



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

**Métodos de autenticação considerando aspectos de
segurança, privacidade e experiência de uso: a visão
dos usuários finais**

Ronald Carvalho Ribeiro de Araujo

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

Orientador

Prof.a Dr.a Letícia Lopes Leite

Brasília
2022

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

AA663m ARAUJO, RONALD CARVALHO RIBEIRO DE
Métodos de autenticação considerando aspectos de
segurança, privacidade e experiência de uso: a visão dos
usuários finais / RONALD CARVALHO RIBEIRO DE ARAUJO;
orientador Leticia Lopes Leite. -- Brasília, 2022.
88 p.

Dissertação (Mestrado - Mestrado Profissional em
Computação Aplicada) -- Universidade de Brasília, 2022.

1. Sistemas de gerenciamento de identidade. 2.
Identidade eletrônica. 3. Métodos de autenticação. I. Leite,
Leticia Lopes, orient. II. Título.



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

**Métodos de autenticação considerando aspectos de
segurança, privacidade e experiência de uso: a visão
dos usuários finais**

Ronald Carvalho Ribeiro de Araujo

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

Prof.a Dr.a Leticia Lopes Leite (Orientador)
CIC/UnB

Prof.a Dr.a Edna Dias Canedo Prof. Dr. Jean Everson Martina
CIC/UnB LabSEC/UFSC

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-Graduação em Computação Aplicada

Brasília, 19 de janeiro de 2022

Dedicatória

Dedico esse trabalho a minha esposa Lorena. Sua paciência, confiança, compreensão e força me serviram de inspiração para encarar o desafio, especialmente considerando o cenário do primeiro ano de vida da nossa pequena Lisie e de crescimento do nosso pequeno Davi. Lorena, obrigado por sempre me apoiar em meus projetos pessoais e profissionais.

Agradecimentos

Agradeço imensamente à Prof.^a Dr.^a Letícia Lopes Leite pela parceria, paciência e principalmente por sua clareza em me orientar durante todo o processo.

Agradeço também aos docentes e discentes do programa de mestrado, pela troca de experiências e pelo espírito de construção de elos e conhecimento.

Finalmente, agradeço ao Serviço Federal de Processamento de Dados, especialmente na figura do Sr. Pedro Moacir Rigo Motta, por sempre ter acreditado em mim e me ofertado condições para o crescimento pessoal e profissional.

Resumo

Na ausência da oferta de serviço digital, é comum que o cidadão precise percorrer significativas distâncias para ter acesso a um determinado serviço ou mesmo despende o seu tempo em filas. A virtualização de serviços se apresenta como uma necessidade latente e com a incidência da pandemia provocada pela Covid-19 e a imposição da necessidade de distanciamento social, se torna ainda mais imprescindível o provimento de serviços digitais, criando assim um ambiente propício para a aceleração do processo de transformação digital.

Neste contexto, diversos serviços on-line necessitam de uma forma de identificação dos seus usuários, sendo fundamental a presença de um sistema de gerenciamento de identidades (IdM). É um diferencial competitivo para as empresas ofertarem um serviço customizado de uso dos seus serviços, de forma que o usuário se perceba como único e fundamental para o processo. Por outro lado, as preocupações com privacidade e segurança da informação são cada vez mais presentes e necessárias.

Este trabalho apresenta a visão dos usuários finais a respeito de processos de autenticação que são utilizados em sistemas de IdM, considerando sua percepção a respeito dos aspectos de segurança, privacidade e experiência de uso. É apresentado o método utilizado, os resultados obtidos e as limitações da realização de um questionário e de um experimento com usuários finais. No questionário são abordados aspectos sobre as crenças dos usuários a respeito de métodos de autenticação, enquanto que o experimento busca capturar e entender o comportamento dos usuários quando realizam uma atividade de autenticação. O estudo traz como contribuição a análise e apresentação de diferentes abordagens para a estruturação de um sistema de IdM, o método aplicado e os resultados para a condução de um questionário e um experimento sobre a percepção e o comportamento dos usuários finais durante o processo de autenticação em sistemas. Além disso, este trabalho contribui com a disponibilização de um software que pode ser utilizado para a realização de experimentos de autenticação com usuários finais.

Palavras-chave: Métodos de autenticação, Sistemas de gerenciamento de identidade, Experiência de uso, Privacidade e proteção de dados, Segurança no acesso.

Abstract

In the absence of a digital service offer, it is usual that citizens need to travel significant distances to access a particular service or even spend their time in queues. The virtualization of services becomes a latent need. With the incidence of the pandemic caused by Covid-19 and the imposition of the need for social distancing, the provision of digital services becomes even more essential, creating a favorable environment for the acceleration of the digital transformation process.

In this context, several online services need a way to identify their users, the presence of an identity management system (IdM) being essential. It is a competitive advantage for companies to offer a customized process for using their services so that the end-user perceive themselves as unique and fundamental to the process. On the other hand, concerns about privacy and information security are increasingly present and necessary.

This work presents the vision of end-users regarding authentication methods used in IdM systems. The applied method, the results, and the limitations of conducting a questionnaire and an experiment with end-users are shown. The main objective was to investigate the perception and behavior of these users when faced with sentences and with a practical application of different forms of authentication. The study shows as a contribution the method applied and the results of tests on the belief and evaluation of end-users about aspects of user experience, security, and privacy. Also, this works provides software to perform new authentication experiments.

Keywords: Authentication methods, Identity management systems, User experience, Privacy and data protection, Access security.

Sumário

1	Introdução	1
1.1	Definição do Problema	2
1.2	Hipóteses	3
1.3	Justificativa	4
1.4	Objetivos	5
1.4.1	Objetivo Geral	5
1.4.2	Objetivos Específicos	5
1.5	Resultados Esperados	6
1.6	Estrutura da Dissertação	6
2	Revisão da Literatura	8
2.1	Conceito de Identidade Eletrônica	8
2.2	Privacidade de Dados	9
2.3	Infraestrutura de Chaves Públicas	11
2.4	Abordagens de Sistemas de Identidade Eletrônica	13
2.4.1	Isolada	14
2.4.2	Centralizada	15
2.4.3	Federada	15
2.4.4	Centrada no Usuário	16
2.4.5	Auto-soberana (Descentralizada)	17
2.5	Métodos de Autenticação	20
2.5.1	Senha	20
2.5.2	Código de Acesso	20
2.5.3	Biometria	21
2.5.4	Duplo Fator de Autenticação (2FA)	22
2.6	Metodologia de Pesquisa	22
2.6.1	Preparação da Pesquisa	23
2.6.2	Apresentação e Interrelação dos Dados	24
2.6.3	Detalhamento e Compilação dos Trabalhos Recuperados	25

2.7	Trabalhos Relacionados	25
3	Percepção dos Usuários de Serviços de Autenticação	28
3.1	Método Aplicado	28
3.2	Resultados e Discussão	32
3.3	Limitações e Ameças	38
3.4	Síntese do Capítulo	38
4	Comportamento e Avaliação dos Usuários de Serviços de Autenticação	39
4.1	Método Aplicado	39
4.1.1	<i>Design</i> da Solução de Software Desenvolvida	40
4.1.2	Métodos de Autenticação Utilizados	43
4.1.3	Avaliação do Usuário	48
4.1.4	Participantes do Experimento	49
4.2	Resultados e Discussão	51
4.3	Limitações e Ameças ao Experimento	55
4.4	Síntese do Capítulo	56
5	Conclusão	57
5.1	Contribuições	59
5.2	Trabalhos Futuros	60
	Referências	61
	Apêndices	69
A	Termo de Consentimento Livre e Esclarecido do Questionário	70
B	Formulário do Questionário	71
C	Termo de Consentimento Livre e Esclarecido do Experimento	77
D	Documentação da API do Experimento	79
E	Dicionário de Dados das Tabelas do Experimento	87

Lista de Figuras

2.1	Abordagem de identidade isolada.	14
2.2	Abordagem de identidade centralizada.	15
2.3	Abordagem de identidade federada.	16
2.4	Abordagem de identidade centrada no usuário.	17
2.5	Relações em um sistema de credenciais verificáveis.	19
2.6	Nuvem de Palavras.	24
3.1	Resultado das questões demográficas.	33
3.2	Resultado do questionários para as Sentenças 1 a 5.	35
3.3	Resultado do questionários para as Sentenças 6 a 11.	37
4.1	Componentes da solução de software.	41
4.2	Modelo de dados do software do experimento.	42
4.3	Experimento de autenticação com senha.	44
4.4	Experimento de autenticação com código de acesso.	45
4.5	Experimento de autenticação com biometria facial.	46
4.6	Experimento de autenticação com duplo fator de autenticação.	48
4.7	Avaliação do método de autenticação.	49
4.8	Exemplo de URLs utilizadas no experimento.	50
4.9	Resultados do experimento de autenticação.	52
4.10	Diagrama de radar para cada um dos métodos de autenticação.	53
4.11	Duração dos processos de autenticação.	54
4.12	Matriz de correlação entre as variáveis do experimento.	55

Lista de Tabelas

2.1 Temática dos trabalhos relacionados.	27
--	----

Lista de Abreviaturas e Siglas

AES *Advanced Encryption Standard.*

eID *Electronic Identification.*

GDPR *General Data Protection Regulation.*

HOTP *HMAC-based One-Time Password.*

ICP *Infraestrutura de Chaves Públicas.*

ICP-Brasil *Infraestrutura de Chaves Públicas Brasileira.*

IdM *Identity Management System.*

IdP *Identity Provider.*

LGPD *Lei Geral de Proteção de Dados.*

MFA *Múltiplos Fatores de Autenticação.*

NUI *Natural User Interface.*

ONU *Organização das Nações Unidas.*

OTP *One-Time Password.*

PAD *Personal Authentication Device.*

SP *Service Provider.*

SSL *Secure Sockets Layer.*

SSO *Single Sign-On.*

TCLE Termo de Consentimento Livre e Esclarecido.

TEMAC Teoria do Enfoque Meta Analítico Consolidado.

TI Tecnologia da Informação.

TLS *Transport Layer Security*.

TOTP *Time-based One-Time Password*.

YSH Yeh-Shen-Hwang.

Capítulo 1

Introdução

O excesso de burocracia constitui uma barreira no acesso dos cidadãos aos serviços de governo e inviabiliza a adoção de um processo de transformação digital. O modelo de provimento de serviços baseado em balcão de atendimento presencial é contraproducente e de custo financeiro elevado, ao mesmo passo que é necessário ampliar as ofertas de serviço para os cidadãos.

Visando remover gargalos de produtividade e aumentar a efetiva participação da sociedade, a implementação de um governo digital tem originado mudanças significativas e duradouras na forma como as pessoas vivem e interagem entre si, bem como com o ambiente e os serviços públicos. De acordo com o Estudo sobre Governo Eletrônico, realizado pela Organização das Nações Unidas ONU [1], existe uma tendência global, positiva e persistente em direção a maiores níveis de desenvolvimento de governo digital. Ainda segundo a ONU, a participação da sociedade em um governo digital é definida como a soma de programas governamentais que encorajam a participação dos cidadãos, compreendendo a demanda e a oferta nas interações envolvendo governo e cidadãos [2].

Com a incidência da pandemia provocada pela Covid-19 e a imposição da necessidade de distanciamento social, se torna ainda mais importante o provimento de serviços digitais, requerendo um novo olhar sobre os processos instituídos e buscando evolução e otimização na prestação de serviços, caracterizando assim um processo de transformação digital. É de se destacar que a transformação digital não depende apenas de tecnologias mas, também, de uma abordagem abrangente que ofereça serviços acessíveis, rápidos, confiáveis e personalizados. Princípios como eficácia, inclusão, prestação de contas, credibilidade e transparência devem guiar as tecnologias, e não o contrário. A adesão massiva ao digital se apresenta como um caminho sem volta. [1]

Sistemas de gerenciamento de identidades eletrônicas (IdM) são fundamentais para um processo de transformação digital [3]. Respeitar aspectos de proteção e privacidade de dados, ser inclusivo e possuir uma experiência de uso facilitada, com uma interface

amigável são requisitos fundamentais para um sistema de IdM. Além destes requisitos, confiança é um ponto chave para viabilizar a adoção duradoura dos cidadãos em um sistema de IdM [4] [5]. Neste cenário, é um desafio fundamental prover uma solução que permita aos usuários o controle sobre os seus dados e e sobre ações que possam ser realizadas a partir da sua identidade.

1.1 Definição do Problema

A adoção de um modelo de sociedade digital faz com que os cidadãos não despendam parte do seu tempo em atividades burocráticas presenciais, por vezes sendo necessário percorrer significativas distâncias para ter acesso a serviços de governo ou mesmo despendem muito tempo em filas de serviços públicos. Desta forma, parte considerável da capacidade produtiva é perdida, o que impacta diretamente em seu desempenho [1] [6]. Nesta esteira, a virtualização de serviços torna-se uma necessidade latente e não se aplica apenas à relação entre cidadão e governo, uma vez que as relações privadas também requerem uma abordagem cada vez mais direcionada para serviços digitais.

Com a necessidade de se ofertar serviços em meio virtual é comum que diversos destes serviços necessitem de uma forma de identificação dos seus usuários. O conhecimento sobre o usuário possibilita que as aplicações ofereçam uma experiência de uso customizada de acordo com o seu perfil e necessidades, contribuindo para a adesão do usuário ao processo de digitalização e evidenciando o valor percebido pelo mesmo sobre o serviço oferecido [7]. Neste contexto, é fundamental que se tenha um sistema de gerenciamento de identidades (IdM) para viabilizar o processo de autenticação dos usuários.

A ausência de um sistema de identidade eletrônica robusto e interoperável, desacelera o processo de transformação digital e constitui uma barreira para a implementação de uma estratégia de governo digital [3] [8]. Além disso, em situações que requeiram a ação imediata do Estado, o não conhecimento dos cidadãos dificulta a definição e a implementação de políticas públicas eficientes. Exemplo disso foi observado durante a execução do programa Auxílio Emergencial ¹, onde mediante a necessidade de isolamento social, foram observadas enormes filas em diversas localidades do país. O programa Auxílio Emergencial foi implementado pelo Estado Brasileiro com o objetivo de garantir uma renda mínima para os brasileiros mais vulneráveis que foram afetados pela crise econômica decorrente da pandemia provocada pela Covid-19. Com o decorrer dos meses, o governo brasileiro conseguiu maior estabilidade no serviço digital ofertado através da aplicação Auxílio Emergencial ²,

¹<https://www.gov.br/cidadania/pt-br/servicos/auxilio-emergencial>

²<https://auxilio.caixa.gov.br/#/inicio>

destinado para o pagamento do auxílio, porém problemas de fraudes decorrentes de não garantia de identidade ainda são frequentes [9].

Um problema no processo de garantia da identidade é a autenticação dos usuários, uma vez que é neste momento que o usuário apresenta suas credenciais e o serviço digital precisa ter a convicção que o usuário realizando o acesso é de fato quem se diz ser. O equilíbrio entre usabilidade, segurança e respeito à proteção e privacidade de dados se constitui como um desafio difícil de ser superado. Se por um lado abordagens de credenciais de acesso baseadas em login e senha são massificadas e fáceis de utilizar, estas abordagens são consideradas como sendo de baixo nível de segurança, uma vez que as credenciais podem ser descobertas e utilizadas sem que o titular tenha conhecimento, tornando-se passíveis de serem transmitidas para terceiros e objetos de ataques de engenharia social. Por outro lado, abordagens com o uso de chaves públicas possuem elevado nível de segurança, entretanto são complexas de serem implementadas e utilizadas, já que, em geral, requerem um dispositivo de hardware adicional e instalação de softwares específicos [10].

O fato é que, independente da abordagem utilizada, sistemas de gerenciamento de acesso são vulneráveis a cenários de roubo de identidade, desrespeito à privacidade dos usuários e dificuldade na recuperação destas chaves. A experiência de uso dificultada agrava estes problemas e contribui para que os titulares da identidade fiquem mais expostos e vulneráveis. A adoção de padrões abertos, a utilização de dispositivos de segurança baseados em hardware, o uso de biometria e a adoção códigos de acesso únicos podem oferecer uma possibilidade de solução para o problema da autenticação dos usuários finais em sistemas de IdM.

