecarregar a experiência do usuário [63].

No entanto, alguns desafios foram identificados, especialmente no que se refere à complexidade técnica e operacional do RBA, sendo eles:

- **Monitoramento contínuo de dados de localização**: Refere-se a rastrear constantemente a localização dos usuários durante as tentativas de acesso. Essa prática ajuda a identificar comportamentos suspeitos, como acessos realizados de regiões inesperadas. Os desafios relacionados está em se manter aderente as legislações vigentes bem como o uso de rede virtual privada, em inglês, VPN. Infraestrutura robusta: Infraestrutura necessária para suportar as verificações em tempo real sem comprometer a performance ou a disponibilidade da plataforma.
- **Equipes de suporte capacitadas**: Profissionais qualificados para atender dúvidas e resolver problemas reportados pelos cidadãos, aspecto importante quando os usuários enfrentam dificuldades decorrentes de verificações adicionais, bloqueios ou falsos positivos.
- **Interpretar os alertas gerados**: Analisar os sinais de risco emitidos pelos indicadores, antecipando um potencial ataque orquestrado por robôs ou comportamentos suspeitos de regiões específicas.

Esse aspecto é especialmente relevante em um contexto como o gov.br, que atende milhões de usuários diariamente, tornando essencial a eficiência na triagem de possíveis falso positivos[1]. A literatura aponta que, embora o RBA seja eficaz, sua implementação pode ser prejudicada por limitações em termos de capacidade computacional e custos associados [64]. A implementação do RBA, como demonstrado por Ashibani (2019), é

[1]falso positivo ocorre quando o mecanismo de autenticação baseada em risco identifica um comportamento ou tentativa de acesso legítima como suspeita ou maliciosa, solicitando autenticações adicionais ou bloqueando o acesso indevidamente.

desafiadora devido à necessidade de realizar múltiplas verificações em tempo real, como a autenticação em duas etapas, a validação de dispositivos e a geolocalização. Essas verificações exigem um alto poder computacional e podem aumentar significativamente os custos com hardware e software.

Além disso, a latência introduzida por essas verificações pode impactar a experiência do usuário, comprometendo a usabilidade do sistema [64].

Outro problema identificado foi a necessidade de maior transparência e comunicação com os usuários sobre as intervenções realizadas pelo sistema, pois a falta de explicações claras sobre as razões de bloqueios ou solicitações de autenticação adicional pode gerar insatisfação ou confusão entre os usuários. Esse desafio pode ser mitigado por meio de campanhas educativas e interfaces mais intuitivas, que expliquem de forma acessível os mecanismos de segurança e como eles protegem os dados pessoais dos cidadãos, em consonância com as exigências da LGPD [2].

O uso de dados de geolocalização levanta preocupações éticas e regulatórias, especialmente em relação à conformidade com a LGPD [2]. O estudo reforça que, para maximizar os benefícios do RBA, é essencial garantir que os dados sejam tratados de maneira segura, anônima e proporcional aos riscos identificados.

4.4.5 Análise do Impacto do RBA na Plataforma ID gov.br

Analisando os dados relativos aos acessos diários, tem-se uma visão geral que indica 684.170.697 de logins nesse período com uma média diária de 9.122.276 logins dia, entre um mínimo de 3.158.069 e uma data de pico com 14.433.302 acessos. Referente a localização, temos um total de 9.900.200 acessos com o compartilhamento dessa informação tendo uma média de 132.003 acessos com localização por dia, variando de um mínimo de 8.476 e um máximo de 307.261 logins por dia. Os números relativos aos acessos a partir de dispositivos com vinculação são bem próximos dos números de logins com localização compartilhada tendo um total de 9.216.735 logins no período enquanto a média de logins dia foi de 122.890 e a variação dia foi de 7.993 a 287.188. Logins efetuados no mesmo estado do vinculado ao dispositivo somaram um total de 8.809.846, tendo uma média diária de 117.465 acessos e uma variação que vai de 7.766 a 374.557. Por fim, a visão de logins efetuados em estado diferente do vinculado ao dispositivo somaram um total de 406.889, tendo uma média diária de 5.425 acessos e uma variação entre 227 até 13.222. Uma visão consolidada desses números é apresentada na tabela 4.11:

Tabela 4.11: Consolidado de métricas de Login diário no período de validação do RBA

Métrica	Total Geral	Média	Mínimo	Máximo
Logins	684.170.697	9.122.276	3.158.069	14.433.302
com Localização	9.900.200	132.003	8.476	307.261
com Vinculação	9.216.735	122.890	7.993	287.188
Mesmo Estado	8.809.846	117.465	7.766	274.557
em Estado Diferente	406.889	5.425	227	13.322

Ao observar o total geral de logins, identifica-se que 95% ocorreram no estado vinculado ao dispositivo, enquanto apenas 0,05% correspondem a logins realizados em estados diferentes. Esse baixo percentual pode estar relacionado à possibilidade de que o 2FA e/ou a gestão de dispositivos estejam habilitados, o que impede a ativação do RBA neste contexto. Ademais, durante o período em que o mecanismo esteve em produção, o aplicativo exigia a informação da localidade. Por outro lado, nas autenticações realizadas por navegador, era solicitado acesso à localização do usuário; contudo, caso o usuário negasse a permissão, ele ainda podia prosseguir normalmente com a autenticação.

4.4.5.1 Tendências e Padrões Identificados

Os resultados fornecem evidências sobre a utilidade do RBA na mitigação de acessos suspeitos e no aumento da segurança da autenticação digital. A análise dos dados, em conexão com a fundamentação teórica apresentada na dissertação, demonstra como o RBA contribuiu para identificar e prevenir comportamentos não conformes, além de gerar *insights* sobre padrões de uso e vulnerabilidades regionais. Há uma conexão com os fluxos e os requisitos estabelecidos nesta dissertação uma vez que a plataforma conseguiu alinhar-se à necessidade de um sistema mais seguro e resiliente, conforme destacado no contexto da LGPD[2] e nos desafios apresentados na introdução do estudo.

A análise dos dados de login por estado identificou que dispositivos primariamente vinculados no estado de São Paulo, seguido de Minas Gerais e Santa Catarina são os estados que mais receberam logins de estados diferentes. Os achados mostram também que o Acre foi o estado que menos sofreu com os logins de estados diferentes, enquanto o estado de Mato Grosso do Sul não apresentou login no período. O gráfico a seguir apresenta um mapa de calor de logins que ocorreram fora do estado de origem do vínculo do dispositivo 4.5:

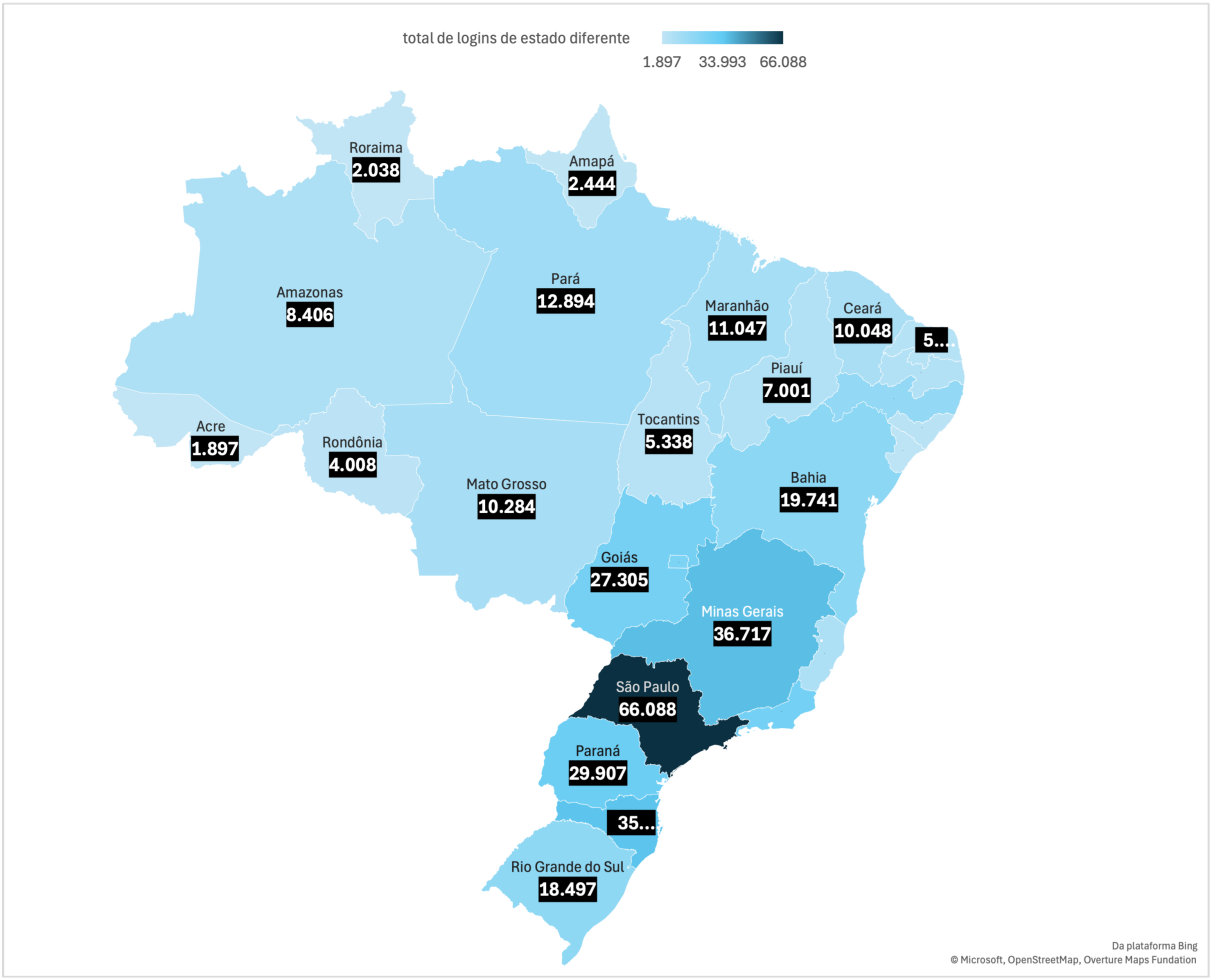

Figura 4.5: Mapa de Calor de Logins fora do estado do vínculo por Estado. Fonte: autor

Os dados diários evidenciam uma média consistente de logins realizados com sucesso e a frequência de autenticações adicionais acionadas pelo RBA. Por exemplo, no dia 1º/11/2024, dos 12.037.164 logins registrados, 265.782 (2,20%) forneceram a localização para monitoramento e detecção de comportamentos atípicos. Esse padrão foi semelhante nos dias anteriores, confirmando que o RBA está desempenhando um papel proativo na detecção de acessos. A taxa de logins com dispositivos vinculados manteve-se elevada, acima de 92% em todos os dias analisados.

Como uma amostra dos dados diários que foram analisados sob os padrões de logins e as intervenções do RBA, são apresentados os relatos em três datas específicas:

1. 1º/11/2024: Houve 12.037.164 logins, dos quais 265.782 (2,20%) permitiram acesso a localização geográfica para monitoramento. Entre estes, 246.469 (92,7%) foram com dispositivos vinculados, enquanto 12.017 (4,8%) ocorreram em estados diferentes do usual.

2. 31/10/2024: Dos 11.628.131 logins registrados, 292.213 (2,51%) permitiram acesso a localização geográfica para monitoramento, dos quais 270.163 (92,4%) envolveram dispositivos vinculados, e 13.322 (4,9%) foram realizados em estados diferentes.

3. 30/10/2024: Com 11.088.325 logins totais, 272.197 (2,45%) ativaram o RBA, com 252.542 (92,7%) realizados em dispositivos vinculados e 12.046 (4,7%) de estados distintos.

A tabela 4.12 demonstra a consistência das intervenções do RBA, em média 2,4% dos logins acionando validações adicionais diariamente. Percebe-se o elevado número de dispositivos vinculados entre as autenticações (acima de 92%). A frequência de logins em estados diferentes é baixa (aproximadamente 4,8%), mas importante para detectar possíveis tentativas de fraude.

Data	**Logins Totais**	**Verificação RBA (%)**	**Dispositivos Vinculados (%)**	**Logins Estados Diferentes (%)**
1º/11/2024	12.037.164	2,20	92,7	4,8
31/10/2024	11.628.131	2,51	92,4	4,9
30/10/2024	11.088.325	2,45	92,7	4,7

Tabela 4.12: Tabela de Logins e Métricas

Além disso, a análise regional para o dia 1º/11/2024, revelou dinâmicas interessantes sobre os padrões de acesso e possíveis vulnerabilidades. Os dados por estado mostraram que a maioria dos logins ocorreu entre dispositivos e localizações compatíveis, mas houve casos significativos de acessos realizados a partir de estados diferentes.

Data da Amostragem	**Estado**	**Total de Logins**	**Logins no Próprio Estado**	**Logins de Estados Diferentes**	**% de Logins Em Estados Diferentes**
30/09/2024	Distrito Federal	5.098	4.508	590	11,57%
16/10/2024	São Paulo	74.291	71.855	2.436	3,28%
1º/11/2024	Acre	948	920	28	2,95%

Tabela 4.13: Análise de Amostragem de Logins por Estado

A análise por Estado destaca três casos ilustrativos:

1. Distrito Federal (30/09/2024): Obteve um total de 5.098 logins, sendo 4.508 ocorrendo dentro do Distrito Federal e 590 logins foram realizados em Estados distintos da vinculação, destacando a relevância da localização como critério de risco.

2. São Paulo (16/10/2024): Com um total de 74.291 logins realizados, destes 71.855 no próprio Estado e 2.436 logins foram registrado em Estado diferente, indicando uma intervenção do RBA para autenticação adicional.

3. Acre (1º/11/2024): Totalizando 948 logins realizados, com 920 acessos dentro do Estado, tendo 28 acessos originados em Estados diferentes.

A análise dos dados diários e regionais demonstrou a aplicação do RBA na plataforma ID gov.br para lidar com desafios de segurança digital. O mecanismo demonstrou capacidade de identificar comportamentos atípicos, considerando a proteção dos dados e a conformidade com a LGPD [2]. As evidências apresentadas neste capítulo fornecem uma base inicial que servirá como insumo para decidir sobre a utilização desse mecanismo de aprimoramento da plataforma gov.br

Os dados por estado apresentam informações sobre o desempenho do RBA ao identificar padrões de login em diferentes regiões. No Estado de São Paulo, por exemplo, foi registrado um volume significativo de logins oriundos de estados distintos (2.436), indicando a capacidade do RBA de mapear situações que podem ser caracterizadas como atípicas. A análise apresentada na tabela 4.13 ilustra a correlação entre os estados de origem e destino, evidenciando o funcionamento da plataforma na identificação de comportamentos divergentes das expectativas.

Os dados analisados apontam que o mecanismo atuou na mitigação de riscos, preservando a usabilidade para os usuários. A baixa ocorrência de logins em estados diferentes do estado do vínculo pode estar associada à implementação no gov.br, que não exigiu informação sobre a localização do cidadão no momento do acesso. Adicionalmente, alternativas como o uso de 2FA ou a gestão de dispositivos com a flag de dispositivo autorizador configurada poderiam mitigar a aplicação do RBA em algumas situações. Mesmo assim, os dados observados apresentam a funcionalidade do mecanismo RBA.

Por fim, a aplicação do RBA no gov.br respondeu à questão de pesquisa QP.4 ao demonstrar que a solução é promissora na melhoria da segurança da identidade digital, reduzindo o número de acessos não autorizados e melhorando a confiabilidade geral da plataforma.

Os desafios identificados, embora significativos, são superáveis por meio de melhorias contínuas na infraestrutura, comunicação com usuários e governança de dados. Dessa forma, o RBA se mostra uma estratégia valiosa para plataformas digitais de alta criticidade, com potencial de ser aprimorado e replicado em outros contextos governamentais e privados.