1.2 Hipóteses

Para a condução deste trabalho, algumas hipóteses foram levantadas e serão examinadas no decorrer do estudo. São elas:

- A experiência de uso é mais valorizada pelos usuários em comparação com a privacidade e a segurança do processo de autenticação.
- Os cidadãos confiam em armazenar suas credenciais de usuário em soluções de computação em nuvem.
- A adoção de biometria no processo de identificação é mais bem aceita pelos usuários em detrimento de outros métodos de autenticação.

1.3 Justificativa

Segundo o Banco Mundial [11], cerca de 1,1 bilhão de pessoas no mundo não possuem identidade legal. A falta de identidade restringe o acesso dos cidadãos aos serviços públicos e ao sistema financeiro, fazendo com que seja agravada a situação de desigualdade social, como exemplo é possível mencionar o acesso aos sistemas públicos de saúde e a participação em programas sociais, onde somente cidadãos que possuem identidade podem usufruir. Além disso, problemas de identificação de usuários moldam um cenário propício para a ocorrência de fraudes. Nesse contexto, as identidades digitais têm sido oferecidas como uma forma de efetivamente agilizar o processo de identificação das pessoas [12].

A preocupação com sistemas de IdM é latente a ponto de ser incluída como um dos Objetivos de Desenvolvimento Sustentáveis da Agenda 2030 [13]. Com o objetivo de desenvolver ações que promovam o desenvolvimento global e sustentável, a Agenda 2030 é um compromisso firmado por 193 países, incluindo o Brasil, onde são descritos 17 objetivos de desenvolvimento sustentável e 169 metas para a promoção de desenvolvimento sem comprometer as necessidades das gerações futuras. O Objetivo de Desenvolvimento Sustentável 16, denominado **Paz, Justiça e Instituições eficazes**, visa promover sociedades pacíficas e inclusivas. Dentro deste objetivo, a meta 16.9 prevê o provimento de identidade legal para todos e, nesse aspecto, o uso de Identidade Eletrônica (eID) é considerado fundamental para viabilizar o alcance da referida meta [14]. Segundo o Instituto Global McKinsey [15] a implementação de um sistema de IdM no Brasil é capaz de otimizar diversos setores da sociedade e pode propiciar um incremento entre 8% e 13% do PIB até 2030.

Com o distanciamento social provocado pela pandemia da Covid-19 ficou evidente a necessidade das interações virtuais, inclusive como forma de movimentar a economia [16] [17]. Novos modelos de negócio foram criados e modelos antigos foram atualizados e, neste contexto, é fundamental que as entidades sejam identificadas de maneira confiável, segura e com respeito à privacidade de seus dados. Uma identificação eletrônica massificada e interoperável possibilita que as aplicações não dupliquem dados pessoais do cidadão, fornecendo a ele o controle sobre seus dados e sobre quem poderá acessá-los, alinhando-se assim com a LGPD [18]. Ainda, com a utilização de mecanismos de gestão de identidade espera-se também uma redução nas fraudes de identificação, promovendo um incremento na segurança do sistema de IdM.

Segurança, no escopo de sistemas de IdM, é definida como um conjunto de políticas, técnicas e procedimentos que visam proteger os usuários e os seus dados contra o uso indevido e/ou não autorizado [5]. No escopo deste trabalho, a segurança será abordada da perspectiva do usuário durante processos de autenticação. Já a privacidade, de acordo com Cavoukian [19], deve ser observada desde a concepção das aplicações, visando preservar

a vontade dos usuários sobre o acesso a seus dados pessoais, criando uma relação de confiança entre o usuário e o serviço de identidade.

De acordo com Cameron [5], confiança é fundamental para que seja possível a adoção de um sistema de IdM por parte dos usuários e, neste contexto, ainda de acordo com Cameron [5], confiança é definida como um compromisso para com o usuário, de forma que ele tenha controle de quais identidades serão utilizadas e de quais informações serão compartilhadas, direcionando assim para a proteção e privacidade dos dados. O sistema de IdM também deve proteger o usuário contra ações e entidades fraudulentas, zelando para que as informações de identidade sejam compartilhadas apenas com destinatários verificados. Um exemplo de situação fraudulenta são ataques baseados em engenharia social, onde um atacante tenta ludibriar o usuário legítimo para que possa obter acesso às suas credenciais ou a informações que possam levar o atacante a ter acesso às credenciais legítimas do usuário. Um processo eficiente de gestão de acesso de usuário é fundamental para a construção e o fortalecimento da relação de confiança entre usuário e provedor de serviço digital. Um exemplo que chama atenção é com relação ao projeto Acesso Gov.br, o provedor de identidades do Governo Federal Brasileiro, onde cerca de 44% dos acessos de usuário final apresentam falha de credencial durante a autenticação [20].

1.4 Objetivos

1.4.1 Objetivo Geral

Investigar o processo de autenticação em sistemas de IdM sob o ponto de vista dos usuários finais, considerando sua percepção a respeito dos aspectos de segurança, privacidade e experiência de uso.

1.4.2 Objetivos Específicos

Os objetivos específicos foram elencados de forma a contribuir para o alcance do objetivo geral deste trabalho.

- Conhecer os principais atores envolvidos no gerenciamento de identidades eletrônicas e como eles se relacionam.
- Realizar análise das principais abordagens de IdM.
- Aplicar um questionário para investigar a crença e percepção dos usuários a respeito de processos de autenticação em sistemas de IdM.

- Realizar um experimento onde se possa avaliar o comportamento dos usuários quando deparados com diferentes formas de autenticação, como: usuário e senha, biometria e códigos de acesso descartáveis.
- Implementar software com diferentes métodos de autenticação, de forma que possa viabilizar a investigação do comportamento dos usuários quando deparados com estes métodos.
- Avaliar os resultados coletados pelo experimento realizado com o intuito de analisar o comportamento dos participantes.

1.5 Resultados Esperados

É esperado que este trabalho apresente como resultado um método para investigação e maior entendimento acerca de crenças e comportamentos dos usuários finais sobre soluções de autenticação em serviços on-line, sendo abordada a percepção dos usuários sobre segurança, privacidade e experiência de uso. O resultado dos ensaios realizados neste trabalho poderá servir como subsídio para a construção de soluções de autenticação direcionadas a suprir as necessidades dos usuários e que, desta forma, possam contar com maior engajamento destes. Adicionalmente, é esperado que este trabalho disponibilize um software que implemente diferentes mecanismos de autenticação e que, para cada um dos métodos de autenticação implementados, o usuário final possa indicar a sua avaliação a respeito do método de autenticação a qual foi submetido.

A construção do software se mostrou pertinente, uma vez que é possível coletar a avaliação do usuário imediatamente após este usuário ser submetido a um processo de autenticação na prática, onde se supõe que sua avaliação seja mais fidedigna do que quando comparada à leitura de uma sentença acerca de um método de autenticação. O software é expansível de forma a fomentar investigações futuras no tema abordado, incluindo a habilitação de novas formas de autenticação ou a adaptação de uma das formas já apresentadas.

1.6 Estrutura da Dissertação

Este trabalho está estruturado em cinco seções contemplando, além deste Capítulo introdutório, o Capítulo 2 que apresenta os atores e as principais abordagens de IdM, além de uma revisão da literatura com os conceitos que serviram como base para o desenvolvimento da pesquisa.

O Capítulo 3 apresenta um questionário que objetiva entender a percepção dos usuários finais com relação a métodos de autenticação utilizados em sistemas de IdM.

O Capítulo 4 demonstra o método aplicado, com os detalhes do software implementado e da condução de um experimento. Além de apresentar os resultados do experimento realizado com o intuito de capturar o comportamento dos usuários quando deparados com diferentes métodos de autenticação.

O Capítulo 5 apresenta as conclusões deste trabalho, suas contribuições e endereça trabalhos futuros.

Capítulo 2

Revisão da Literatura

Nesta seção será apresentado um levantamento sobre os principais conceitos e abordagens envolvidas em sistemas de gerenciamento de identidades.

2.1 Conceito de Identidade Eletrônica

A identidade eletrônica (eID) é a forma identificação inequívoca de um usuário no mundo digital [21] [7] [22]. Já a identificação eletrônica é definida como o processo de representação de “*quem você é*”, compreendendo um conjunto limitado de atributos da sua vida real [23].

Em geral, serviços digitais requerem que os seus usuários se identifiquem para que tenham acesso às funcionalidades desejadas. Desta forma, uma eID é peça-chave no processo de identificação e autenticação dos usuários [24].

Cada vez mais, um crescente número de serviços digitais tem se utilizado de mecanismos de identificação eletrônica [25]. Sistemas de identificação eletrônica são elementos fundamentais para a implantação de estratégias de governo digital, especialmente no que se refere à comunicação entre governos e os cidadãos [26] [27]. Conforme apresentado por Priesnitz [28] e Prusa [29], um sistema de identificação eletrônica confiável é pré-requisito para a implementação de uma estratégia de governo digital. Já Meyerhoff [30] define identificação eletrônica como sendo um facilitador essencial no processo de transformação digital da prestação de serviços públicos. Além de identificar o usuário de forma individualizada, é necessário estender o conhecimento sobre o mesmo. Para tanto, é requisito obter atributos adicionais, de modo a ofertar serviços mais complexos e que requerem um grau de conhecimento adicional acerca do cidadão [7].

Independente da solução tecnológica adotada, o ponto mais importante é que as abordagens de eID atentem para os aspectos de privacidade, integridade, confiabilidade e qualidade dos dados [30].

Um IdM é um conjunto de políticas, processos e tecnologias que possibilitam o controle de acesso de usuários, gerenciamento de acesso a recursos e auditoria baseados no uso de identidades digitais [31]. Reduzir custos de gerenciamento, possibilitar compartilhamento de informação e aumentar a segurança e a privacidade das identidades são objetivos de um IdM [32]. Gerenciar o ciclo de vida das identidades é o papel fundamental de um IdM, incluindo processos de criação, segurança, gerenciamento de atributos, agregação, sincronização e exclusão de identidades [33].

Em diversos cenários de um sistema de identificação eletrônica, é importante que, a partir da identidade, também sejam derivados atributos adicionais a respeito do usuário em questão como, por exemplo, data de nascimento, sexo, idade, nacionalidade [28]. Ao longo dos anos, os sistemas eletrônicos passaram cada vez mais a coletar, processar e armazenar dados de atributos de usuários. O maior conhecimento dos usuários possibilita que as aplicações ofereçam serviços personalizados e mais direcionados para o perfil e as necessidades dos seus usuários [7]. Em outra via, episódios envolvendo comercialização de dados pessoais e constantes vazamentos de dados, despertaram a sociedade e os governos para a necessidade de um maior controle e regulação sobre o tema [34]. Em decorrência deste cenário, surgiram os marcos regulatórios de privacidade e proteção de dados.

2.2 Privacidade de Dados

Em sistemas de IdM, mesmo que o requisito de segurança dos dados seja atingido, os usuários são prejudicados se não for implementada uma estratégia de proteção à privacidade dos dados [35]. Neste sentido, é importante a diferenciação entre privacidade e proteção de dados. De acordo com a definição do Banco Mundial [36] a privacidade diz respeito à existência de governança para os processos de coleta, compartilhamento e manipulação dos dados pessoais. Por sua vez, a proteção se refere à segurança da informação, à criação de barreiras contra vazamento de dados e à utilização de técnicas de criptografia, ofuscação de dados, assinaturas digitais, entre outras.

A análise e cruzamento de dados pessoais são estratégias poderosas em uma sociedade cada vez mais digital e, quando aplicadas de forma estruturada, possibilitam influenciar o modo como as pessoas se comportam, o perfil de consumo, convicções ideológicas e, até mesmo, como os representantes são eleitos [37] [38]. Neste cenário, as informações pessoais possuem alto valor comercial e são alvo de ataques e vazamentos de dados [39], despertando a sociedade e os governos para a necessidade de um maior controle e regulação sobre o tema [34]. Em decorrência desta situação, surgiram os marcos regulatórios de privacidade e proteção de dados como, por exemplo, o Regulamento Geral de Proteção de Dados Europeu (GDPR) [40] e a Lei Geral de Proteção de Dados (LGPD) [18].

A LGPD redefine a relação entre os prestadores de serviços e os titulares dos dados. A orientação da LGPD é direcionada para a proteção e a privacidade dos dados dos usuários, introduzindo um aparato legal unificado para todo o país no que se refere a estas informações.

A LGPD fez com que o Brasil se inserisse no cenário global, habilitando-se para que dados possam ser compartilhados respeitando os aspectos de privacidade e segurança. A fiscalização e as penalidades fazem parte deste contexto como uma forma de regular a manipulação de dados pessoais.

No escopo de sistemas de IdM, as preocupações com a privacidade são consolidadas no que é conhecido como as **Sete Leis de Identidade** [5] [19]. São elas:

1. Controle e consentimento pessoal: o controle e a liberdade de escolha são fundamentais para a privacidade. O consentimento é necessário para ambos os casos, devendo ser informado e não coagido, além de poder ser revogado a qualquer tempo.
2. Divulgação mínima: a divulgação das informações de identificação deve ser o mínimo possível. Como forma de auxiliar no cumprimento desta lei, a coleta e a retenção de dados deve ser limitada ao mínimo necessário para a realização do objetivo, reduzindo a possibilidade de exposição.
3. Partes justificáveis: o acesso aos dados pessoais deve ser realizado apenas pelas partes que de fato precisam ter acesso aos dados, obedecendo o ideia de necessidade de saber.
4. Identidade direta: a possibilidade de uso de identificadores unidirecionais como forma de minimizar o rastreamento de identidade. É incentivado o uso de identificadores unidirecionais nas relações entre entes privados. O uso de identificadores unidirecionais minimizam a possibilidade de correlação dos dados de um titular em diferentes contextos, uma vez que para cada contexto existirá um novo identificador.
5. Pluralidade de operadores e tecnologias: a interoperabilidade de operadores e tecnologias é um requisito fundamental em um sistema de gerenciamento de identidade. A obediência a esta lei protege o sistema do aprisionamento tecnológico.
6. Integração humana: as interfaces com o usuário devem ser claras, objetivas, de simples entendimento e que ofereçam proteção contra ataques de identidade. A confiança com o sistema é baseada na sua capacidade de se fazer entender.
7. Experiência consistente: os usuários precisam ter uma experiência de uso simples e consistente, com a clara separação dos contextos envolvidos. A compreensão do

usuário facilita a sua tomada de decisão e o coloca no controle efetivo das ações envolvendo os seus dados.

A observação das Leis de Identidade deixa explícita a relação entre a proteção de dados pessoais e os sistemas de IdM. Para o escopo deste trabalho é relevante o respeito aos dados dos usuários, sendo que o processo de gerenciamento de chaves possibilita que a identificação dos usuários ocorra respeitando a privacidade.

2.3 Infraestrutura de Chaves Públicas

Uma infraestrutura de chaves públicas (ICP) é uma cadeia hierárquica de confiança que usualmente utiliza certificados digitais X.509 definidos na RFC 5280 [41]. O principal objetivo desta RFC é definir um perfil para fomentar o uso de certificados digitais, buscando padronizar as técnicas aplicadas para o desenvolvimento de sistemas e ferramentas, provendo interoperabilidade. Uma ICP busca, a partir das informações contidas nos certificados digitais, atender às necessidades de identificação, autorização e controle de acesso a determinado recurso. As ICPs se baseiam no conceito de criptografia assimétrica, também conhecido como criptografia de chaves públicas [42]. Neste modelo cada titular é representado por um par de chaves criptográficas: uma pública e uma privada. A chave pública precisa ser distribuída para que todos possam conhecer o titular da referida chave privada. Desta forma, utilizando a chave pública de um determinado usuário, é possível confirmar ações realizadas por este usuário com a sua chave privada [43].

Em uma ICP, as Autoridades Certificadoras funcionam como uma parte confiável e certificam que determinada chave pública pertence a determinado usuário. O certificado digital é uma declaração pública, desta forma é mandatório se preocupar com o conjunto de atributos do titular da chave que será contido nos certificados digitais. A cultura de uma ambiente de confiança federada fez com que as ICP's fossem adotadas em larga escala no mundo digital. Os padrões *Secure Sockets Layer* (SSL) [44] e *Transport Layer Security* (TLS) [45] são baseados em ICP e a grande maioria das abordagens de sistemas de gerenciamento de identidades federadas utilizam ICP como base para suas transações.

No Brasil, uma ICP foi instituída oficialmente em 2001, através da medida provisória nº 2.200-2 [46], dando origem assim à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Esta mesma medida provisória instituiu o Comitê Gestor da ICP-Brasil como autoridade gestora desta ICP, sendo este comitê composto por membros da administração pública e da sociedade civil. Ainda no âmbito da MP 2.200-2, os documentos assinados com certificados digitais emitidos na ICP-Brasil possuem presunção de verdade em relação aos signatários, ou seja, se equivalem a uma assinatura manuscrita.

O Brasil atualmente possui cerca de cinco milhões de certificados digitais ativos emitidos na ICP-Brasil [47], um número baixo quando comparado com a população de aproximadamente 212 milhões de brasileiros [48]. Considerando a importância das interações digitais e a necessidade de massificação e popularização das assinaturas eletrônicas, o Estado brasileiro promulgou a Lei nº 14.063, de 23 de Setembro de 2020 [49], que trata de processos de assinaturas eletrônicas em interações com entes públicos, entre pessoas jurídicas e em questões de saúde. A referida lei institui a classificação das assinaturas eletrônicas em três grupos:

- Assinaturas eletrônicas simples: permite identificar o assinante e associa dados do assinantes ao objeto assinado.
- Assinaturas eletrônicas avançadas: utiliza certificados digitais emitidos em outra ICP diferente da ICP-Brasil ou algum outro meio de comprovação da autoria e da integridade de documentos, desde que admitido pelas partes como válido. Uma assinatura será classificada como avançada quando o assinante for identificado de forma única, for possível certificar que o assinante possui a posse das chaves de assinatura e que mudanças posteriores nos documentos assinados possam ser detectáveis.
- Assinaturas eletrônicas qualificadas: realizadas com o uso de certificados digitais emitidos na ICP-Brasil.

A Lei nº 14.063 [49] também impõe restrições para o uso das classificações das assinaturas de acordo com a criticidade do documento ou da relação. Um dos efeitos esperados desta lei e da classificação das assinaturas é possibilitar uma maior oferta de serviços digitais, uma vez que as assinaturas simples e avançadas possuem um processo mais ágil para sua relação no que diz respeito às assinaturas qualificadas, que dependem da emissão de um certificado ICP-Brasil e submetem ao regimento da ICP-Brasil para emissão destes certificados.

Ainda no propósito de acelerar os processos de transformação digital, o Estado brasileiro também promulgou a Lei nº 14.129, de 29 de Março de 2021 [50], também conhecida como Lei do Governo Digital, que dispõe princípios e regras para o Governo Digital e que tem, dentre seus princípios, o estímulo ao uso das assinaturas eletrônicas nas interações entre os órgãos públicos e entre estes e os cidadãos. A Lei nº 14.129 amplia de forma significativa as possibilidades de uso das assinaturas avançadas, fazendo com que estas sejam aceitas em diversos processos a exemplo de: processo de digitalização de documentos, constituições de sociedades anônimas, prontuário digital, atos do código de trânsito brasileiro, previdência complementar e o programa Minha Casa Minha Vida ¹.

¹<https://www.gov.br/mdr/pt-br/assuntos/habitacao/minha-casa-minha-vida>

Como exposto, as ICP são estruturas fundamentais em processos de identificação, autenticação e assinaturas eletrônicas, se configurando como figura central em processos de IdM. O gerenciamento das chaves privadas dos usuários é um desafio para que a implementação de uma ICP possa ser massificada sem comprometer a segurança do processo e dos usuários, garantindo assim a confiabilidade e a validade dos atos praticados.

2.4 Abordagens de Sistemas de Identidade Eletrônica

Esta seção abordará as principais abordagens utilizadas para endereçar o desafio de identificação eletrônica [4]. Cabe ressaltar que não existe abordagem mais correta de implementação e que, cada uma delas, apresenta suas forças e fraquezas [30]. Atualmente, a tendência é que as arquiteturas de eID sejam elaboradas com foco em prover maior empoderamento do usuário no tratamento da sua identidade e dos seus dados pessoais [23]. Neste sentido, é importante apresentar os principais atores de um IdM [31] [32]. São eles:

- Usuário: é o representado pela identidade.
- Provedor de Serviço (SP): é a entidade que provê serviços e que requer uma identidade.
- Provedor de Identidade (IdP): é o responsável pela emissão da identidade dos usuários.

As abordagens de IdM apresentadas neste trabalho são: Isolada, Centralizada, Federada, Centrada no Usuário e Auto-soberana.

2.4.1 Isolada

A abordagem isolada é definida pelo poder de gerenciamento das identidades ficar restrito a uma única entidade. Nesta abordagem, o usuário é apenas um portador da sua identidade e não possui nenhum tipo de poder sobre a forma como a sua identidade é utilizada [51]. Os provedores de serviço realizam a guarda e possuem o controle total sobre a identidade e os dados do usuário. A Figura 2.1 ilustra graficamente o modelo de identidade centralizada.

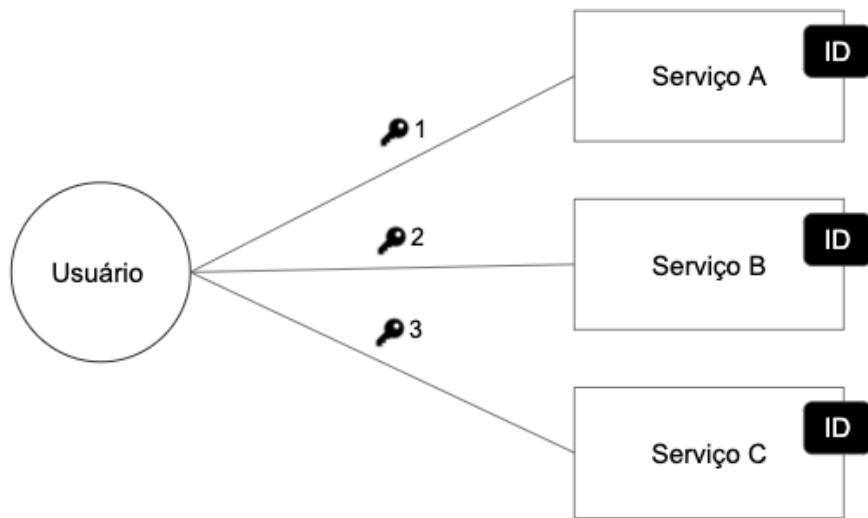


Figura 2.1: Abordagem de identidade isolada.

Fonte: O autor.

Do ponto de vista do provedor de serviço, a abordagem isolada possui uma implementação mais direta, pois independe de relações entre os provedores de serviço e provedores de identidade [51].

Um problema do isolamento é que, com a maior oferta de serviços, os usuários acabam tendo múltiplas identidades e tendo que arcar com toda a complexidade de conviver com um mundo de credenciais, muitas vezes baseadas no paradigma de usuário e senha, sendo bastante comum o esquecimento da senha por parte dos usuários [4].

Outro problema é que cada provedor de serviço é também um provedor de identidade, sendo assim, responsável pela gestão do ciclo de vida da identidade. Desta forma, a superfície de ataque é esparsa, o que permite que usuários mal intencionados possam se utilizar desta amplitude para explorar brechas de segurança em provedores de serviços que estão mais vulneráveis.

2.4.2 Centralizada

A abordagem centralizada se assemelha a abordagem isolada. A principal diferença entre estas abordagens é o fato de que na abordagem centralizada os papéis de provedor de serviço e provedor de identidade são exercidos por entidades distintas, porém existe apenas um único provedor de identidade [31]. A Figura 2.2 representa o modelo centralizado.

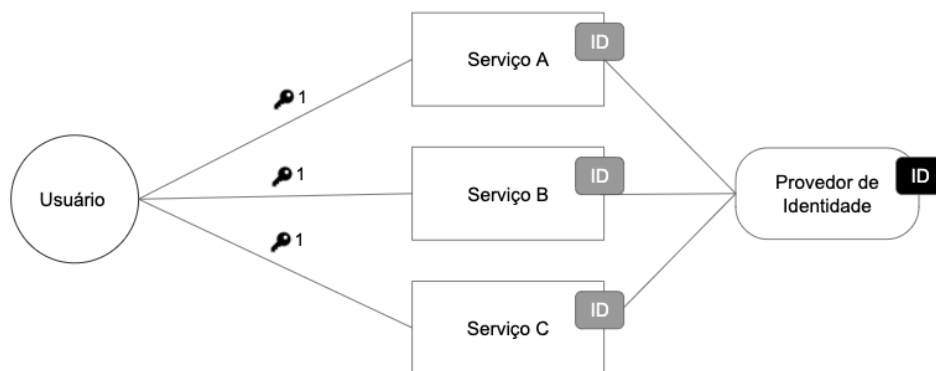


Figura 2.2: Abordagem de identidade centralizada.

Fonte: O autor.

Na centralização a responsabilidade dos provedores de serviço é reduzida em relação ao modelo isolado, porém a existência de um único provedor de identidade faz com que este seja um ponto único de falha do sistema [52]. Do ponto de vista dos usuários a abordagem centralizada melhora o aspecto de gerenciamento de várias senhas, porém mantém sua atuação apenas nos serviços que são alcançados pelo provedor de identidade único [32].

2.4.3 Federada

Na abordagem federada é constituída uma federação de entes confiáveis de forma que uma identidade emitida por um ente federado pode ser utilizada para possibilitar acesso a serviços em qualquer outro ente da federação [51] [53] [22]. Diferentemente da abordagem centralizada, na abordagem federada existem vários provedores de identidade que se filiam em uma federação e possibilitam o uso de credenciais mútuas. A Figura 2.3 ilustra a abordagem federada.

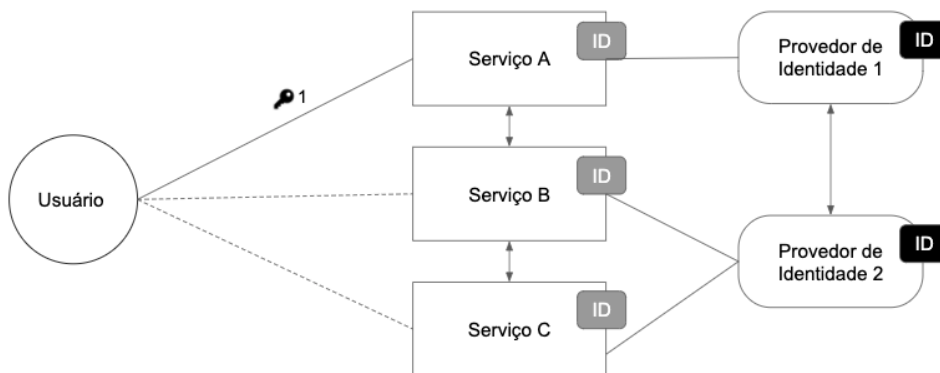


Figura 2.3: Abordagem de identidade federada.

Fonte: O autor.

A abordagem federada ataca um dos problemas da abordagem centralizada, que é o de serviços de diferentes domínios requererem credencial de autenticação distinta e o usuário precisar gerenciar as identidades e credenciais para diversos domínios de serviços [53]. Com a federação é possível que o usuário utilize a mesma credencial de autenticação nos serviços providos pelas entidades da federação [54].

A maior crítica à abordagem federada é que ela, ao invés de conferir poder ao titular da identidade, apenas divide o poder observado na centralização, para um grupo de entes [4]. Outra desvantagem desta abordagem é que com a grande gama de serviços é inevitável que surjam diversas federações e, desta forma, o problema de múltiplas credenciais acaba por se reproduzir, ainda que em menor frequência, no modelo federado [51].

2.4.4 Centrada no Usuário

A abordagem de identidade centrada no usuário é focada em fornecer um repositório de credenciais universal e controlado diretamente pelo usuário [54]. Neste modelo o usuário armazena suas credenciais de diversos serviços ou federações em um único repositório, conhecido como *Personal Authentication Device* (PAD), a credencial deste repositório é suficiente para que faça acesso aos diversos serviços e com os diversos níveis de informações requeridas [51]. A Figura 2.4 apresenta o modelo de identidade centrada no usuário.

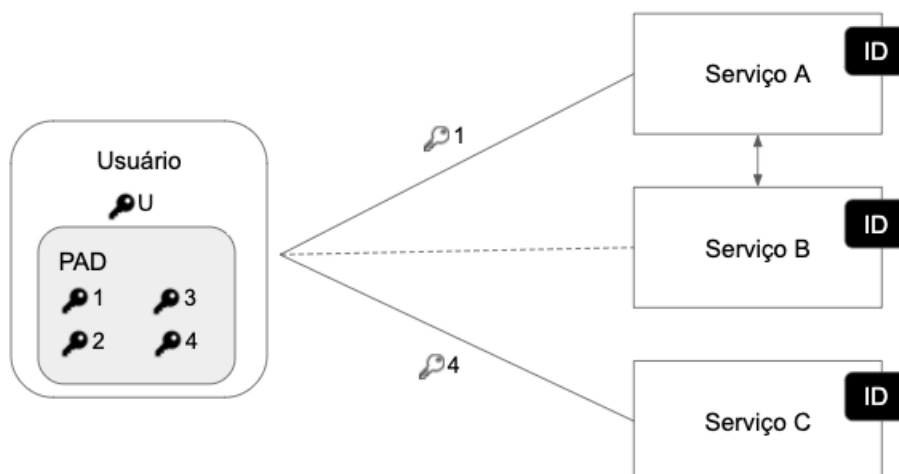


Figura 2.4: Abordagem de identidade centrada no usuário.

Fonte: O autor.

A imagem ilustra as diversas credenciais do usuário armazenadas em seu PAD e sendo este protegido por uma única credencial. Uma vez acessado o PAD, o usuário consegue acesso aos diversos serviços, sejam eles individuais ou federados.

Esta abordagem melhora sensivelmente a experiência de uso dos usuários, uma vez que o controle de diversas credenciais se resume a uma única credencial [51].

Apesar desta abordagem fornecer ao usuário um maior controle sobre suas credenciais, elas ainda pertencem exclusivamente aos serviços e estes serviços ainda continuam com o poder unilateral de revogação destas credenciais[4].

Algumas iniciativas que se destacam na abordagem de identidade centrada no usuário são: OpenID [55], OAuth [56] e FIDO [57].

2.4.5 Auto-soberana (Descentralizada)

O conceito de identidade auto-soberana [4] surgiu a partir da observação de que mesmo na abordagem de identidades centradas nos usuários, em última instância, os provedores ainda detinham o poder sobre as identidades. Para endereçar esta questão, a abordagem auto-soberana propõe o usuário no controle e na posse da sua identidade, não apenas ofertando consentimento sobre o uso dos seus dados, mas se tornando de fato o proprietário destes, sem a intermediação de terceiros [58].

A discussão filosófica à respeito de identidade auto-soberana é ampla e coloca a identidade como intrinsecamente ligada à condição da existência humana, ou seja, se eu existo, logo possuo identidade [4]. O senso comum trata identidade como um processo de individualização, em geral realizada por governos e que confere um documento físico utilizado

para identificar os cidadãos. Já na abordagem auto-soberana, a identidade pertence em sua totalidade ao próprio usuário [59].

Os princípios da identidade auto-soberana buscam fazer do usuário a parte fundamental do processo de identidade. Allen [4] define dez princípios que direcionam a concepção de um sistema de gerenciamento de identidade para o equilíbrio entre transparência, justiça e proteção do indivíduo:

1. Existência: a existência reflete o indivíduo em si e é algo que deriva do simples fato da pessoa existir.
2. Controle: o uso de técnicas de criptografia com o intuito de oferecer ao titular da identidade o controle pleno sobre qualquer interação realizada com seus dados e, até mesmo, que o usuário controle a forma de apresentação dos seus dados.
3. Acesso: o titular deve poder acessar os seus dados a qualquer tempo e sem dificuldade.
4. Transparência: a utilização de padrões abertos, de forma que qualquer pessoa possa inspecionar o funcionamento do sistema de gerenciamento de identidade.
5. Persistência: o sistema de identidades deve perdurar por tempo suficiente até ser tornada obsoleta por um novo sistema de identidades.
6. Portabilidade: o titular deve ser capaz de portar sua identidade entre os provedores disponíveis.
7. Interoperabilidade: a identidade deve ser usada no máximo de sistemas tanto possíveis, de forma a simplificar as interações e promover desenvolvimento.
8. Consentimento: o titular deve ter conhecimento e dar anuência para a utilização de seus dados.
9. Minimalização: a divulgação dos dados deve ser a menor possível, ficando restrita ao indispensável para a prestação de determinado serviço.
10. Proteção: o interesse do titular da identidade deve sempre prevalecer. Em situações de disputa, o titular deve ser privilegiado.