Capítulo 5

Análise e Discussão dos Resultados

5.1 Discussões dos Resultados

Os achados obtidos na Fase 1 desta dissertação, derivados da condução Revisão Sistemática de Literatura (RSL), ressaltaram a identificação de fatores adicionais para autenticação de segurança. A análise envolveu 9 trabalhos primários selecionados, oferecendo um panorama das abordagens propostas na literatura acadêmica. Esses resultados fornecem uma base essencial para o aperfeiçoamento de sistemas de identidade digital, como a plataforma ID gov.br.

Durante a etapa inicial, percebeu-se a necessidade de ajustes nas strings de busca, a fim de garantir a abrangência e eficácia da pesquisa em diferentes bases de dados. Após esse refinamento, foram identificados 248 estudos preliminares, os quais passaram por critérios rigorosos de inclusão e exclusão. Esse processo culminou na seleção de 9 estudos de alta relevância, sendo 5 classificados como fontes primárias com base em uma avaliação criteriosa de qualidade. Apenas os trabalhos que atenderam aos critérios previamente estabelecidos foram analisados em maior profundidade, assegurando a relevância das conclusões.

Entre os fatores adicionais destacados, o One-Time Password (OTP) se mostrou o mais frequentemente empregado, muitas vezes em combinação com outros mecanismos. Contribuições inovadoras também se destacaram, como a autenticação baseada em riscos (RBA), os métodos *tripwire*, *rituals logins* e o modelo 2D-2FA, que acrescentam novas camadas de segurança aos sistemas. A abordagem RBA, por exemplo, demonstrou eficácia na detecção de comportamentos suspeitos, desencadeando etapas adicionais de autenticação. O modelo 2D-2FA apresentou melhorias significativas tanto em termos de usabilidade quanto de resistência a ataques, destacando-se como alternativa promissora frente a métodos mais tradicionais.

Os mecanismos *tripwire* e *rituals logins* propõem soluções baseadas na personalização, aumentando a dificuldade para possíveis invasores. No caso do *tripwire*, o usuário pode configurar armadilhas que ativam contramedidas de segurança em situações de acesso não autorizado. Já os *rituals logins* utilizam sequências de autenticação personalizadas que bloqueiam o acesso caso sejam executadas de maneira incorreta. Ambas as estratégias demonstraram resultados promissores, validando sua aplicabilidade prática.

No caso do OTP, algumas propostas exploraram sua integração com outras tecnologias, como o uso de *bluetooth* no mecanismo SecuriCast. Essa solução apresentou desempenho competitivo frente a ferramentas consolidadas, como o Google Authenticator, destacando o potencial do modelo *zero-touch* em reduzir a interação do usuário e simplificar o processo de autenticação. Por outro lado, a combinação de OTP com o algoritmo SHA1 revelou limitações críticas, indicando que essa abordagem não é ideal para cenários de alto risco.

Esses resultados evidenciam a relevância de explorar modelos de autenticação multifatorial, destacando a necessidade de soluções que aliem segurança e usabilidade sem infringir regulamentações como a LGPD. Os fatores identificados representam contribuições importantes para a evolução de sistemas como o ID gov.br, indicando caminhos para o desenvolvimento de estratégias mais robustas e amigáveis ao usuário. Esses avanços são fundamentais para alinhar os objetivos da dissertação à promoção de melhorias na segurança de sistemas de identidade digital.

Os resultados obtidos na Fase 2 focaram na análise dos fatores de segurança atualmente implementados na plataforma ID gov.br, com o objetivo de compará-los aos fatores adicionais identificados na literatura durante a RSL. Essa investigação revelou que a plataforma adota, como principais mecanismos de autenticação, a Biometria Facial e o OTP. Esses elementos desempenham papéis essenciais na criação e recuperação de uma ID gov.br, garantindo a segurança dos usuários em processos críticos.

A Biometria Facial está integrada ao processo de onboarding, utilizando bases de dados da ICN ou do Renach. Conforme a base utilizada para validação, o usuário recebe a classificação de ID Ouro ou ID Prata, respectivamente. Após a criação da identidade, é possível ativar o 2FA baseado no OTP, que solicita um código gerado para validar qualquer tentativa de login, tanto na versão web quanto no aplicativo da plataforma.

Quando comparados aos fatores apresentados na literatura, observa-se que a plataforma já utiliza o OTP, mas ainda não incorpora outros mecanismos inovadores identificados como promissores. Entre esses fatores adicionais, destacam-se o RBA, os métodos *tripwire* e *rituals logins*, além de combinações do OTP com *bluetooth* e o algoritmo SHA1. Essas abordagens apresentam potencial para aprimorar a segurança. O RBA, por exemplo, demonstra eficácia em detectar comportamentos anômalos, solicitando etapas adicionais de autenticação quando necessário. Já os mecanismos *tripwire* e *rituals lo-*

gins apostam na personalização, criando barreiras singulares que dificultam o acesso por intrusos.

A análise comparativa dos fatores implementados e os sugeridos pela literatura revela que as soluções propostas poderiam complementar os mecanismos já existentes. Combinações mais robustas, como OTP integrado ao *bluetooth*, apresentaram resultados positivos em estudos empíricos, sugerindo que poderiam ser adotadas para aprimorar a experiência de autenticação do usuário na plataforma. Por outro lado, a combinação de OTP com SHA1 demonstrou limitações significativas, indicando que não seria uma solução prática para contextos de alto risco.

Esses achados confirmam que os fatores adicionais identificados possuem o potencial de abordar lacunas no sistema atual, mas sua implementação exige análises detalhadas de aplicabilidade técnica, alinhamento com as políticas de segurança do gov.br e conformidade com normas como a LGPD. Os resultados da Fase 2 forneceram subsídios importantes para a avaliação de aplicabilidade que é realizada na Fase 3 do estudo, indicando caminhos promissores para o fortalecimento da segurança na plataforma ID gov.br.

Ainda na Fase 2 do estudo avaliou-se a viabilidade de incorporar fatores adicionais de segurança à plataforma ID gov.br, levando em conta a infraestrutura já existente, os desafios técnicos e as exigências legais. Os resultados indicaram que o RBA possui um grande potencial, especialmente em sistemas que contam com infraestrutura robusta para coletar e analisar dados comportamentais. Esse método possibilita identificar padrões de comportamento do usuário e acionar autenticações adicionais quando detectados acessos fora do padrão, fortalecendo a segurança. Contudo, sua aplicação no contexto do gov.br apresenta desafios relacionados à privacidade e ao cumprimento da LGPD, já que depende da coleta de dados como localização e informações de dispositivos, exigindo atenção cuidadosa para evitar conflitos com a legislação.

Fatores adicionais, como aqueles baseados no conceito de *tripwire* e *ritual logins*, destacaram-se por sua abordagem inovadora, centrada no conhecimento exclusivo do usuário. Essas técnicas envolvem a configuração de sequências ou armadilhas específicas que podem ser redefinidas periodicamente, adicionando uma barreira importante contra ataques. Além de aumentar a segurança do sistema, essa estratégia promove o engajamento ativo do usuário na proteção de sua identidade digital.

Por outro lado, a combinação de OTP com o algoritmo SHA1, de acordo com o artigo, apresentou desempenho insatisfatório, inviabilizando seu uso como alternativa para melhorar a ID gov.br. Em contrapartida, a integração do OTP com tecnologias baseadas em *bluetooth*, como os modelos *zero-touch* e *notify*, revelou-se uma solução promissora, oferecendo uma experiência de autenticação mais prática e segura. Entretanto, implementar essa tecnologia em escala nacional exigirá uma análise detalhada sobre questões logísticas

e regulatórias que não foram passíveis de execução nesse momento.

Os resultados do estudo apontam para uma tendência de adoção de um modelo aprimorado de MFA, expandindo as funcionalidades do sistema atual, que já utiliza OTP como solução básica. As propostas levantadas pela revisão sistemática sugerem que a diversificação de fatores adicionais e a integração de tecnologias complementares podem melhorar significativamente a segurança e a experiência do usuário. Assim, conclui-se que essas abordagens têm o potencial de elevar os níveis de segurança e confiabilidade da plataforma, desde que estejam alinhadas aos requisitos legais e técnicos.