Em geral, as arquiteturas de identidades auto-soberanas se utilizam de uma infraestrutura de chaves públicas para suportar sua operação [58]. O processo de autenticação de um usuário é realizado através da utilização de um par chaves, onde a chave pública

é utilizada para referenciar determinado usuário. Enquanto que a chave privada é mantida secreta e utilizada para assinaturas do usuário. Essa abordagem é conhecida como “Infraestrutura de chaves públicas descentralizadas” [60].

As credenciais verificáveis são um conceito chave em um esquema de identidade auto-soberana e podem representar a versão digital de credenciais no mundo físico. Exemplos de credenciais no mundo físico são: carteira de motorista, carteira profissional e um receituário médico.

Em uma credencial verificável é possível representar exatamente o conceito das credenciais físicas, além de se valer dos benefícios de autenticidade trazidos pelo uso de criptografia, conferindo assim mais confiabilidade. Outro benefício de credenciais digitais é que elas podem transitar de forma mais rápida do que no mundo físico [61]. A Figura 2.5 ilustra as relações em um sistema de credenciais verificáveis.

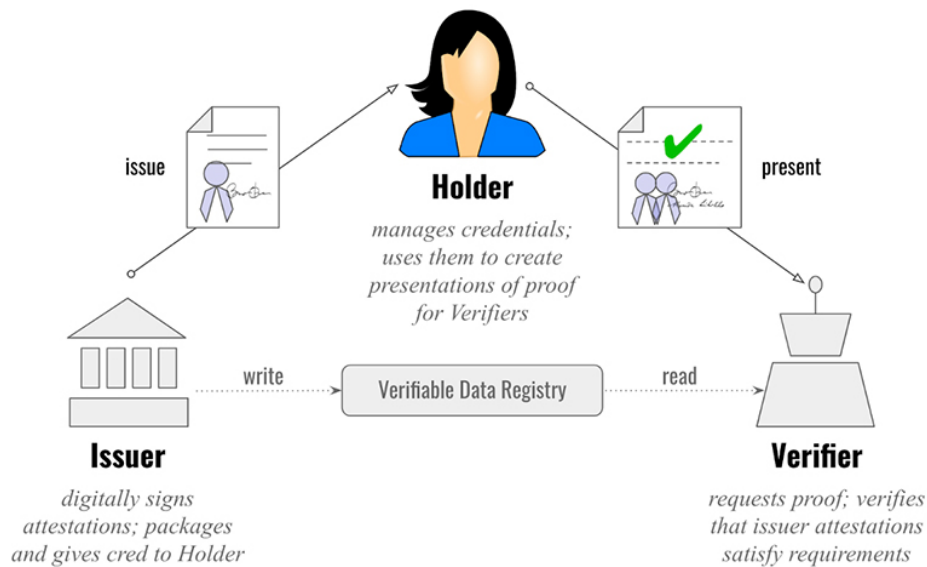


Figura 2.5: Relações em um sistema de credenciais verificáveis.

Fonte: Evernym [62].

Com o surgimento das tecnologias de confiança baseadas em descentralização, como o *blockchain*, a materialização da filosofia de identidade auto-soberana se tornou viável do ponto de vista da tecnologia e a discussão a respeito de implementações práticas deste conceito vêm ganhando força [58].

2.5 Métodos de Autenticação

Os métodos de autenticação fornecem o mecanismo para que os usuários finais possam realizar o processo de identificação em um determinado serviço. Uma grande gama de métodos podem ser aplicados neste processo de identificação do usuário e este trabalho irá apresentar alguns dos métodos de autenticação que são amplamente utilizados em processos de identificação eletrônica.

2.5.1 Senha

O processo de identificação baseado em senhas, que é amplamente utilizado por provedores de identidade (IdP), se caracteriza pela simplicidade de implementação. Ele se tornou um padrão de fato quando se trata de autenticação, porém sofre com problemas de usabilidade e segurança. Da perspectiva de segurança, métodos de autenticação puramente baseados em conhecimento (“*o que você sabe*”) são vulneráveis a diversos tipos de ataque como, por exemplo: adivinhação da senha, ataques de dicionário, captura do que é digitado em um teclado *Key Logger*, observação de terceiros (*Shoulder Surfing*) e engenharia social.

Com a crescente oferta de serviços digitais, os usuários acabam tendo que arcar com a complexidade de conviver com múltiplas senhas, sendo comum o esquecimento destas credenciais [4]. Outro problema relacionado com segurança é a reutilização das senhas em mais de um serviço, fazendo com que o usuário fique mais exposto a ataques, especialmente com os variados episódios de vazamento de senhas. Diversos sites, como *Have I Been Pwned* [63], *MyPwd* [64] e *Leak Check* [65], agrupam senhas vazadas e oferecem ao usuário a possibilidade de verificar se sua senha foi exposta.

2.5.2 Código de Acesso

Códigos de Acesso têm se apresentado como uma eficiente alternativa em processos de autenticação uma vez que se caracterizam por ser um código de uso descartável e, desta forma, seu uso é menos suscetível à ataques do que a autenticação usando senhas. Códigos de acesso único também são conhecidos como *One-Time Password* (OTP) e sua especificação é dada pela RFC 2289 [66]. Atualmente, existem vários protocolos para a geração de OTP, a exemplo de *Simple Hash Function* [67], Yeh-Shen-Hwang (YSH) [68], *HMAC-based One-Time Password* (HOTP) [69] e *Time-based One-Time Password* (TOTP) [70].

Independente do protocolo utilizado, códigos de acesso são vulneráveis a ataques de *phishing* e apresentam limitações em sua abordagem [66]. Códigos gerados a partir do protocolo HOTP são suscetíveis a roubo e, uma vez gerados, não possuem validade limi-

tada [69]. Já o protocolo TOTP é capaz de gerar códigos com validade limitada, porém impede a reautenticação do usuário enquanto o código anterior for válido e sofre com a necessidade de sincronia de tempo entre o cliente e o servidor do código de acesso [70].

Uma preocupação de segurança com os códigos de acesso diz respeito ao canal em que o código de acesso será entregue. É comum a utilização de SMS para a entrega de códigos de acesso, porém Grassi [71] indicou que a utilização de SMS para entrega de OTP não é segura, estando vulnerável a diversos tipos de ataques, entre eles o ataque de Sequestro de SIM Card.

Os códigos de acesso, diferentemente das senhas, não requerem que o usuário memorize de forma permanente nenhuma informação e, desta forma, se apresenta como uma alternativa eficiente de ponto de vista da experiência de usuário.

2.5.3 Biometria

Processos de autenticação de usuários com base em biometria estão se tornando cada vez mais presentes em sistemas computacionais. A conveniência provida por um processo de identificação que requer apenas que o usuário se apresente faz com que esta abordagem seja adotada nos sistemas.

Da perspectiva do usuário, a biometria é um método de autenticação bastante simples de utilizar e que potencialmente gera uma sensação de segurança superior em relação às demais abordagens (senhas e códigos de acesso, por exemplo). De acordo com Jain [72], as biometrias podem ser classificadas como fisiologias e comportamentais. As fisiológicas são as que se apresentam como parte do indivíduo, no grupo das biometrias fisiológicas estão, por exemplo: impressões digitais, íris e face. Já as biometrias comportamentais dizem respeito a como esse usuário interage com o mundo ao seu redor. No grupo das biometrias comportamentais, estão: marcha de caminhada, padrão de digitação e assinatura manual. Uma abordagem com o uso de múltiplas biometrias pode ser aplicada para robustecer o processo de autenticação.

A utilização de dados biométricos requer atenção especial na manipulação e custódia dos dados por parte dos IdP. Os diversos regulamentos de proteção de dados como GDPR [40] e LGPD [18] categorizam dados biométricos como informação sensível e, desta forma, requerem um alto grau de atenção e proteção dos dados manipulados. No caso da LGPD, em seu artigo 11, são apresentadas as condições para que seja realizado o tratamento de dado sensível e apresenta, dentre outras obrigações, a de que dado biométrico requer o consentimento explícito e específico do titular, com finalidade de uso bem definida.

2.5.4 Duplo Fator de Autenticação (2FA)

Uma abordagem que vem sendo utilizada para melhorar a segurança nos processos de autenticação é a implementação de Duplo Fator de Autenticação (2FA), como forma de complementar a utilização da senha. A estratégia de utilizar mais de um fator de autenticação visa robustecer o processo e prover uma maior confiança de que determinado usuário é de fato quem se diz ser. Apesar de incrementar a segurança no processo de identificação, o uso de 2FA pode prejudicar a usabilidade, uma vez que é requerido um maior esforço do usuário, que deve se submeter a uma autenticação em duas etapas.

Implementações da indústria que utilizam 2FA não são novidade, o Google já oferece este recurso desde 2011 e ainda não conta com uma adesão massiva. De acordo com Grzegorz [73], em 2018 menos do que 10% das contas do Google utilizavam 2FA. Entretanto, o Google está em um esforço para a adoção massiva de 2FA e pretende tornar este o padrão para autenticação em seu provedor de identidade [74]. No Brasil o projeto Acesso Gov.br, um IdP provido pelo Governo Federal Brasileiro, possibilita o uso de 2FA e conta com cerca de 8% do total das contas com o recurso de 2FA habilitado [20].

De modo geral, as implementações de 2FA utilizam a senha em conjunto com um código de acesso, porém não é uma limitação a utilização destes fatores. Abordagens de autenticação que se utilizam de mais de um fator, também conhecidas como Múltiplos Fatores de Autenticação (MFA), e neste caso, diferentemente de 2FA, podem ser utilizados N fatores de autenticação, como: senhas, código de acesso, biometrias físicas, comportamentais, reconhecimento de padrões, reconhecimento de imagens, entre outros.

2.6 Metodologia de Pesquisa

É crescente o número informações produzidas pela sociedade e o fluxo de informação é cada vez mais facilitado, rápido e acessível. As tecnologias reduzem a barreira da conectividade e potencializam o trânsito de informação. Este cenário acaba por se refletir em um aumento exponencial do número de publicações científicas e, se por um lado é muito rico que se tenha um grande volume de publicações, por outro se torna mais árdua a tarefa de encontrar informações relevantes e de qualidade a respeito de determinado tema. Em um processo de pesquisa é importante se inserir em um contexto de publicações acadêmicas representativas do objeto de estudo, visando encontrar os principais autores, estudos e conhecer as principais abordagens acerca do tema estudado.

Uma abordagem muito comum para realizar a revisão da literatura de determinado tema é através da revisão narrativa, conhecida também como exploratória [75]. Uma desvantagem deste tipo de revisão é a condução apenas pela percepção direta do pesquisador e de forma não estruturada. Já a abordagem sistêmica é realizada com maior rigor

metodológico, buscando reduzir a subjetividade com a aplicação de critérios objetivos e, por conseguinte, a seleção dos materiais científicos a serem estudados [76].

A revisão sistemática conduz o estudo direcionando para obter uma visão geral de determinada área de pesquisa e identificar quais estudos possuem relação com uma questão de pesquisa definida [77]. Um processo de mapeamento sistemático é capaz de identificar e categorizar pesquisas disponíveis para um tema específico, fornecendo um panorama dos principais estudos e áreas de interesse dentro de determinado tema [78].

No contexto das revisões sistêmicas, se apresenta o enfoque meta-analítico com o objetivo de fornecer uma revisão bibliográfica para o levantamento do estado da arte de um determinado assunto. Uma derivação do enfoque meta-analítico é a denominada de Teoria do Enfoque Meta Analítico Consolidado (TEMAC) [76], que foi aplicada neste trabalho e que visa apresentar uma visão geral dos trabalhos realizados sobre um determinado tema. Na sequência são apresentadas as fases da abordagem TEMAC utilizadas neste trabalho.

2.6.1 Preparação da Pesquisa

A preparação da pesquisa se iniciou com a definição do espaço temporal a ser avaliado, considerando as seguintes situações: i) o volume de publicações sobre o tema e as evoluções tecnológicas; ii) a popularização dos smartphones e a consequente mudança na forma de interação dos usuários com a tecnologia [79]; iii) a franca expansão do acesso à internet banda larga [80]; foi definido que a pesquisa se iniciaria a partir do ano de 2009, constituindo assim uma janela de pouco mais de 10 anos.

O próximo passo na etapa de Preparação da Pesquisa é a definição das bases de dados a serem exploradas. Nesta dissertação, as bases de dados escolhidas foram *Web of Science* e *Scopus*, pois tratam-se de plataformas de pesquisa consolidadas e bem conceituadas na comunidade acadêmica. Além disso, agrega-se o fato de serem bases de dados que contam com classificação do conteúdo por metadados, o que possibilita ampliar a gama de análises dos resultados da pesquisa.

Uma vez definidas as bases, foram definidas as áreas de conhecimento a serem inspecionadas. Nesta dissertação, foram filtrados os resultados categorizados na área de conhecimento Ciência da Computação (*Computer Science*), uma vez que se trata de um estudo com foco na referida área.

O último passo desta etapa foi a consolidação dos critérios de inclusão e exclusão do estudo. Os critérios de inclusão foram:

- I.1) Estudos escritos entre os anos de 2009 e 2021.
- I.2) Escritos em língua portuguesa ou inglesa.
- I.3) Texto completo do trabalho contido nas bases pesquisadas.

Já os critérios de exclusão foram:

- E.1) Estudos incompletos e resumos estendidos.
- E.2) Estudos não focados em IdM.
- E.3) Estudos não focados na perspectiva do usuário final.
- E.4) Estudos que não contém resumo ou abstract.

2.6.2 Apresentação e Interrelação dos Dados

Uma vez finalizada a etapa de Preparação da Pesquisa, se inicia a etapa de Apresentação e Interrelação dos Dados, com a verificação das palavras-chave envolvidas na pesquisa. Nesta etapa, o objetivo foi verificar se os estudos recuperados tratavam da temática desta pesquisa. A Figura 2.6 apresenta uma nuvem de palavras com a representação das palavras-chave constantes em todos os documentos recuperados por esta pesquisa. Para a construção da nuvem de palavras foi utilizado o software TagCrowd [81].



Figura 2.6: Nuvem de Palavras.

Gerado pelo software TagCrowd.

A observação da nuvem de palavras reforça que, em sistemas de IdM, a autenticação e o gerenciamento de credenciais são fatores preponderantes e estão intimamente ligados à aplicação de criptografia, com enfoque na segurança, proteção e privacidade dos dados dos usuários. São destaque também as abordagens baseadas em nuvem e dispositivos móveis.

2.6.3 Detalhamento e Compilação dos Trabalhos Recuperados

Uma vez realizado o levantamento bibliográfico, o passo seguinte foi a leitura dos resumos dos trabalhos recuperados na pesquisa com o intuito de selecionar os artigos que mais apresentassem relação com o tema central da presente dissertação, ou seja, os artigos que mais diretamente tratassem de sistemas de gerenciamento de identidade eletrônica.

Considerando a base Web of Science, foram inicialmente levantados 271 artigos científicos. Após a leitura dos resumos destes artigos e, considerando o alinhamento ao tema principal deste trabalho, identidade eletrônica, foram selecionados 29 artigos para maior aprofundamento.

Já para a base Scopus foram inicialmente listados 492 artigos. Após as mesmas análises preliminares, restaram 46 artigos para avaliação detalhada. Assim, a base de artigos para verificação detalhada contou com 75 artigos.

Após a avaliação dos artigos e com um melhor embasamento sobre a temática de IdM, foram realizadas pesquisas exploratórias nas bases Google Scholar, IEEE Xplore, ACM e DBLP de forma a complementar o referencial teórico dos assuntos abordados neste trabalho.

2.7 Trabalhos Relacionados

O trabalho de Ferdous e Poet [82] realiza uma análise comparativa entre implementações de sistemas de gerenciamento de identidade com relação ao seguinte conjunto de atributos: requisitos funcionais, segurança, privacidade, interoperabilidade, confiabilidade, conformidade legal, requisitos de usabilidade e acessibilidade. Uma das conclusões do trabalho de Ferdous e Poet é que nenhuma das implementações inspecionadas pode ser considerada ideal, uma vez que não contemplam plenamente os atributos investigados e é improvável que uma única abordagem de IdM possa ser plena a ponto de se consolidar como um padrão de fato, sendo necessária a elaboração de informações comparativas sobre as abordagens, de forma que os gestores de um sistema de IdM possam ponderar qual a melhor estratégia para resolver determinado problema.

Um extenso trabalho sobre métodos de autenticação candidatos a substituição de senhas foi apresentado por Bonneau [10] e, neste foram inspecionados aspectos de segurança, usabilidade e viabilidade de implantação. Ainda segundo Bonneau, diversas abordagens promovem incremento de segurança no processo de autenticação, porém acabam por sacrificar a usabilidade ou a viabilidade de implantação. O referido autor afirma que nenhum esquema de autenticação supera o esquema baseado em senha no que se refere à viabilidade e ao custo de implantação. O trabalho de Bonneau é focado em métricas técnicas e contribui com a apresentação de critérios objetivos que podem ser aplicados para a

avaliação de métodos de autenticação, como por exemplo: esforço de memorização de uma credencial ou esforço de portar um dispositivo criptográfico. Uma lacuna observada no trabalho é o fato de não focar em verificar a percepção dos usuários finais sobre os métodos de autenticação.

Duston [83] realizou uma pesquisa com membros da Universidade Brigham Young, Utah, Estados Unidos, que adotou duplo fator de autenticação baseado no provedor de serviços Duo [84]. O Duo oferece diferentes formas de implementação para 2FA, como: OTP, ligações telefônicas, senhas e chaves de segurança em hardware, está última utilizando soluções como YubiKey [85] e Titan [86]. A partir da pesquisa, Duston observou que a maioria dos usuários considera que a implementação de 2FA 2.5.4 aumentou a sensação de segurança, porém não foi conclusiva a análise a respeito da sensação dos usuários com respeito à usabilidade, uma parte dos usuários observados classificou a usabilidade como boa, enquanto que outro grupo considerou que o processo com 2FA foi significativamente pior. Duston observou ainda que o processo de informação e capacitação dos usuários é um fator importante na experiência de uso percebida.

Os trabalhos de Chen [87] e Shan [88] apresentam uma abordagem de autenticação onde é traçado um perfil do usuário, se baseando em uma série de características coletadas nos processos de autenticação realizados por este usuário, como exemplo: endereços IPs utilizados, geolocalização, horário dos acessos. Após a definição do perfil, o método de autenticação a qual o usuário vai ser submetido é escolhido de acordo com um nível de confiabilidade de que se trata do usuário em questão. Esta abordagem de autenticação oferece uma experiência de uso facilitada para os usuários finais que se enquadram no perfil de confiável, por outro, para que seja possível definir o perfil do usuário, é necessário coletar diversas informações pessoais, se configurando como um desafio relacionados à privacidade.

Sae-Bae [89] apresentou processos de autenticação baseados em *Natural User Interface* (NUI), ou seja, interfaces naturais do usuário que potencializam comportamentos naturais e intuitivos, como o toque, o gesto, a fala e o olhar. Essencialmente é considerado um processo de autenticação biométrica utilizado em situações em que o uso de dispositivos como teclado ou mouse são desaconselháveis, a exemplo de uma sala de cirurgia. Sae-Bae observou que, do ponto de vista de experiência de uso, as abordagens de autenticação baseadas em NUI são bem recebidas pelos usuários, porém desafios relacionados ao ambiente externo, como luminosidade ou ruídos comprometeram a acurácia.

A Tabela 2.1 apresenta uma síntese dos trabalhos correlatos apresentando a principal temática abordada em cada um deles.

Título do trabalho e autores	Temática
A comparative analysis of Identity Management Systems. (Ferrous, Md. Sadek and Poet, Ron)	Atributos de um sistema de IdM
The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. (Bonneau, Joseph and Herley, Cormac and Oorschot, Paul C. van and Stajano, Frank)	Métricas para comparação técnica de métodos de autenticação
Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication (Dutson, Jonathan and Allen, Danny and Eggett, Dennis and Seamons, Kent)	Duplo de fator de autenticação e a percepção dos usuários finais
Continuous Authentication Based on User Interaction Behavior (Chen, Long and Zhong, Yi and Ai, Weidong and Zhang, Difang)	Autenticação contínua e baseada em risco
Automated Login Method Selection in a Multi-modal Authentication System: Login Method Selection based on User Behavior (Shan, Chang Pei and Hon Loon, Wong and Win, Lee Kay And Din, Dahlia and Seak, Sea Chong)	Autenticação contínua e baseada em risco
Emerging NUI-Based Methods for User Authentication: A New Taxonomy and Survey (Sae-Bae, Napa and Wu, Jonathan and Memon, Nasir and Konrad, Janusz and Ishwar, Prakash)	Autenticação baseada em biometria com interfaces naturais

Tabela 2.1: Temática dos trabalhos relacionados.

Fonte: O autor.

É possível observar que diversas iniciativas visam fornecer uma solução de autenticação alternativa para o uso das senhas, porém muitas delas focam apenas no aspecto da segurança e desconsideram a experiência de uso, fazendo com que se tenha baixa adesão por parte do usuário e que o método não logre o sucesso pretendido. Métodos baseados em biometria são promissores, porém desafios relacionados à acurácia e à privacidade fazem com que estas abordagens ainda careçam de evolução. Este trabalho busca preencher uma lacuna identificada que diz respeito a percepção dos usuários finais sobre os métodos e formas de autenticação. Investigar a aceitação por parte dos usuários e buscar o equilíbrio com aspectos de segurança e privacidade é um desafio posto para a academia e a indústria que tratam do assunto IdM.

Capítulo 3

Percepção dos Usuários de Serviços de Autenticação

Esta seção destina-se à investigação das crenças dos usuários quando apresentados à sentenças a respeito de métodos de autenticação. Ter o diagnóstico de como pensa o usuário final, possibilita que o serviço digital entregue uma solução mais direcionada para estes usuários e, conseqüentemente, aumenta as chances de um determinado serviço ser adotado [5], especialmente nos cenários em que a utilização do serviço não se trata de uma obrigação do usuário.

É comum que os gestores de serviços digitais definam os critérios de autenticação orientados, majoritariamente, pelo critério de segurança, o que inicialmente parece uma decisão acertada, dado que se trata de um pilar fundamental em sistemas de IdM [30] [31]. O contraponto é que, em alguns cenários, o nível elevado de segurança faz com que os usuários não adotem determinado serviço e, quando o fazem, utilizam práticas indevidas que comprometem a segurança pretendida [90] [91]. Um exemplo dessa situação é a má prática de compartilhamento de dispositivos físicos pessoais, como *tokens* ou cartões inteligentes. Um outro exemplo diz respeito à cópia e ao compartilhamento de uma senhas.

A Seção 3.1 apresentará o método aplicado neste trabalho, que objetiva capturar a percepção dos usuários sobre sistemas de IdM a partir da avaliação de sentenças sobre a relação do usuário final com métodos de autenticação e gerenciamento de credenciais. A discussão dos resultados obtidos e as limitações do trabalho são apresentados nas Seções 3.2 e 3.3, respectivamente.

3.1 Método Aplicado

O método aplicado neste estudo compreende a elaboração e a aplicação de um questionário com o objetivo principal de investigar a crença dos indivíduos em relação a soluções de

identificação para acesso a serviços on-line. Estes aspectos foram selecionados por serem considerados fundamentais para que uma solução de IdM conte com maior probabilidade de adesão dos usuários e consequente manutenção e longevidade da solução [5] [19].

Uma vez definido o objetivo principal, foi identificada a população-alvo a ser abordada. Considerando o propósito desta pesquisa, foi definido que as unidades de análise deveriam ser profissionais de Tecnologia da Informação (TI) e não profissionais de Tecnologia da Informação. A escolha por estas unidades visou investigar se maior fluência com TI se reflete em diferenças de crenças e atitudes com relação a soluções de identificação digital.

Após a definição das unidades de análise, foi elaborado o projeto de amostragem. Considerando que este trabalho é focado em sistemas de IdM e que estes são utilizados por diversos setores da sociedade, optou-se por utilizar uma abordagem aleatória, não probabilística. Este tipo de amostragem é caracterizada pela utilização do critério de conveniência para a seleção das amostras e é comum a sua utilização em pesquisas de Engenharia de Software [92]. O convite para os entrevistados seu deu por meio de contatos pessoais e o método de levantamento foi o de questionário web, distribuído através de redes sociais e e-mail.

O passo seguinte na estruturação do questionário foi a definição do formato de questão a ser adotado. Por se tratar de uma pesquisa quantitativa e com característica de levantamento, foram utilizadas questões fechadas. Já para as respostas, foi utilizada a escala Likert [93], visando determinar a intensidade e a frequência de uma opinião ou comportamento [94]. Foram elaboradas sentenças afirmativas e as opções de respostas variam entre os valores um e cinco, indicando a intensidade da concordância com a afirmação. O valor 1 (um) indica discordância forte e o valor 5 (cinco) concordância forte.

A sequência de elaboração do questionário se deu com a identificação das questões demográficas, que descrevem características do respondente. A preocupação com a privacidade de dados esteve presente neste trabalho e, por este motivo, as questões foram definidas visando capturar apenas as informações relevantes para o trabalho em curso, observando os princípios de *privacy by design* [95]. As questões demográficas presentes no trabalho estão relacionadas à faixa etária, gênero, nível de formação e área de atuação, totalizando quatro questões. Tais perguntas visam identificar eventuais padrões comportamentais pertencentes aos agrupamentos gerados pelas respostas.

Definidas as questões demográficas, a etapa seguinte foi a de definição das sentenças que visam identificar a intensidade das crenças dos respondentes frente às afirmações apresentadas no questionário. As sentenças foram elaboradas de forma a observar a percepção dos usuários perante os mecanismos de autenticação comumente utilizados em sistemas de IdM, tais como: i)senha, ii)biometria e iii)código de acesso único e estão apresentadas a seguir.

Sentença 1: "Você se sente confortável com o processo de login utilizando nome de usuário e senha."

A primeira sentença tem o intuito de verificar o grau de aceitação dos respondentes com relação à autenticação em sistemas de identidade que são baseados em login e senha.

Sentença 2: "Frequentemente esqueço das minhas senhas nos serviços on-line."

A segunda sentença busca contrapor a eventual popularidade dos sistemas de IdM baseados em senha e apresenta a frequência com que os usuários esquecem suas senhas. O esquecimento da senha é um dos principais problemas de usabilidade e segurança verificados em sistemas de autenticação baseados em login e senha e, em boa parte deles, é derivado de sistemas de IdM com característica centralizada, onde o usuário precisa conviver com diversas senhas para acesso a variados serviços [82].

Sentença 3: "Utilizo a mesma senha em mais de um serviço."

Esta sentença busca avaliar o comportamento dos usuários sobre a prática de repetição de senha em mais de um serviço. A princípio é uma prática que emula uma melhora na usabilidade, porém reduz a segurança uma vez que, utilizando a mesma senha em mais de um serviço, a superfície de ataque é expandida e uma vazamento de senha compromete o usuário em mais de um serviço.

Sentença 4: "Acho imprudente repetir a mesma senha em mais de um serviço."

A quarta sentença visa obter a opinião do usuário em relação à redução da segurança causada pela repetição da mesma senha em mais de um serviço.

Sentença 5: "Costumo manter uma cópia das minhas senhas em outros locais (por exemplo: papel, editor de texto, serviço de nuvem)."

Um aspecto relevante na segurança de processos de autenticação baseados em senha é como os usuários armazenam suas credenciais de acesso. Assim, a quinta sentença busca investigar se os usuários praticam uma medida de segurança não recomendada: manter uma cópia de suas senhas armazenadas em algum meio diferente da própria memória ou de um sistema especializado.

Sentença 6: "Costumo utilizar softwares gerenciadores de senhas."

A sexta sentença visa investigar se os usuários utilizam softwares especializados em realizar a guarda de credenciais, conhecidos como software gerenciadores de senha. Alguns exemplos destes software são: LastPass [96], 1Password [97], DashLane [98] e os

gerenciadores de senha contidos nos principais navegadores de internet (Google Chrome, Mozilla Firefox e Microsoft Edge) e sistemas operacionais (Windows, Linux e MAC OS).

Sentença 7: "Softwares gerenciadores de senhas são confiáveis."

Além da eventual utilização de um software gerenciador de senha, outro aspecto a ser avaliado é o grau de confiança que os usuários têm sobre a segurança em utilizar estes serviços, especialmente considerando que softwares gerenciadores de senha entregam para o usuário final uma experiência de uso mais facilitada, pois o usuário não precisa fazer o esforço de memorizar suas diferentes senhas nos variados serviços.

Sentença 8: "Considero mais seguro fazer login em um serviço utilizando um código aleatório encaminhado por e-mail e/ou SMS do que fornecer uma senha."

Seguindo a linha de eventual incremento na relação entre segurança e usabilidade, a oitava sentença avalia o comportamento dos usuários em relação a mecanismos de autenticação baseados em códigos de acesso único, comumente conhecidos como One-Time Password (OTP). O uso de OTP elimina a necessidade de memorização de uma senha, porém requer um canal de comunicação para a entrega do código único, como por exemplo e-mail ou SMS.

Sentença 9: "O acesso a serviços por meio de impressões digitais e reconhecimento facial torna o processo de login mais seguro."

A nona sentença busca avaliar a crença dos respondentes a respeito de um eventual incremento de segurança percebida pelos usuários quando dados biométricos são utilizados no processo de autenticação.

Sentença 10: "O acesso a serviços por meio de impressões digitais e reconhecimento facial torna o processo de login mais simples e conveniente."

Já a décima sentença busca avaliar a crença dos usuários quando se trata do aspecto de simplicidade e conveniência, considerando o uso de dados biométricos durante a autenticação.

Sentença 11: "Me preocupo mais com o vazamento de um cadastro de impressões digitais e reconhecimento facial do que com o vazamento de uma senha."

A décima primeira sentença é direcionada para verificar a percepção dos usuários a respeito da preocupação com o vazamento de dados biométricos em comparação com o

vazamento de credenciais baseadas em senha.

Considerando que a biometria é uma tendência nos processos de autenticação e, que por ser decorrente de uma característica física do usuário, elimina a necessidade de esforço de memorização de senha ou da necessidade de posse de código ou dispositivo de acesso. Uma questão relevante quando se trata de sistemas baseados em biometria é a privacidade, uma vez que dados biométricos são dados sensíveis e requerem controles ainda mais efetivos com a guarda e blindagem contra vazamentos de dados, conforme abordado nas leis de privacidade e proteção de dados LGPD [18] e GDPR [40]. Esta forma de autenticação, quando utilizada como único fator de verificação, se configura como um risco de segurança de alto impacto, pois o dado biométrico, diferentemente de uma senha ou código único, não pode ser substituído.

Uma vez definida a composição do questionário, foi elaborado o Termo de Consentimento Livre e Esclarecido (TCLE), disponível no Apêndice A. O termo explicita o objetivo da pesquisa, a condição de anonimato dos respondentes e a confidencialidade das respostas. O TCLE se baseou no termo elaborado para a pesquisa social de avaliação das atividades da UnB (Avaliação das Atividades Letivas do 1/2020) [99]. O Apêndice B apresenta o formulário do questionário aplicado.

O questionário estruturado foi aplicado no período de 21/01/2021 a 31/01/2021. Os resultados coletados foram analisados com o olhar de captar as percepções dos usuários entrevistados e, os resultados são apresentados e discutidos da Seção 3.2

3.2 Resultados e Discussão

O questionário aplicado atingiu um total de 132 respondentes, sendo que a distribuição deles ocorreu na proporção de 2/3 de não profissionais de TI, ou seja, 31,1% respondentes. Os respondentes que se declararam como mais identificados com o gênero feminino foram 54,5%. Os que possuem pós-graduação foram 60% e 50% pertencem à faixa etária dos 25 aos 39 anos. A Figura 3.1 apresenta um compilado dos resultados das questões demográficas.