A Fase 4 concentrou-se na análise das evidências coletadas após a implementação do RBA, considerando aspectos quantitativos e qualitativos. Os dados confirmam que o mecanismo trouxe melhorias para a segurança da plataforma, reduzindo riscos sem afetar a experiência do usuário.

A autenticação baseada em risco atuou na detecção de possíveis acessos fraudulentos sem gerar um aumento significativo de bloqueios indevidos, evidenciando a eficácia do modelo. A literatura destaca que mecanismos que utilizam georreferenciamento combinado com análise comportamental oferecem níveis mais altos de segurança [63].

Os resultados apresentados demonstram que o RBA pode ser uma importante mecanismo sob a perspectiva de duplo fator de autenticação baseado em comportamento, conforme o papel descrito na fundamentação teórica desta dissertação ao oferecer uma abordagem para autenticação digital. O alinhamento entre os dados e os fluxos previstos apresentam que o mecanismo mitigou riscos sem prejudicar a usabilidade. A baixa frequência de logins suspeitos pode estar relacionada à forma como o RBA foi implementado. Isso ocorre porque não foi exigido que o cidadão informasse sua localidade no momento do acesso. Além disso, caso o usuário tivesse o 2FA habilitado ou utilizasse a gestão de dispositivos com a *flag* de dispositivo autorizador ativada, essas opções permitiriam contornar a aplicação do RBA, entretanto na amostragem verificada demonstra a eficácia da análise comportamental. Ademais, a capacidade do RBA de incorporar fatores de risco geográficos e de dispositivos configura um modelo robusto para autenticação em plataformas digitais críticas, como o ID gov.br, corroborando estudos que destacam o potencial do RBA para aumentar a segurança digital [49, 63].

De acordo com os relatórios, logins suspeitos de localizações distintas do Estado que houve a vinculação representaram menos de 5% do total de acessos, um percentual modesto mas significativo para a proteção contra possíveis fraudes. O uso do RBA, que avalia riscos em tempo real, torna possível respostas mais eficientes a eventos incomuns, como o aumento de tentativas de acesso em regiões específicas. Esses benefícios foram previstos na dissertação, que destacou a importância da coleta de dados georreferenciados para identificar padrões atípicos, como demonstrado pelos resultados.

A análise dos dados diários e regionais demonstrou reforçar a aplicação do RBA na plataforma ID gov.br para lidar com desafios de segurança digital. O mecanismo demonstrou capacidade de identificar e prevenir comportamentos atípicos, assegurando a proteção dos dados e a conformidade com a LGPD [2]. As evidências apresentadas neste capítulo fornecem uma base inicial que servirá como insumo para decidir sobre a utilização desse mecanismo de aprimoramento do sistema, consolidando o RBA como uma estratégia efetiva.

A elevada taxa de logins feitos com dispositivos vinculados reforça a eficácia da análise. A pesquisa demonstra que o RBA tem potencial para contribuir com a melhoria do processo de autenticação da plataforma, aperfeiçoando o fluxo de autenticação e reduzindo os riscos de acessos não autorizados. Esses resultados são consistentes com a literatura recente sobre segurança digital e autenticidade, consolidando o RBA como uma solução prática e confiável para plataformas de alta criticidade, como o ID gov.br.

Por fim, no terceiro arquivo [44], a análise comparativa pelos tipos de recuperação de contas revela as seguintes variações entre os períodos anterior ao RBA (06/07/2024 a 18/08/2024) e com o RBA ativo (19/08/2024 a 01/11/2024):

1. Recuperação via E-mail

- **Média diária antes do RBA:** 80.544 recuperações.
- **Média diária com o RBA:** 77.795 recuperações.
- **Variação percentual: -3,41%**.
- Houve uma ligeira redução no uso deste método durante o período em que o RBA esteve ativo.

2. Recuperação via SMS

- **Média diária antes do RBA:** 20.703 recuperações.
- **Média diária com o RBA:** 22.619 recuperações.
- **Variação percentual: +9,25%**.
- Esse aumento pode indicar maior dependência do SMS para recuperação de contas durante o período de análise.

3. Recuperação por Biometria CNH

- **Média diária antes do RBA:** 6.673 recuperações.
- **Média diária com o RBA:** 6.909 recuperações.
- **Variação percentual: +3,54%**.

- Pequeno aumento no uso dessa modalidade, que pode estar relacionado ao fortalecimento de mecanismos mais seguros.

4. Recuperação por Biometria ICN

- **Média diária antes do RBA:** 53.810 recuperações.
- **Média diária com o RBA:** 67.374 recuperações.
- **Variação percentual: +25,21%**.
- Essa foi a modalidade com o maior crescimento percentual, possivelmente associada à eficácia desse método como alternativa segura.

5. Recuperação via Bancos

- **Média diária antes do RBA:** 54.145 recuperações.
- **Média diária com o RBA:** 61.480 recuperações.
- **Variação percentual: +13,55%**.
- O aumento sugere maior utilização de instituições bancárias para validação de identidade no período analisado.

Os resultados indicam que, durante o período de ativação do RBA, houve um aumento considerável no uso de métodos considerados mais seguros, como **biometria ICN** (+25,21%) e **recuperação via bancos** (+13,55%), enquanto métodos tradicionais, como **recuperação por e-mail**, apresentaram uma redução discreta (-3,41%).

Essas tendências podem refletir a influência do RBA no fortalecimento da segurança e na mudança de comportamento dos usuários, priorizando métodos mais robustos de autenticação. Contudo, o aumento geral nos números de recuperação de contas sugere que a complexidade adicional introduzida pelo RBA pode ter elevado as dificuldades de acesso, ampliando a necessidade de recuperações.

O presente estudo evidenciou avanços significativos na compreensão e na aplicação de fatores adicionais de segurança na plataforma ID gov.br, especialmente com a introdução do RBA como método de autenticação. No entanto, os resultados foram impactados pela decisão de adaptar a implementação original do RBA, especificamente ao excluir a gestão de dispositivos como variável de controle em situações de mudança de dispositivo no contexto do RBA. Essa alteração diminuiu a robustez do mecanismo, pois deixou de considerar uma camada adicional de segurança que, conforme identificado na literatura, é essencial para detectar padrões de acesso atípicos e garantir maior confiabilidade no processo de autenticação. A gestão de dispositivos permite associar a identidade digital

a um conjunto confiável de equipamentos previamente autorizados, reduzindo significativamente o risco de acessos não autorizados. Sua exclusão fragilizou a total eficácia do mecanismo ao permitir que mudanças de dispositivo não fossem tratadas no ambiente do RBA em *background*, limitando, assim, a capacidade do RBA de atender plenamente às expectativas de mitigação de tentativas de acessos.

5.2 Limitações do Estudo

As limitações desta pesquisa estão intrinsecamente relacionadas aos desafios metodológicos da condução de Revisões Sistemáticas de Literatura (RSL) e às características do Estudo de Caso aplicado.

O processo de pesquisa foi realizado apenas por um autor, o que pode ocasionar inconsistências e equívocos de interpretação pela ausência de um segundo ou terceiro autor para contribuir e realizar comparativos entre as execuções. Nesse sentido para minimizar essa limitação foi considerada a revisão pelo professor orientador deste trabalho.