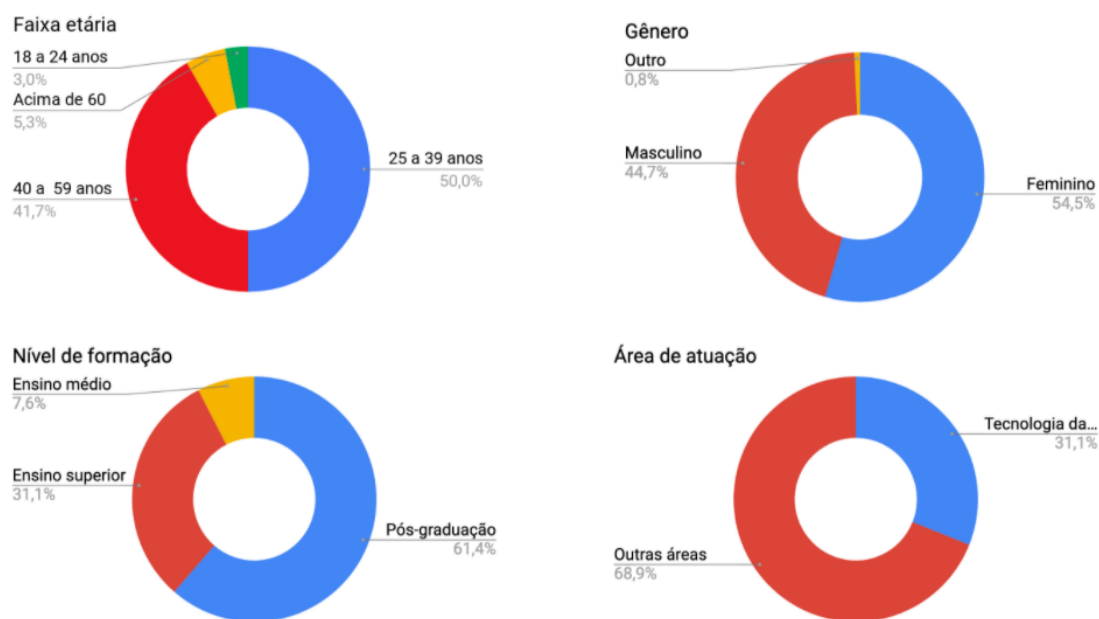


Figura 3.1: Resultado das questões demográficas.

A utilização de uma amostragem aleatória e a observação das respostas às questões demográficas indicam que os resultados obtidos podem apresentar algum viés. Uma discussão mais ampla sobre as limitações deste estudo é encontrada na Seção 3.3.

A análise das respostas às questões aponta que os profissionais de TI se sentem menos confortáveis com o uso de senha quando comparados com os não profissionais de TI, conforme ilustrado na Figura 3.2. Tal comportamento pode ocorrer pelo fato de que profissionais de TI possuem um maior conhecimento em relação às fragilidades apresentadas em processos de autenticação que se utilizam de modelos baseados em login e senha (Seção 4.1.2.1). Ainda assim, é observado que, majoritariamente, em ambos os grupos, profissionais de TI e não profissionais de TI, o uso de autenticação baseada em senha é percebido como confortável por parte dos usuários. A facilidade e a familiaridade com esta forma de autenticação são fatores que podem contribuir para o resultado apresentado.

A partir dos resultados da Sentença 2: "**Frequentemente esqueço das minhas senhas nos serviços on-line.**", com relação ao esquecimento de senhas, os profissionais de TI esquecem menos a senha do que os demais usuários (Figura 3.2), e isso pode ser em decorrência do fato de que profissionais de TI operam durante mais tempo no meio digital e, por conseguinte, se relacionam mais vezes com os serviços que requerem autenticação com login e senha. O esforço de memorizar a senha é um dos principais aspectos negativos dessa abordagem e as soluções de IdM buscam evoluir os mecanismos de redefinição de senha de forma a tornar a experiência percebida pelo usuário mais agradável durante este processo. Neste sentido, um desafio que se apresenta é o de garantir mecanismos de

segurança adequados para que seja possível redefinir a senha sem um processo que onere muito o usuário.

A reutilização de senhas é um traço comum em ambos os grupos, mesmo sendo uma prática inadequada no que diz respeito à segurança [10], conforme apresenta a Figura 3.2, derivada da Sentença 3. Quando nos deparamos com uma grande gama de serviços é comum que o usuário, e de certa forma natural, mantenha a mesma senha [82].

Considerando que a maioria das soluções operam em uma abordagem de IdM isolada, a senha dos usuários é espalhada por diversos provedores de serviços, ampliando a superfície de potenciais ataques de roubo de identidade. O grupo de profissionais de TI reconhece que é imprudente a reutilização de senha, entretanto o grupo de não profissionais de TI se apresenta como neutro em relação a esta questão (Figura 3.2, Sentença 4). Ainda assim, ambos os grupos são adeptos desta prática. A neutralidade observada pelo grupo de não profissionais de TI indica que estes usuários podem desconhecer o funcionamento dos sistemas de IdM e as implicações decorrentes de um eventual vazamento de senha. Essa percepção reforça a necessidade dos provedores de identidade se preocuparem com o aspecto de segurança e com a implementação de controles que visem atestar com maior efetividade que um determinado usuário de fato é quem diz ser.

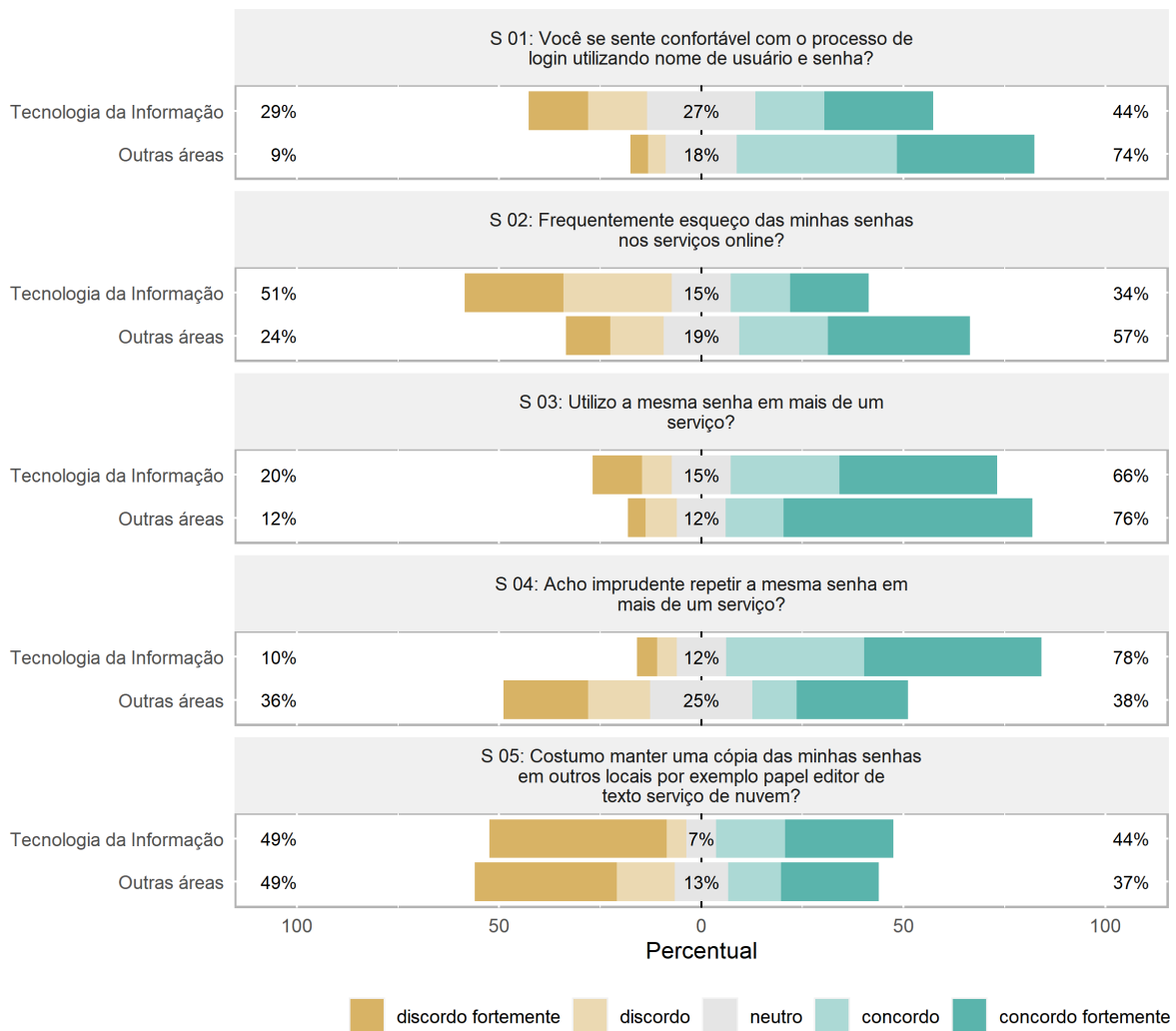


Figura 3.2: Resultado do questionários para as Sentenças 1 a 5.

Softwares gerenciadores de senha buscam criar uma abstração de um *Single Sign-On* (SSO), se apresentando como umas das soluções para os usuários finais no cenário de gerenciamento de diversas credenciais baseadas em senha. Em geral, estes softwares são capazes de armazenar em um banco de dados a relação de credenciais de um usuário. Existem diversas abordagens para estes softwares e, a mais popular, é a de armazenamento das credenciais criptografadas na nuvem, onde é comumente utilizada criptografia simétrica derivada de uma chave mestra criada pelo próprio usuário. Os dados são criptografados localmente e, depois, trafegam até a nuvem do serviço de gerenciamento de senhas, onde são armazenadas, possibilitando que o usuário tenha acesso a suas credenciais a partir de diferentes dispositivos.

A depender do algoritmo de criptografia utilizado pela solução de gerenciador de senhas, um eventual vazamento ocorrido do lado do servidor não deveria comprometer imediatamente a segurança dos usuários. Em geral, é utilizado o algoritmo *Advanced*

Encryption Standard (AES) com chave de 256 bits. Na abordagem de softwares gerenciadores de senha o elo fraco fica sendo a senha mestre do usuário final, uma vez que o comprometimento desta senha imediatamente leva a um comprometimento de todas as credenciais armazenadas.

As respostas às Sentenças 6 e 7, indicam que softwares gerenciadores de senhas são pouco conhecidos e, por conseguinte, pouco utilizados entre os entrevistados, tal desconhecimento se reflete na confiabilidade declarada a respeito destes softwares.

Na Sentença 8, observou-se que ambos os grupos (profissionais e não-profissionais de TI) percebem que o processo de autenticação utilizando um código de acesso aumenta a sensação de segurança do usuário e não é observada resistência quanto à adoção desta estratégia de identificação. A adoção de códigos de acesso tem se difundido e cada vez mais soluções adotam esta estratégia em seus processos de autenticação. A maior parte dos IdP utilizam estes códigos como um segundo fator de autenticação, buscando elevar o grau de segurança do processo, porém desconsideram que a experiência do usuário final fica prejudicada. Os códigos de acesso são bem vistos pelos usuários pelo fato de não requererem esforço de memorização e, a depender da forma de entrega do código, também dispensam o esforço de portar algum dispositivo adicional como, por exemplo, um gerador de token.

As duas unidades de análise deste estudo, profissionais de TI e não profissionais de TI, indicaram que o uso de biometria torna o processo de autenticação mais seguro, simples e conveniente, conforme apresenta a Figura 3.3, baseada nas respostas das Sentenças 09 e 10. A autenticação com uso de biometria se baseia em informações do “que você é” e não requer nenhum esforço de memorização por parte dos usuários finais, como ocorre com as senhas. De forma complementar, biometria não requer ao usuário portar um dispositivo de segurança em hardware, como pode ser os casos de código de acesso. Apesar do grupo de profissionais de TI considerar mais grave o vazamento de dados biométricos, este grupo se mostrou propenso à utilização de autenticação baseada em biometria.

Episódios de vazamentos de dados e credenciais são cada vez mais frequentes [100] [101] e, sistemas de IdM que utilizam a biometria como único fator de acesso cometem uma grave falha de segurança e privacidade dado que, se forem vazadas as informações biométricas do usuário, não será possível redefinir esta credencial e, por conseguinte, todo o sistema de IdM é comprometido. A abordagem de biometria como único fator de acesso é bastante comum em sistemas de IdM de controle predial.

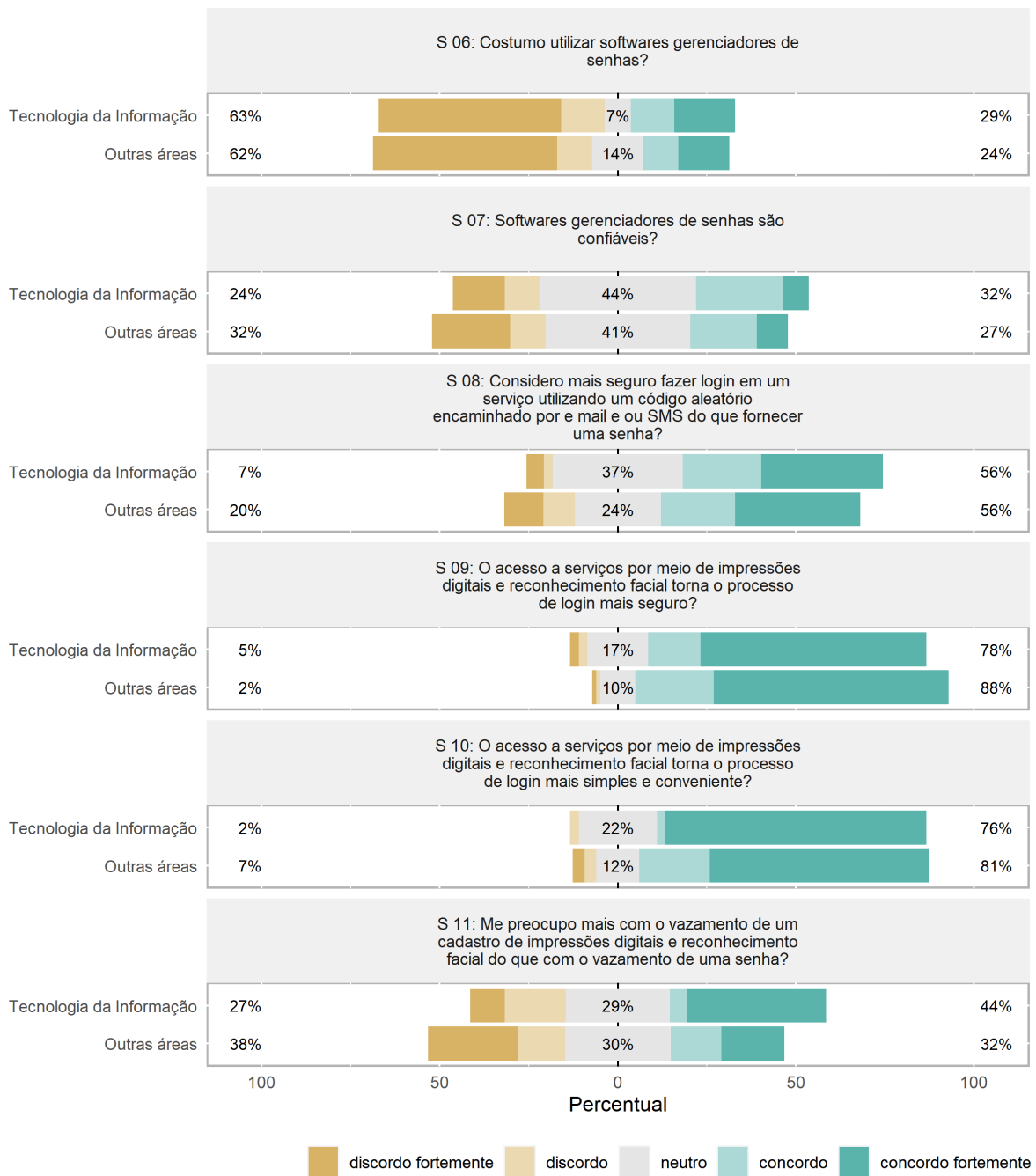


Figura 3.3: Resultado do questionários para as Sentenças 6 a 11.

A análise dos resultados do ensaio realizado aponta que os usuários de sistemas on-line valorizam com maior intensidade o aspecto da experiência de uso da solução de identificação, independente do usuário ser ou não um profissional de TI. Os aspectos de segurança, proteção e privacidade de dados são menos percebidos na perspectiva do usuário final. Tal constatação, reforça o imprescindível compromisso dos provedores de identidade com relação à segurança e à privacidade, uma vez que são pilares importantes

no estabelecimento de um efetivo sistema de IdM. O desafio posto é o de se encontrar um equilíbrio adequado entre as dimensões segurança, privacidade e usabilidade.