Outra limitação está relacionada ao tema de identidade digital, que ainda é incipiente na literatura científica. Essa lacuna contribuiu para a identificação de um número limitado de estudos primários relevantes para a RSL, especialmente no que se refere à interseção entre identidade digital e fatores adicionais de segurança. Para contornar essa limitação, a *string* de busca foi adaptada e validada conforme os critérios de cada base de dados, conforme apresentada na tabela 4.1 na Seção de Resultados.4

Adicionalmente, como limitação o fato de ser a primeira condução de uma RSL por parte do pesquisador, possibilitando margem para interpretações passíveis de revisão, o que foi mitigado com a repetição da execução do protocolo de RSL para garantia dos resultados e avaliação por parte do professor orientador deste trabalho. No contexto do estudo de caso, que avaliou a aplicação do RBA na plataforma gov.br, a análise foi limitada pela impossibilidade de exigir que todos os acessos incluíssem informações de localidade, uma vez que essa ação é opcional ao cidadão. No âmbito da segurança da informação, usuários com intenções maliciosas poderiam deliberadamente evitar o uso de tais mecanismos. Ademais, caso o cidadão já tivesse ativado o segundo fator de autenticação (2FA) e configurado a gestão de dispositivos, a aplicação do RBA se tornaria redundante, incluindo uma camada adicional que poderia impactar negativamente na experiência do usuário.

Por fim, destaca-se que o RBA não foi implementado considerando as duas variáveis de controle (mudança de localidade e mudança de dispositivo). Essa restrição, limitou a análise e os resultados obtidos, restringindo as conclusões.

As limitações listadas reforçam a necessidade de abordagens metodológicas mais robustas e de um escopo ampliado para futuras pesquisas, permitindo maior refinamento nos resultados e maior aplicabilidade prática.

5.3 Contribuições Acadêmicas

Como resultado desta pesquisa, apresenta-se uma análise detalhada sobre a aplicação do (RBA) no contexto da identidade digital gov.br, destacando sua eficácia, benefícios e desafios no aumento da segurança e confiabilidade do sistema. Este estudo culminou na formulação de uma abordagem prática e teórica para a autenticação baseada em riscos, aplicada em uma plataforma de grande escala e alta criticidade. A análise dos resultados oferece um modelo robusto que pode ser utilizado tanto para avaliação quanto para o desenvolvimento de sistemas digitais que necessitam de autenticação segura.

Entre as principais contribuições acadêmicas do estudo, destaca-se a geração de conhecimento empírico sobre o uso do RBA em sistemas de identidade digital. Este trabalho amplia a literatura existente ao fornecer dados reais e análises detalhadas de sua aplicação em um ambiente de alta demanda e regido por regulamentações como a LGPD. A pesquisa evidencia como a integração de fatores comportamentais e geográficos à autenticação pode mitigar riscos, enquanto mantém a experiência do usuário consistente.

Dessa forma, os achados podem servir como base para futuras investigações acadêmicas relacionadas à segurança digital, autenticação e governança de dados.

5.4 Contribuições Profissionais

Profissionalmente, o estudo apresenta contribuições práticas que podem ser imediatamente aplicadas em cenários similares. A pesquisa resultou em diretrizes operacionais baseadas nos resultados empíricos obtidos, oferecendo *insights* valiosos para equipes técnicas e gestores de sistemas. Essas diretrizes incluem a priorização de investimentos em infraestrutura tecnológica para suportar soluções voltadas para a segurança da informação e análise comportamental, além de estratégias para melhorar a comunicação com usuários sobre intervenções realizadas, promovendo maior transparência e aceitação do sistema. O RBA demonstrou ser uma ferramenta viável e em conformidade com a LGPD, possibilitando um equilíbrio entre segurança, privacidade e usabilidade.

Este modelo pode ser replicado e adaptado por outras instituições que necessitem implementar soluções de autenticação em larga escala. Assim, a pesquisa não apenas contribui para o avanço das contribuições da literatura no âmbito de fatores adicionais

e identificação digital, mas também oferece um conjunto de práticas recomendadas que podem ser adotadas por profissionais de TIC e gestores de segurança da informação.

Por fim, as contribuições deste trabalho reforçam a importância de adotar mecanismos de autenticação que alinhem inovação tecnológica e conformidade. O RBA, como demonstrado neste estudo, é um exemplo prático de como a tecnologia pode ser utilizada para atender às demandas de segurança e privacidade em ambientes digitais críticos.

5.5 Conclusão

Nesse trabalho, foi conduzida uma revisão sistemática de literatura, que identificou 248 trabalhos preliminares e após aplicar os critérios de inclusão e exclusão, resultou na seleção de 9 estudos primários para extração dos dados. A partir de uma RSL, foram identificados fatores adicionais de segurança com potencial de aplicabilidade no contexto da plataforma gov.br, incluindo autenticação baseada em riscos (RBA), OTP (One-Time Password), e mecanismos como Tripwire e Login Rituals.

A implementação piloto do RBA apresentou resultados promissores na identificação de comportamentos atípicos, apenas em mudanças de localização, uma vez que a mudança de dispositivo não foi implementada.

O mecanismo demonstrou a capacidade de suportar a plataforma na detecção e bloqueio acessos não autorizados. Além disso, a análise quantitativa indicou que aproximadamente 10 milhões de logins permitiram utilização do georreferenciamento no objeto desta pesquisa.

A presente dissertação demonstrou que o RBA tem a capacidade de contribuir para a plataforma gov.br, especialmente no que tange à identificação e autenticação de usuários. A crescente digitalização dos serviços públicos, acompanhada de regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD), trouxe à tona desafios substanciais no que diz respeito à proteção das identidades digitais de milhões de cidadãos brasileiros.

Os resultados desta dissertação fornecem evidências da aplicabilidade do RBA no contexto das identidades digitais no Brasil. A aplicação de fatores adicionais de autenticação, embora desafiadora, mostrou-se viável e eficiente, reforçando a importância de estratégias proativas para mitigar riscos associados a crimes cibernéticos, como roubo de identidade e fraudes financeiras. Nesse sentido, este trabalho contribui para a evolução tecnológica da plataforma gov.br, e visa desempenhar um papel relevante no fortalecimento da confiança pública em serviços digitais governamentais.

5.5.1 Trabalhos Futuros

O cenário observado reforça a importância de explorar, em pesquisas futuras, o impacto de diferentes configurações do RBA no fortalecimento da segurança de identidades digitais. Recomenda-se a reintrodução da gestão de dispositivos como uma variável de controle fundamental, avaliando sua eficácia em combinação com outros fatores adicionais de segurança. Sugere-se que o RBA atue como um mecanismo passivo, isto é, em segundo plano como um agente para os casos em que o cidadão não tenha optado por habilitar o 2FA. Nesse sentido, é imprescindível avançar nos normativos para que os acessos à plataforma gov.br passem a exigir o compartilhamento o compartilhamento da localização.

Esta pesquisa também identificou desafios técnicos e operacionais que devem ser abordados em futuros trabalhos. A complexidade de implementação de múltiplos fatores de autenticação, como o RBA, demanda não apenas maior capacidade computacional, mas também uma abordagem equilibrada para assegurar que os mecanismos de segurança não impactem negativamente a experiência do usuário.

Com advento de novas tecnologias, em específico, a inteligência artificial, uma abordagem validando comportamentos, como tempo para clicar, movimentação de mouse ou pressão de teclado podem ser úteis para uma nova abordagem, contribuindo para a evolução contínua das estratégias de autenticação digital.

Referências

[1] Group, World Bank: *Id4d practitioner's guide*, 2019. https://id4d.worldbank.org/guide, Acessado em 25 de outubro de 2021. xi, 6, 7, 8

[2] Brasil: *Lei nº 13.709/2018, lei geral de proteção de dados pessoais (lgpd)*, 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. 1, 65, 66, 69, 74

[3] Executivo, Poder: *Decreto nº 9.745/2019*, 2020. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9745.htm#art13, Acessado em: 2020-10-25. 1

[4] Executivo, Poder: *Decreto nº 10.332/2020*, 2020. https://www.in.gov.br/en/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358, Accessed in: 2020-10-20. 1

[5] Kitchenham, Barbara, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey e Stephen Linkman: *Systematic literature reviews in software engineering - a systematic literature review*. Information and Software Technology, 51:7–15, janeiro 2009, ISSN 09505849. 2, 16, 17

[6] ANPD: *ANPD está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas*. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas, acesso em 2021-10-15. 3

[7] EBC: *Procon de sp notifica empresas de telefonia sobre vazamentos de dados*, 2021. https://agenciabrasil.ebc.com.br/justica/noticia/2021-02/procon-de-sp-notifica-empresas-de-telefonia-sobre-vazamentos-de-dados>. 3

[8] Kalloniatis, Christos: *Incorporating privacy in the design of cloud-based systems: a conceptual meta-model*. Inf. Comput. Secur., 25(5):614–633, 2017. https://doi.org/10.1108/ICS-06-2016-0044. 3

[9] Canedo, Edna Dias, Angélica Toffano Seidel Calazans, Eloisa Toffano Seidel Masson, Pedro Henrique Teixeira Costa e Fernanda Lima: *Perceptions of ICT practitioners regarding software privacy*. Entropy, 22(4):429, 2020. https://doi.org/10.3390/e22040429. 3

[10] MENEGAZZI, Diego: *Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução*. feb 2021. https://repositorio.ufpe.br/handle/123456789/40280. 3

[11] Alves, Carina e Moisés Neves: *Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso*. Em Cruz, Maria Lencastre Pinheiro de Menezes (UPE, Brasil), Argentina) Hadad, Graciela Dora Susana (UNO e Brasil) Marques, Johnny Cardoso (ITA (editores): *Anais do WER21 - Workshop em Engenharia de Requisitos*, Brasília, DF, 2021. Editora PUC-Rio. 3

[12] EBC: *Sites e aplicativo do ministério da saúde sofrem ataque cibernético*, 2021. https://agenciabrasil.ebc.com.br/saude/noticia/2021-12/sites-e-aplicativo-do-ministerio-da-saude-sofrem-ataque-cibernetico. 3

[13] Ford, Matthew: *Identity authentication and 'e-commerce'.* Journal of Information, Law and Technology, 1998, janeiro 1998. 6, 7

[14] Halonen, Teppo: *Authentication and authorization in mobile environment*. Em *Tik-110.501 Seminar on Network Security*. Citeseer, 2000. 6

[15] Dressel, T, E List e F Echtler: *SecuriCast: Zero-touch two-factor authentication using WebBluetooth*. Em *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems, EICS 2019*, 2019. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072378602&doi=10.1145%2F3319499.3328225&partnerID=40&md5=2fa988bb5621e6c49cba029779bef22c. 6, 32, 36

[16] Standards, National Institute of e Technology: *Digital Identity Guidelines: NIST SP 63b*. CreateSpace Independent Publishing Platform, North Charleston, SC, USA, 2017, ISBN 154839954X. 7

[17] Geteloma, V, C K Ayo e R N Goddy-Wurlu: *A Proposed Unified Digital Id Framework for Access to Electronic Government Services*. Em *Journal of Physics: Conference Series*, volume 1378, 2019. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077780963&doi=10.1088%2F1742-6596%2F1378%2F4%2F042039&partnerID=40&md5=8be00fdb70860c5d0d2ecbe8f4a47fa9. 7, 32

[18] Executivo, Poder: *Landing page gov.br*, 2021. https://www.gov.br/governodigital/pt-br/conta-gov-br, Acessado em: 2020-10-25. 8

[19] Shirvanian, M e S Agrawal: *2D-2FA: A New Dimension in Two-Factor Authentication*. Em *ACM International Conference Proceeding Series*, páginas 482–496, 2021. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121611728&doi=10.1145%2F3485832.3485910&partnerID=40&md5=fbf98f25b5d2b9aa018b9ce284dec3ad. 10, 23, 33, 35

[20] Stanislav, Mark: *Two-factor authentication*, volume 4. IT Governance Ltd, 2015. 10

[21] Aloul, Fadi, Syed Zahidi e Wassim El-Hajj: *Two factor authentication using mobile phones*. Em *2009 IEEE/ACS International Conference on Computer Systems and Applications*, páginas 641–644, 2009. 10

[22] Geteloma, Victor, Charles Ayo e Rowland Goddy-Worlu: *A proposed unified digital id framework for access to electronic government services*. Journal of Physics: Conference Series, 1378:042039, dezembro 2019. 10

[23] Camp, L.: *Digital identity.* Technology and Society Magazine, IEEE, 23:34 – 41, fevereiro 2004. 10

[24] Odun-Ayo, Isaac, Olasupo Ajayi e Sanjay Misra: *Cloud computing security - issues and development.* julho 2018. 10

[25] KOSE, Busra OZDENIZCI, Onur BUK, Haci Ali MANTAR e Vedat COSKUN: *TrustedID: An Identity Management System based on OpenID Connect Protocol.* Em *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, páginas 1–6, oct 2020. 11, 33

[26] Konoth, Radhesh Krishnan, Björn Fischer, Wan Fokkink, Elias Athanasopoulos, Kaveh Razavi e Herbert Bos: *Securepay: Strengthening two-factor authentication for arbitrary transactions.* Em *2020 IEEE European Symposium on Security and Privacy (EuroS P)*, páginas 569–586, 2020. 11

[27] Yin, Robert K.: *Estudo de Caso: Planejamento e Métodos.* Bookman, Porto Alegre, 5ª edição, 2015. 13, 16, 21, 22, 23, 24, 26, 27, 60, 61, 62, 63

[28] Richardson, R. J.: *Metodologia do trabalho científico.* Atlas, 6ª edição, 2017. 14

[29] Gil, Antonio Carlos: *Métodos e técnicas de pesquisa social.* Atlas, São Paulo, 2008. 14

[30] Meltzoff, J.: *Critical Thinking about Research: Psychology and Related Fields.* Critical Thinking about Research: Psychology and Related Fields. American Psychological Association, 1998, ISBN 9781557984555. `https://books.google.com.br/books?id=1wxLcAAACAAJ`. 15

[31] Creswell, J.W.: *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE Publications, 2014, ISBN 9781452226095. `https://books.google.com.br/books?id=PViMtOnJ1LcC`. 15

[32] Kitchenham, Barbara e Stuart Charters: *Guidelines for performing Systematic Literature Reviews in Software Engineering.* julho 2007. 17

[33] Freitas, Vitor: *Parsifal.* `https://parsif.al/`, acesso em 2021-10-17. 17

[34] Brereton, Pearl, Barbara A. Kitchenham, David Budgen, Mark Turner e Mohamed Khalil: *Lessons from applying the systematic literature review process within the software engineering domain.* Journal of Systems and Software, 80(4):571–583, 2007, ISSN 0164-1212. `https://www.sciencedirect.com/science/article/pii/S0164121206001970X`, Software Performance. 17

[35] Branski, Regina, Raul Arellano, Caldeira Franco e Orlando Lima Jr: *Metodologia de estudo de casos aplicada À logÍstica.* janeiro 2010. 20

[36] Yin, Robert K.: *Case Study Research and Applications: Design and Methods.* Sage Publications, Thousand Oaks, CA, 2018. 20

[37] Stake, Robert E.: *The Art of Case Study Research*. Sage Publications, Thousand Oaks, CA, April 1995. 20, 21

[38] Stake, Robert E.: *Multiple Case Study Analysis*. Guilford Press, New York, NY, 2006. 20

[39] Creswell, John W.: *Qualitative Inquiry & Research Design: Choosing Among Five Approaches*. Sage Publications, Thousand Oaks, CA, 2nd edição, 2007. 21

[40] Yin, R.K. e D.T. Campbell: *Case Study Research: Design and Methods*. Applied Social Research Methods. SAGE Publications, 1984, ISBN 9780803920576. https://books.google.com.br/books?id=bA1HAAAAMAAJ. 21

[41] Yin, R.K.: *Case Study Research and Applications: Design and Methods*. SAGE Publications, 2017, ISBN 9781506336183. https://books.google.com.br/books?id=6DwmDwAAQBAJ. 21

[42] govbr: *Arquivos analisados gov. br*, janeiro 2025. https://docs.google.com/spreadsheets/d/1-F83l_2y-l5EKUseWXyvhzrxIuBqQBce/edit?usp=sharing&ouid=113060917238752453472&rtpof=true&sd=true, último acesso 05 de fevereiro de 2024. 24, 43, 63