O ensaio realizado não evidenciou, nas questões abordadas no questionário, uma divergência clara em relação à percepção dos profissionais de TI quando comparados com a percepção dos usuários que não são profissionais de TI e, as características demográficas também não alteraram de forma significativa o resultado apresentado no ensaio. As limitações ao ensaio realizado são apresentadas na Seção 3.3

3.3 Limitações e Ameças

O ensaio realizado com o uso de questionário, contou com uma seleção amostral aleatória e não probabilística, realizada a partir de contatos de redes sociais e e-mail, não sendo possível determinar o nível de fluência dos respondentes no tema abordado, sendo assim, inerentemente apresenta um grau de viés nos resultados encontrados. A replicação deste mesmo experimento em uma nova rodada amostral poderá apresentar resultados divergentes, desta forma os resultados encontrados não devem ser encarados como generalizáveis, o que não desqualifica os achados, mas zela para que medidas precipitadas não sejam aplicadas.

Para análise dos resultados dos ensaios não foram utilizadas medidas como Alfa de Cronbach, uma vez que o contexto se trata de questões que refletem crenças e opiniões dos entrevistados. Do ponto de vista estatístico, não se percebe adequado buscar um número global para reflexo de eventual confiança do instrumento. Os resultados apresentados configuram um cenário que aponta uma possível direção sobre a percepção dos usuários no que diz respeito ao processo de autenticação em sistemas de IdM.

3.4 Síntese do Capítulo

Este capítulo apresentou o método para elaboração, a aplicação e os resultados de um questionário com usuários finais de sistemas de IdM. O objetivo principal do questionário foi investigar a crença dos respondentes em relação a soluções de identificação para acesso a serviços on-line, considerando aspectos como segurança, privacidade e experiência de uso. As unidades de análise foram os profissionais de TI e os não profissionais de TI e a seleção das amostras foi realizada de forma aleatória e não probabilística. A partir dos resultados obtidos, foi observado que não existe significativa divergência nas respostas apresentadas pelas unidades de análise e que, na percepção dos usuários finais, o aspecto de experiência de uso se sobrepõe à percepção de segurança e à privacidade.

Capítulo 4

Comportamento e Avaliação dos Usuários de Serviços de Autenticação

Capturar e entender a reação dos usuários imediatamente após a realização de um processo de autenticação pode revelar importantes aspectos a respeito de seu comportamento, contribuindo, assim, para a construção de uma solução de autenticação que esteja alinhada com suas expectativas e preferências, possivelmente tornando a solução mais eficiente e com maior possibilidade de adoção. Diante desta observação e, em complemento à investigação das crenças e percepções dos usuários sobre diferentes formas de autenticação, apresentada na Seção 3, o presente capítulo apresenta um experimento realizado com usuários finais de sistemas de IdM, no qual estes usuários são convidados a se autenticarem em uma aplicação real e, ao final de cada processo de autenticação, o usuário indica a sua avaliação a respeito da experiência de uso, sensação de segurança e privacidade. Assim, o experimento apresentado neste capítulo visa analisar métodos de autenticação, com a finalidade de avaliar em relação a segurança, privacidade e experiência de uso, do ponto de vista dos usuários finais, no contexto de sistemas de IdM.

Em continuidade, será apresentado o método aplicado na construção do experimento, seguido da apresentação e análise resultados coletados. As ameaças e limitações também são apresentadas ao final deste capítulo.

4.1 Método Aplicado

O experimento faz com que o usuário final experiencie um processo real de autenticação. O objetivo principal deste experimento prático é coletar o julgamento dos usuários imediatamente após serem submetidos a um determinado processo de autenticação. Desta forma, é esperado que a avaliação realizada possa refletir com maior fidelidade o seu comportamento em relação ao processo de autenticação apresentado.

O método aplicado neste experimento consiste na apresentação dos usuários a um software que implementa diferentes formas de autenticação (senha, código de acesso, duplo fator de autenticação e biometria facial). Após o fluxo de autenticação, o usuário é convidado a atribuir uma graduação de 1 (um) a 5 (cinco) para três questões que refletem o seu comportamento e reação sobre os aspectos de experiência de uso, segurança e privacidade naquele processo de autenticação em específico. A nota 1 (um) significa "Muito Insatisfeito" e 5 (cinco) significa "Muito Satisfeito". Os questionamentos apresentados aos usuários foram:

1. "Como você se sente com relação a sua experiência de uso?"
2. "Como você se sente com relação a sua percepção de segurança?"
3. "Como você se sente com relação ao respeito a sua privacidade?"

Ao final da avaliação do usuário, os resultados coletados são persistidos em uma base de dados relacional, possibilitando análise dos dados coletados a cada interação do usuário com o experimento.

4.1.1 *Design* da Solução de Software Desenvolvida

A realização do experimento demandou o desenvolvimento de um software para a implementação das diferentes formas de autenticação a serem analisadas e que, ao final do processo, possibilitasse ao usuário realizar a avaliação do método de utilizado. O software construído foi denominado **uAUTH Experimento** e o seu desenvolvimento foi dividido em dois módulos: uma API implementada utilizando a tecnologia NodeJS ¹ com Typescript e, um segundo módulo, para representar o *frontend*, desenvolvido com a utilização do *framework* Vue.JS ² e a linguagem de programação Javascript. Já a persistência dos dados foi realizada utilizando uma base de dados PostgreSQL. A escolha da suíte de tecnologias considerou que se tratam de tecnologias utilizadas na atualidade [102] que conseguem entregar soluções responsivas, com possibilidade de utilização em diversos dispositivos como computadores pessoais e *smartphones* e, ainda, que são de conhecimento do autor da presente pesquisa. A Figura 4.1 apresenta o diagrama com os componentes da solução implementada, com uma aplicação web como *front-end* consumindo serviços web providos pela API de *back-end*. As notificações para os usuários são encaminhadas através de um serviço de mensageria SMS e os dados do experimento são persistidos em uma base de dados relacional.

¹<https://nodejs.org/>

²<https://vuejs.org/>

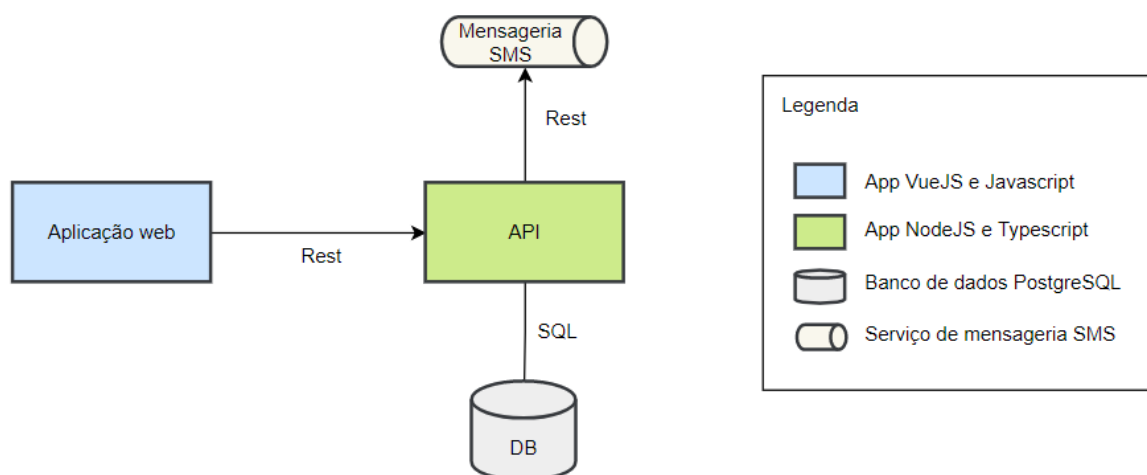


Figura 4.1: Componentes da solução de software.

Fonte: O autor.

O modelo de dados é composto por duas tabelas (usuários e autenticações) e pode ser observado na Figura 4.2. A tabela ‘usuários’ armazena os dados de identificação e contato referentes aos participantes do experimento. Já os campos ‘inicializado’ e ‘notificado’ são utilizados para indicar o aceite e a notificação dos participantes do experimento. Estes campos de controle são importantes para que o início e a evolução do experimento possam ser acompanhados e para que o software do experimento possa garantir ao participante a visualização e a aceitação do Termo de Consentimento Livre e Esclarecido, disponível no Apêndice C. Após o primeiro acesso e aceite do TCLE, o valor do campo inicializado é alterado para ‘true’. Já o campo ‘notificado’ é alterado para ‘true’ quando o participante é notificado do início do experimento. O campo ‘senha’ armazena o resumo criptográfico da senha definida pelo participante quando este realiza a definição ou a redefinição da senha a ser utilizada durante a realização do experimento.

A tabela ‘autenticacoes’ contém as entradas referentes aos processos de autenticação aos quais os participantes serão submetidos. Para cada participante do experimento existem N entradas na tabela de autenticações e estas entradas são específicas para cada um dos participantes. A escolha por entradas de autenticação únicas possibilita que o pesquisador possa acompanhar a execução do experimento e, eventualmente, interagir com os participantes para que possam se manter engajados e respondendo às solicitações de autenticação, além de ser útil para armazenar informações específicas de cada autenticação realizada pelo participante. O campo ‘tipo’ indica o método de autenticação ao qual o usuário será submetido (senha, código de acesso, duplo fator de autenticação e biometria facial). O campo ‘codigo_link’ armazena um identificador único e aleatório que é utilizado para compor a URL de autenticação encaminhada para o participante

do experimento. O campo 'data' registra a informação de data e hora em que o usuário realizou a autenticação. Os registros de data e hora podem fomentar análises baseadas no momento em que a autenticação foi realizada. O campo duração indica o tempo gasto pelo usuário para completar a tarefa de autenticação e possibilita a análise de correlação entre tempo gasto e a avaliação do usuário sobre o método de autenticação. A quantidade de vezes que o participante errou ao apresentar uma credencial e a quantidade de vezes que o participante solicitou uma redefinição de credencial são armazenados nos campos 'qtd_falha_credencial' e 'qtd_recuperacao_credencial', respectivamente. A informação de falhas e redefinições de credenciais possibilitam a realização de análises sobre a facilidade com que o usuário realiza o processo de autenticação e de apresentação da credencial. O campo 'turno_preferencial' indica quando o usuário será convidado a participar de uma autenticação no software do experimento.

O Apêndice D, apresenta a documentação da API desenvolvida neste experimento e o Apêndice E apresenta a descrição do dicionário de dados.

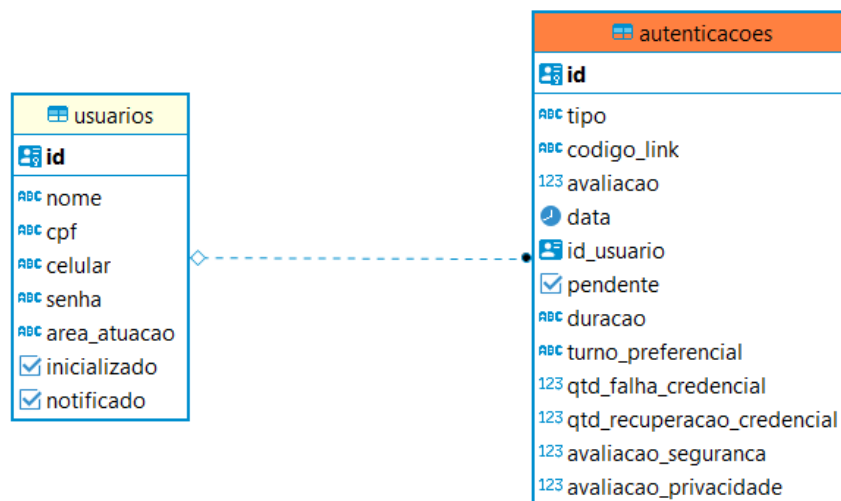


Figura 4.2: Modelo de dados do software do experimento.

A solução de software desenvolvida possibilita que novos métodos de autenticação possam ser adicionados e que o experimento possa ser reproduzido com a configuração desejada pelo pesquisador. Como uma forma de facilitar o processo de montagem da solução em diversos ambientes, os componentes (Aplicação web, API e Banco de Dados) foram distribuídos em *containers* e estão prontos para serem executados utilizando a tecnologia Docker ³. A escolha pela tecnologia se deve ao fato da popularidade do Docker, representando um padrão de fato no processo de distribuição de soluções em *containers*, com mais de 7 milhões de aplicativos e 13 milhões de desenvolvedores utilizando a tecnologia [103]. A distribuição em formato de *containers* Docker possibilita que a solução possa ser

³<https://www.docker.com/>

instanciada de maneira isolada e padronizada independente do sistema operacional em questão, fornecendo um comportamento consistente, independente do ambiente em que é instanciada a solução.

Durante a condução deste trabalho não foram encontradas implementações alternativas que pudessem ser aplicadas para a condução do experimento proposto. Desta forma, foi observada a necessidade de implementação de uma solução, como forma de materializar um experimento com diferentes formas de autenticação e que requisitasse dos participantes uma avaliação sobre os aspectos de experiência de uso, privacidade e segurança. Soluções comerciais como Duo [84] e Auth0 [104] oferecem implementação de diversos métodos de autenticação, porém não se alinham com o objetivo deste experimento, uma vez que são soluções pagas e direcionadas para a efetiva implementação da autenticação não sendo voltadas à coleta da avaliação dos usuários.

Todos os artefatos que fazem parte da solução de software desenvolvida estão disponíveis em <https://github.com/araujoronald/uauth> e, neste mesmo endereço, são encontradas instruções sobre como instanciar a solução.

4.1.2 Métodos de Autenticação Utilizados

A aplicação desenvolvida para suportar este experimento utiliza os métodos de autenticação baseados em senhas, códigos de acesso, 2FA (senha e código de acesso) e biometria facial. A escolha por estes métodos se deu devido à popularidade dos mesmos e considerando serem métodos que podem ser aplicados em diversas soluções, independente de um hardware de usuário específico, como um cartão inteligente ou um token, ou da plataforma utilizada: *web*, *mobile* ou *desktop*.

Alguns dispositivos móveis e computadores pessoais possibilitam que os aplicativos possam utilizar senhas sem que os usuários precisem, necessariamente, digitar a sua senha a cada processo de autenticação. Neste modo, o usuário informa sua senha uma vez e o sistema operacional armazena e criptografa esta senha a partir da biometria do usuário, seja ela facial ou impressões digitais. No momento em que o aplicativo requer a senha do usuário, o sistema operacional solicita que o usuário informe a sua biometria, descriptografa a senha previamente salva e encaminha esta senha para o aplicativo, emulando assim a digitação da senha por parte do usuário final. Para o presente experimento, não foi considerada esta abordagem, uma vez que ela ainda não é massificada e aplicada de forma amplas nas plataformas *web*, *mobile* ou *desktop*.

4.1.2.1 Senha

Método de autenticação onde é exigido do usuário o esforço de memorização de credencial. Neste método o usuário informa o CPF e uma senha. Na primeira interação do usuário com o uAUTH Experimento, foi requerida a definição de uma senha para ser utilizada durante todo o conjunto de testes. O requisito para a definição da senha é que esta deve conter ao menos oito caracteres, sendo no mínimo uma letra maiúscula, uma letra minúscula, um número e um caractere especial. Um indicativo apresentado na tela de definição da senha apresentava ao usuário a informação sobre o atendimento dos requisitos, conforme observado nas Figuras 4.3a e 4.3b. A definição dos requisitos da senha foi baseado em senhas consideradas fortes pelos projetos *Password Check* [105], *Security.org* [106] e *My1Login* [107].



Figura 4.3: Experimento de autenticação com senha.

Nas sessões seguintes foi requerido que o usuário pudesse recordar da senha inicial, sendo ofertada a opção de redefinição da senha, conforme ilustrado na Figura 4.3c. O experimento registrou, para cada URL de autenticação, quantas vezes o usuário errou e quantas vezes o usuário redefiniu a sua senha. A Figura 4.3 ilustra as telas do experimento nas quais o usuário é convidado a definir e redefinir uma senha, assim como, a tela na qual o usuário realiza a autenticação utilizando o método senha.

4.1.2.2 Código de Acesso

Neste método de autenticação um código de acesso é encaminhado para o usuário e não é necessário que seja memorizada por parte do usuário alguma informação adicional. É solicitado que o usuário informe o seu CPF, conforme ilustrado na Figura 4.4a e, após confirmação de que se trata de um usuário ativo do experimento, a aplicação uAUTH gera um OTP com validade de cinco minutos. O tempo de validade do OTP foi arbitrado pelo autor deste trabalho, observando ser razoável para o propósito de autenticação.