[43] govbr: *Arquivos analisados gov. br*, janeiro 2025. https://docs.google.com/spreadsheets/d/1qKqBuOkDLf1QSefqsM3icVNhy9r72L_1/edit?usp=drive_link&ouid=113060917238752453472&rtpof=true&sd=true, último acesso 05 de fevereiro de 2024. 24, 45

[44] govbr: *Arquivos analisados gov. br*, janeiro 2025. https://docs.google.com/spreadsheets/d/1ZRQFwwG2xB120xVx0NRHgxLC4Cy3mFgq/edit?usp=drive_link&ouid=113060917238752453472&rtpof=true&sd=true, último acesso 05 de fevereiro de 2024. 24, 74

[45] Seta, H, T Wati e I C Kusuma: *Implement Time Based One Time Password and Secure Hash Algorithm 1 for Security of Website Login Authentication*. Em *Proceedings - 1st International Conference on Informatics, Multimedia, Cyber and Information System, ICIMCIS 2019*, páginas 115–120, 2019. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081096828&doi=10.1109%2FICIMCIS48181.2019.8985196&partnerID=40&md5=84e21d881c841c5579ed3a5e07fc82de. 32, 37, 39

[46] Kumar, S, S A A Jafri, N Nigam, N Gupta, G Gupta e S K Singh: *A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing*. Em *IOP Conference Series: Materials Science and Engineering*, volume 748, 2020. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85080960721&doi=10.1088%2F1757-899X%2F748%2F1%2F012026&partnerID=40&md5=aa826c37857018326d2ca8b619af4b7b. 32

[47] Barron, T, J So e N Nikiforakis: *Click This, Not That: Extending Web Authentication with Deception*. Em *ASIA CCS 2021 - Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, páginas 462–474, 2021. https://www.

scopus.com/inward/record.uri?eid=2-s2.0-85108076310&doi=10.1145%2F3433210.3453088&partnerID=40&md5=fe740fa2aec9163fe3bf791ef314a5ca. 33, 36

[48] Bruzgiene, R e K Jurgilas: *Securing remote access to information systems of critical infrastructure using two-factor authentication*. Electronics (Switzerland), 10(15), 2021. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85111326924&doi=10.3390%2Felectronics10151819&partnerID=40&md5=9b1ee7f88c86606e856a751087e20c0f. 33

[49] Wiefling, S., M. Dürmuth e L. Lo Iacono: *"more than just good passwords? a study on usability and security perceptions of risk-based authentication,"*. Annual Computer Security Applications Conference, páginas 203–218, 2020. 33, 35, 63, 64, 73

[50] Sharma, Abhishek e Rakesh Jha: *Secure proximity-based otp authentication using bluetooth le*. International Journal of Computer Applications, 175(2):18–25, 2020. 39, 40, 41, 42

[51] Peterson, John e Alice Smith: *Security and usability of tripwire authentication methods*. Journal of Cybersecurity Research, 5(2):112–125, 2017. 39, 41, 42

[52] Karapanos, Nikolaos, Eiji Hayashi e Saurabh Panjwani: *User-centric approaches to secure authentication rituals*. Proceedings of the ACM Conference on Human Factors in Computing Systems, páginas 1235–1244, 2015. 39, 41, 42

[53] Garfinkel, Simson e Gene Spafford: *Design and Implementation of Secure Authentication Systems*. O'Reilly Media, 2005, ISBN 978-0-596-00887-4. 40, 41

[54] Bonneau, Joseph, Cormac Herley e Paul van Oorschot: *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes*. IEEE Symposium on Security and Privacy, páginas 553–567, 2012. 40, 41, 42

[55] Murdoch, Steven: *Security challenges in user-defined authentication mechanisms*. ACM Transactions on Privacy and Security, 22(3):1–18, 2019. 40, 41

[56] Cabrera, John e Edward Dawson: *Context-aware risk-based authentication: A review*. Computers & Security, 102:102131, 2021. 40, 41, 42

[57] Ashibani, Mustafa e Qusay Mahmoud: *Risk-based authentication using machine learning for online services*. IEEE Access, 7:106087–106099, 2019. 41

[58] Yang, Huan e Mary Tate: *A descriptive literature review and classification of cloud computing research*. Communications of the Association for Information Systems, 31:35–60, 2012. https://aisel.aisnet.org/cais/vol31/iss1/2/. 51

[59] Zissis, Dimitrios e Dimitrios Lekkas: *Addressing cloud computing security issues*. Future Generation Computer Systems, 28(3):583–592, 2012. 51

[60] Yang, Ke e Jian Hsieh: *Governance and accountability in public sector it projects: The case of e-government in practice*. Government Information Quarterly, 36(2):312–320, 2019. 51

[61] Heeks, Richard: *Implementing and Managing eGovernment: An International Text*. SAGE Publications, 2006, ISBN 978-0-7619-4311-6. 51

[62] Furtado, Sandro e George Corrêa: *Identification and applicability of additional security factors on the gov.br digital identity platform*, 2022. `https://www.tecsi.org/contecsi/index.php/contecsi/19CONTECSI/paper/view/7034/4625`. 62

[63] Ford, William: *Authentication and Security for the Digital Age*. Springer, 2019, ISBN 9783030123456. 64, 73

[64] Ashibani, Yosef e Mahmoud Mahmoud: *Challenges and opportunities in implementing risk-based authentication for modern digital systems*. Journal of Information Security and Applications, 45:67–78, 2019. 64, 65

Anexo I

Anexo II - Amostragem do Relatório de Acessos por Estados

Data	Estado do Dispositivo	Estado no Aplicativo	Total Mesmo Estado	Total Estado Diferente	Total com Localização
19/08/2024	Acre	Acre	55	0	55
19/08/2024	Alagoas	Alagoas	139	0	139
19/08/2024	Amapá	Amapá	64	0	64
19/08/2024	Amazonas	Amazonas	279	0	279
19/08/2024	Amazonas	Pernambuco	0	1	1
19/08/2024	Amazonas	São Paulo	0	1	1
19/08/2024	Bahia	Alagoas	0	2	2
19/08/2024	Bahia	Bahia	749	0	749
19/08/2024	Bahia	Ceará	0	1	1
19/08/2024	Bahia	Goiás	0	4	4
19/08/2024	Bahia	Minas Gerais	0	1	1
19/08/2024	Bahia	Rio de Janeiro	0	1	1
19/08/2024	Bahia	Santa Catarina	0	1	1
19/08/2024	Bahia	São Paulo	0	5	5
19/08/2024	Ceará	Ceará	446	0	446
19/08/2024	Ceará	Maranhão	0	2	2
19/08/2024	Ceará	Pará	0	2	2
19/08/2024	Ceará	Piauí	0	3	3

Data	Estado do Dispositivo	Estado no Aplicativo	Total Mesmo Estado	Total Estado Diferente	Total com Localização
19/08/2024	Ceará	São Paulo	0	1	1
19/08/2024	Distrito Federal	Acre	0	1	1
19/08/2024	Distrito Federal	Distrito Federal	371	0	371
19/08/2024	Distrito Federal	Goiás	0	5	5
19/08/2024	Distrito Federal	Mato Grosso	0	2	2
19/08/2024	Distrito Federal	Pernambuco	0	1	1
19/08/2024	Distrito Federal	Piauí	0	2	2
19/08/2024	Distrito Federal	Roraima	0	1	1
19/08/2024	Distrito Federal	Santa Catarina	0	1	1
19/08/2024	Distrito Federal	São Paulo	0	1	1
19/08/2024	Espírito Santo	Bahia	0	3	3
19/08/2024	Espírito Santo	Espírito Santo	228	0	228
19/08/2024	Espírito Santo	Paraná	0	1	1
19/08/2024	Espírito Santo	Pernambuco	0	1	1
19/08/2024	Goiás	Amapá	0	1	1
19/08/2024	Goiás	Bahia	0	1	1
19/08/2024	Goiás	Distrito Federal	0	9	9
19/08/2024	Goiás	Goiás	608	0	608
19/08/2024	Goiás	Maranhão	0	3	3
19/08/2024	Goiás	Pará	0	1	1
19/08/2024	Goiás	São Paulo	0	1	1
19/08/2024	Goiás	Tocantins	0	3	3
19/08/2024	Maranhão	Goiás	0	1	1
19/08/2024	Maranhão	Maranhão	282	0	282
19/08/2024	Maranhão	Piauí	0	1	1
19/08/2024	Maranhão	Rio Grande do Norte	0	1	1
19/08/2024	Maranhão	São Paulo	0	2	2
19/08/2024	Maranhão	Tocantins	0	1	1
19/08/2024	Mato Grosso	Acre	0	1	1
19/08/2024	Mato Grosso	Distrito Federal	0	1	1
19/08/2024	Mato Grosso	Mato Grosso	278	0	278
19/08/2024	Mato Grosso	São Paulo	0	1	1

Data	Estado do Dispositivo	Estado no Aplicativo	Total Mesmo Estado	Total Estado Diferente	Total com Localização
19/08/2024	Minas Gerais	Bahia	0	3	3
19/08/2024	Minas Gerais	Distrito Federal	0	3	3
19/08/2024	Minas Gerais	Goiás	0	4	4
19/08/2024	Minas Gerais	Minas Gerais	1264	0	1264
19/08/2024	Minas Gerais	Pará	0	1	1
19/08/2024	Minas Gerais	Pernambuco	0	1	1
19/08/2024	Minas Gerais	Rio de Janeiro	0	2	2
19/08/2024	Minas Gerais	São Paulo	0	14	14
19/08/2024	Minas Gerais	Sergipe	0	1	1
19/08/2024	Pará	Distrito Federal	0	1	1
19/08/2024	Pará	Espírito Santo	0	1	1
19/08/2024	Pará	Maranhão	0	3	3
19/08/2024	Pará	Pará	469	0	469
19/08/2024	Pará	São Paulo	0	5	5
19/08/2024	Paraíba	Paraíba	153	0	153
19/08/2024	Paraíba	São Paulo	0	1	1
19/08/2024	Paraná	Minas Gerais	0	2	2
19/08/2024	Paraná	Paraná	829	0	829
19/08/2024	Paraná	Rio Grande do Sul	0	3	3
19/08/2024	Paraná	Santa Catarina	0	3	3
19/08/2024	Paraná	São Paulo	0	6	6
19/08/2024	Pernambuco	Alagoas	0	2	2
19/08/2024	Pernambuco	Amazonas	0	1	1
19/08/2024	Pernambuco	Bahia	0	1	1
19/08/2024	Pernambuco	Paraíba	0	2	2
19/08/2024	Pernambuco	Pernambuco	573	0	573
19/08/2024	Pernambuco	Santa Catarina	0	1	1
19/08/2024	Pernambuco	São Paulo	0	2	2
19/08/2024	Piauí	Ceará	0	1	1
19/08/2024	Piauí	Maranhão	0	2	2
19/08/2024	Piauí	Piauí	205	0	205
19/08/2024	Rio de Janeiro	Bahia	0	1	1

Data	Estado do Dispositivo	Estado no Aplicativo	Total Mesmo Estado	Total Estado Diferente	Total com Localização
19/08/2024	Rio de Janeiro	Espírito Santo	0	5	5
19/08/2024	Rio de Janeiro	Maranhão	0	5	5
19/08/2024	Rio de Janeiro	Minas Gerais	0	6	6
19/08/2024	Rio de Janeiro	Rio de Janeiro	1160	0	1160
19/08/2024	Rio de Janeiro	Santa Catarina	0	1	1
19/08/2024	Rio de Janeiro	São Paulo	0	9	9
19/08/2024	Rio Grande do Norte	Bahia	0	1	1
19/08/2024	Rio Grande do Norte	Minas Gerais	0	1	1
19/08/2024	Rio Grande do Norte	Paraíba	0	2	2
19/08/2024	Rio Grande do Norte	Rio Grande do Norte	188	0	188
19/08/2024	Rio Grande do Sul	Bahia	0	1	1
19/08/2024	Rio Grande do Sul	Pará	0	2	2
19/08/2024	Rio Grande do Sul	Paraná	0	2	2
19/08/2024	Rio Grande do Sul	Rio Grande do Sul	1262	0	1262
19/08/2024	Rio Grande do Sul	Santa Catarina	0	7	7
19/08/2024	Rio Grande do Sul	São Paulo	0	4	4
19/08/2024	Rondônia	Rondônia	173	0	173
19/08/2024	Roraima	Alagoas	0	3	3
19/08/2024	Roraima	Roraima	58	0	58
19/08/2024	Santa Catarina	Ceará	0	1	1
19/08/2024	Santa Catarina	Mato Grosso	0	2	2
19/08/2024	Santa Catarina	Paraná	0	5	5
19/08/2024	Santa Catarina	Rio Grande do Sul	0	4	4
19/08/2024	Santa Catarina	Santa Catarina	908	0	908
19/08/2024	Santa Catarina	São Paulo	0	3	3
19/08/2024	São Paulo	Amazonas	0	1	1
19/08/2024	São Paulo	Bahia	0	3	3
19/08/2024	São Paulo	Distrito Federal	0	4	4
19/08/2024	São Paulo	Goiás	0	2	2
19/08/2024	São Paulo	Maranhão	0	5	5
19/08/2024	São Paulo	Mato Grosso	0	4	4
19/08/2024	São Paulo	Minas Gerais	0	11	11

Data	Estado do Dispositivo	Estado no Aplicativo	Total Mesmo Estado	Total Estado Diferente	Total com Localização
19/08/2024	São Paulo	Paraíba	0	1	1
19/08/2024	São Paulo	Paraná	0	13	13
19/08/2024	São Paulo	Pernambuco	0	1	1
19/08/2024	São Paulo	Rio de Janeiro	0	14	14
19/08/2024	São Paulo	Rio Grande do Sul	0	1	1
19/08/2024	São Paulo	Roraima	0	1	1
19/08/2024	São Paulo	Santa Catarina	0	5	5
19/08/2024	São Paulo	São Paulo	3227	0	3227
19/08/2024	São Paulo	Sergipe	0	1	1
19/08/2024	Sem Estado	Alagoas	0	0	6
19/08/2024	Sem Estado	Amazonas	0	0	14
19/08/2024	Sem Estado	Bahia	0	0	57
19/08/2024	Sem Estado	Ceará	0	0	22
19/08/2024	Sem Estado	Distrito Federal	0	0	10
19/08/2024	Sem Estado	Espírito Santo	0	0	20
19/08/2024	Sem Estado	Goiás	0	0	29
19/08/2024	Sem Estado	Maranhão	0	0	10
19/08/2024	Sem Estado	Mato Grosso	0	0	19
19/08/2024	Sem Estado	Minas Gerais	0	0	70
19/08/2024	Sem Estado	Pará	0	0	9
19/08/2024	Sem Estado	Paraíba	0	0	7
19/08/2024	Sem Estado	Paraná	0	0	49
19/08/2024	Sem Estado	Pernambuco	0	0	40
19/08/2024	Sem Estado	Piauí	0	0	6
19/08/2024	Sem Estado	Rio de Janeiro	0	0	68
19/08/2024	Sem Estado	Rio Grande do Norte	0	0	6
19/08/2024	Sem Estado	Rio Grande do Sul	0	0	24
19/08/2024	Sem Estado	Rondônia	0	0	7
19/08/2024	Sem Estado	Roraima	0	0	1
19/08/2024	Sem Estado	Santa Catarina	0	0	29
19/08/2024	Sem Estado	São Paulo	0	0	198
19/08/2024	Sem Estado	Sergipe	0	0	11

Data	Estado do Dispositivo	Estado no Aplicativo	Total Mesmo Estado	Total Estado Diferente	Total com Localização
19/08/2024	Sem Estado	Tocantins	0	0	3
19/08/2024	Sergipe	Bahia	0	1	1
19/08/2024	Sergipe	Rio de Janeiro	0	1	1
19/08/2024	Sergipe	Sergipe	114	0	114
19/08/2024	Tocantins	Goiás	0	1	1
19/08/2024	Tocantins	Maranhão	0	1	1
19/08/2024	Tocantins	Tocantins	114	0	114