Códigos OTP requerem a utilização de uma chave secreta para o processo de geração e posterior verificação da sua validade. No experimento uAUTH, a chave secreta foi constituída a partir da seguinte composição:

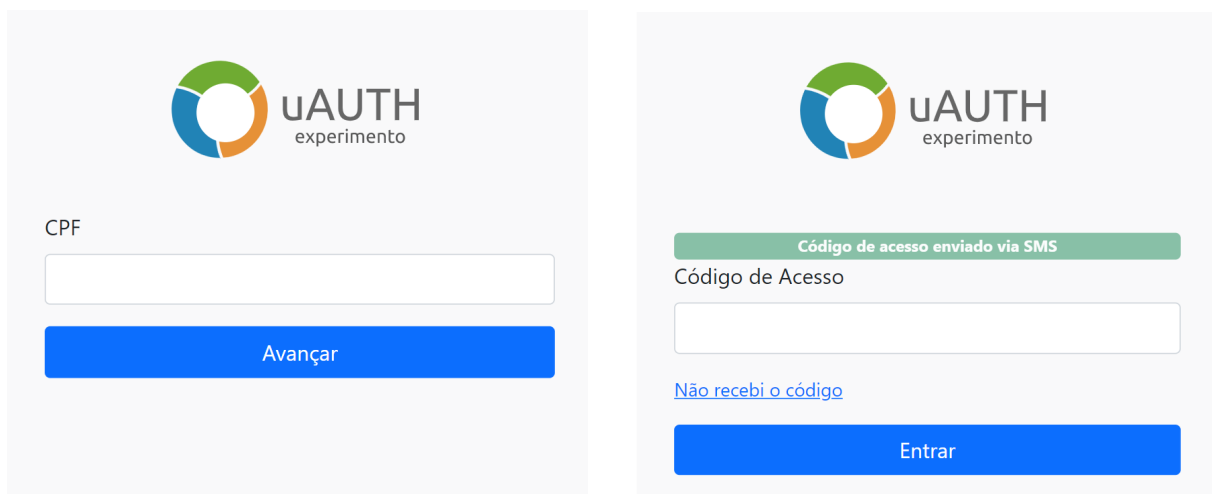
$$SHA-256(CONCAT(SKEY, ID-USUARIO))$$

onde,

SKEY = chave simétrica AES de 256 bits CBC

ID-USUARIO = identificador do usuário no banco de dados

SHA-256 = função de hash SHA-256



(a) Solicitação do CPF

(b) Código de acesso

Figura 4.4: Experimento de autenticação com código de acesso.

Após a geração do código de acesso OTP, a aplicação entrega este código ao participante através de um SMS encaminhado para o número de celular fornecido pelo usuário quando de seu cadastro no experimento, conforme Figura 4.4b. De posse do código de acesso, o usuário informa este código na aplicação, caso a informação esteja correta e dentro da validade, o processo de autenticação é concluído com sucesso. A Figura 4.4 ilustra as telas da aplicação uAUTH quando é solicitado o método de autenticação utilizando código de acesso.

4.1.2.3 Biometria Facial

Por ser um método de autenticação que utiliza uma biometria física, a validação facial não requer do usuário nenhum esforço adicional de memorização de uma senha ou de porte de algum dispositivo ou, ainda, o recebimento de código de acesso.

Em processo de autenticação biométrica é necessário que o sistema de validação realize uma comparação da biometria coletada do usuário que está requerendo a autenticação com uma biometria previamente cadastrada na base de dados e que se refere ao usuário que, de fato, é o detentor da conta. Duas abordagens podem ser utilizadas para que a comparação possa ser efetuada: em uma delas o usuário informa apenas a sua biometria e o sistema efetua uma série de comparações entre a biometria informada pelo usuário e a biometria cadastrada na base de dados. Essa busca pode, no pior caso, percorrer toda a base de dados e realizar N comparações biométricas até ter o resultado se o usuário possui ou não uma conta válida. Uma vantagem dessa abordagem é que o usuário não necessita informar nenhum dado além da sua própria biometria. Por realizar N comparações, no pior caso, esta abordagem é conhecida como 1:N.

Uma segunda abordagem é quando o usuário, além de informar a sua biometria, informa também algum dado de identificação como, por exemplo um número de CPF ou um e-mail. A partir deste dado de identificação, o sistema localiza a conta do usuário e a biometria cadastrada na base e realiza apenas uma comparação biométrica entre o dado fornecido pelo usuário e o dado contido na base. Esta abordagem é conhecida como 1:1.



Figura 4.5: Experimento de autenticação com biometria facial.

Neste experimento, o processo de autenticação utilizando biometria facial segue o conceito de validação 1:1 e se inicia com o usuário sendo solicitado a informar seu CPF, como se observa na Figura 4.5a. A partir desta informação, o sistema localiza a conta do usuário e, em seguida, solicita acesso à câmera do dispositivo ao qual o usuário está utilizando, de modo que o mesmo possa apresentar a sua face, como pode ser visto na Figura 4.5b. Por restrição de implementação, este experimento não realiza uma comparação da

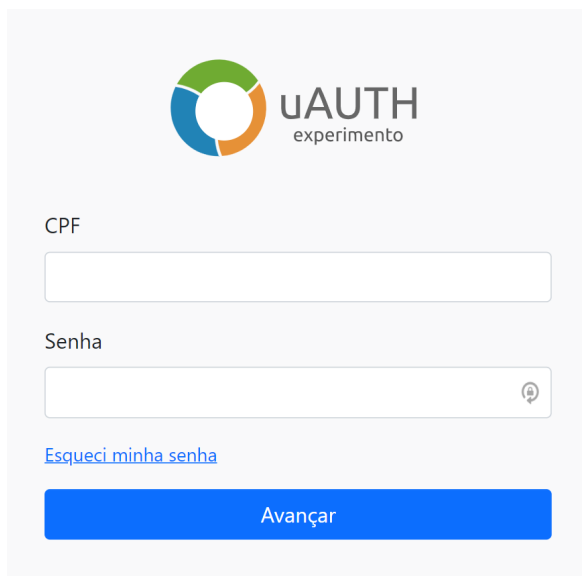
imagem da face apresentada pelo usuário com um registro biométrico prévio contido na base de dados. Ao invés disso, o experimento está configurado para aplicar uma regra de validação biométrica onde uma autenticação é considerada como aceita a partir de uma função pseudo-randômica que considera a autenticação válida na proporção de 7 a cada 10 tentativas, ou seja, em cada 10 processos de autenticação baseada em biometria facial, 7 indicam usuário autenticado com sucesso e 3 apresentam falha na autenticação, reque-rendo do usuário que apresente novamente a sua face. O estabelecimento dessa função pseudo-randômica na proporção de 7:10, se deu de forma arbitrária pelo pesquisador e buscou simular o cenário de falha na autenticação, uma vez que uma comparação biométrica de fato não está sendo realizada e era intuito do experimento observar o comportamento dos usuários nos casos de falha no processo de autenticação. Assim como observado nos demais métodos de autenticação do experimento onde as comparações são efetivamente realizadas.

A Figura 4.5 apresenta as telas envolvidas em um processo de autenticação com utilização de biometria facial. É de se ressaltar que a imagem capturada para efeito de autenticação não é persistida no experimento, sendo utilizada apenas durante a autenticação.

4.1.2.4 Duplo Fator de Autenticação (2FA) - Senha e Código de Acesso

O processo de autenticação com duplo fator requer que o usuário realize dois processos de autenticação. Neste experimento, o primeiro método de autenticação é realizado com uso de senha, como pode ser observado na Figura 4.6a, seguido de um método de autenticação realizado com uso de código de acesso (Figura 4.6b), configurando o segundo fator de autenticação. O processo é similar ao apresentado nas Seções 4.1.2.1 e 4.1.2.2.

No experimento apresentado no presente trabalho, a senha é utilizada sempre como primeiro fator de autenticação e o código de acesso como segundo fator de autenticação. A Figura 4.6 ilustra as telas do método de autenticação com duplo fator.



The screenshot shows the login interface for the uAUTH experiment. At the top left is the logo, a circular icon with blue, green, and orange segments, followed by the text "uAUTH" in a bold font and "experimento" in a smaller font below it. Below the logo, there are two input fields: the first is labeled "CPF" and the second is labeled "Senha". To the right of the password field is a small eye icon for toggling visibility. Below the password field is a blue link that says "Esqueci minha senha". At the bottom of the form is a large blue button with the text "Avançar".

(a) Autenticação com Senha



The screenshot shows the login interface for the uAUTH experiment, specifically for code authentication. At the top left is the same logo as in (a). Below the logo, there is a green notification bar with the text "Código de acesso enviado via SMS". Underneath this is a label "Código de Acesso" followed by an empty input field. Below the input field is a blue link that says "Não recebi o código". At the bottom of the form is a large blue button with the text "Entrar".

(b) Autenticação com Código de acesso

Figura 4.6: Experimento de autenticação com duplo fator de autenticação.

4.1.3 Avaliação do Usuário

Após a realização do processo de autenticação, o usuário é convidado a informar a sua avaliação sobre o método de autenticação ao qual foi submetido. A Figura 4.7 apresenta a tela do software onde o usuário registra a sua percepção sobre o método de autenticação.

The image shows a web form for evaluating the uAUTH experiment. At the top, there is a logo for 'uAUTH experimento' consisting of a circular icon with green, blue, and orange segments. Below the logo, the text reads: 'Olá Ronald Araujo, obrigado por vir até aqui. Agora dê uma nota que represente o uso desta forma de autenticação.' There are three questions, each followed by a 5-point Likert scale. The first question is 'Como você se sente com relação a sua experiência de uso?' with a scale where 1 is red, 2 is pink, 3 is yellow, 4 is light green, and 5 is dark green. The second question is 'Como você se sente com relação a sua percepção de segurança?' with the same color-coded scale. The third question is 'Como você se sente com relação ao respeito a sua privacidade?' also with the same color-coded scale. At the bottom of the form is a blue button labeled 'Confirmar Avaliação'.

Figura 4.7: Avaliação do método de autenticação.

Uma vez registrada a avaliação, o usuário é informado do final do processo de autenticação e a URL utilizada para a realização da autenticação é invalidada, não sendo possível que o usuário reinicie o processo. A unicidade das autenticações possibilita a análise de informações referentes a tentativas malsucedido, tempo gasto no processo de autenticação e acompanhamento da execução do experimento, sendo possível identificar se os respondentes já se autenticaram.

4.1.4 Participantes do Experimento

Uma vez definidos os métodos de autenticação, o passo seguinte foi a definição da forma de contato com os usuários do experimento. Foi definido, de forma arbitrária, que cada um dos usuários fossem submetidos a 2 (dois) processos de autenticação para cada um dos tipos elencados no experimento, totalizando 8 (oito) processos de autenticação para cada usuário. A submissão dos usuários a dois processos de autenticação para cada um dos métodos aplicados visou extrair de forma mais real o comportamento do usuário em relação a determinado método de autenticação, registrando uma segunda avaliação do

usuário para o método de autenticação apresentado, especialmente considerando que por definição do experimento um mesmo método de autenticação não é apresentado de forma consecutiva ao usuário.

Para cada um dos processos de autenticação foi gerada uma URL única, de forma que fosse permitido que o usuário respondesse apenas uma única vez àquele processo de autenticação. A URL gerada estabelece a relação de um determinado usuário e com um determinado método de autenticação. A Figura 4.8 exemplifica URLs utilizadas no experimento.

MÉTODO DE AUTENTICAÇÃO	URL DE ACESSO
SENHA_CODIGO_ACESSO	https://uauth-323213.rj.r.appspot.com/6DqB4y
SENHA_CODIGO_ACESSO	https://uauth-323213.rj.r.appspot.com/Ljv088
FACE	https://uauth-323213.rj.r.appspot.com/cjjLO9
FACE	https://uauth-323213.rj.r.appspot.com/FYXcc4
SENHA	https://uauth-323213.rj.r.appspot.com/3TNVmD
SENHA	https://uauth-323213.rj.r.appspot.com/rL4Th3
CODIGO_ACESSO	https://uauth-323213.rj.r.appspot.com/N3BHBZ
CODIGO_ACESSO	https://uauth-323213.rj.r.appspot.com/F4A3wn

Figura 4.8: Exemplo de URLs utilizadas no experimento.

As URLs utilizadas nos processos de autenticação foram encaminhadas para os participantes do experimento via SMS duas vezes ao dia: às 10:00 e às 16:00. O algoritmo de seleção das URLs para envio aos usuário controlava para que o envio atual utilizasse um método de autenticação diferente do último método encaminhado para aquele usuário. Assim, caso a primeira URL encaminhada fosse, por exemplo, referente ao método de autenticação utilizando senha, o envio posterior seria utilizando um dos outros três métodos de autenticação: código de acesso, biometria facial ou 2FA. O intuito é apresentar ao usuário os métodos de autenticação de forma não repetitiva. Um exemplo de conteúdo da mensagem SMS é: "Olá Ronald, aqui está o link para o experimento de autenticação uAUTH: <https://uauth-323213.rj.r.appspot.com/AcBaz4>".

O experimento foi realizado entre os dias 31/08/2021 e 10/09/2021 e contou com 23 usuários, cada um realizando dois processos de autenticação para cada um dos quatro métodos utilizados neste experimento, totalizando 184 processos de autenticação. A amostra dos participantes foi realizada de forma aleatória e não probabilística. Os convidados receberam instrução sobre a realização do experimento e os interessados em participar preencheram um formulário com as seguintes informações pessoais: Nome, CPF, E-Mail,

Celular e Área de Atuação, sendo esta última um campo de domínio fechado com os valores TI (Tecnologia da Informação) e Outras. A definição das áreas de atuação visou seguir as mesmas unidades de análise do questionário apresentado no Capítulo 3. De posse dos dados dos participantes, a etapa seguinte foi a de carga destes dados na aplicação que materializou o experimento.

Para iniciar a participação, no primeiro acesso ao experimento, cada usuário foi apresentado a uma descrição do objetivo da pesquisa e foi solicitada a sua anuência ao Termo de Consentimento Livre e Esclarecido (Apêndice C).

Na seção seguinte serão apresentados os resultados e uma discussão sobre os achados no experimento realizado.

4.2 Resultados e Discussão

Após a conclusão dos 184 processos de autenticação, oito para cada um dos participantes do experimento, os dados coletados foram analisados e serão apresentados nesta Seção. É pertinente ressaltar que este experimento foi conduzido como um ensaio, com um processo de amostragem aleatória e, a princípio, os dados obtidos não devem ser generalizados, porém servem para delinear o comportamento do grupo de usuários de sistemas de IdM.

A Figura 4.9 apresenta uma visão consolidada dos resultados do experimento com relação aos aspectos de experiência de uso, privacidade e segurança.

Observando sob o aspecto da experiência de uso, o experimento revelou que a autenticação baseada na biometria facial é a que oferta maior grau de satisfação por parte dos usuários, seguidos pelas autenticações baseadas em código de acesso e senha. Neste mesmo aspecto, o método de autenticação que menos agradou aos usuários foi a utilização de duplo fator de autenticação, no caso específico, senha seguida de código de acesso.

Já no aspecto de privacidade, o método de autenticação que foi melhor avaliado pelos usuários foi o de duplo fator de autenticação, com senha e código de acesso, com avaliação ligeiramente superior aos métodos baseados em código de acesso, senha e face, respectivamente. Chama atenção o fato de que, tanto para a autenticação baseada em 2FA como para a baseada em senha, não foi observada nenhuma avaliação de insatisfação, enquanto que para a abordagem baseada em biometria facial o nível de insatisfação foi significativamente superior em relação às demais abordagens. Esses dados indicam que os usuários percebem que sua privacidade é afetada quando se trata de um método de autenticação baseado em biometria.

No aspecto de segurança, foi observado que o método 2FA também se destaca, com elevado grau de segurança percebida pelos usuários, seguido de código de acesso, face e senha, respectivamente. É interessante o fato da abordagem de senha ser apontada com

maior grau de insatisfação com relação à segurança, ao mesmo tempo que apresenta maior grau de indiferença, quando comparada com outras abordagens, mesmo com o cenário do experimento exigindo dos usuários a definição de uma senha considerada forte. Esta observação aponta para uma possível tendência de descrença com relação à segurança percebida em autenticações baseadas em senha.

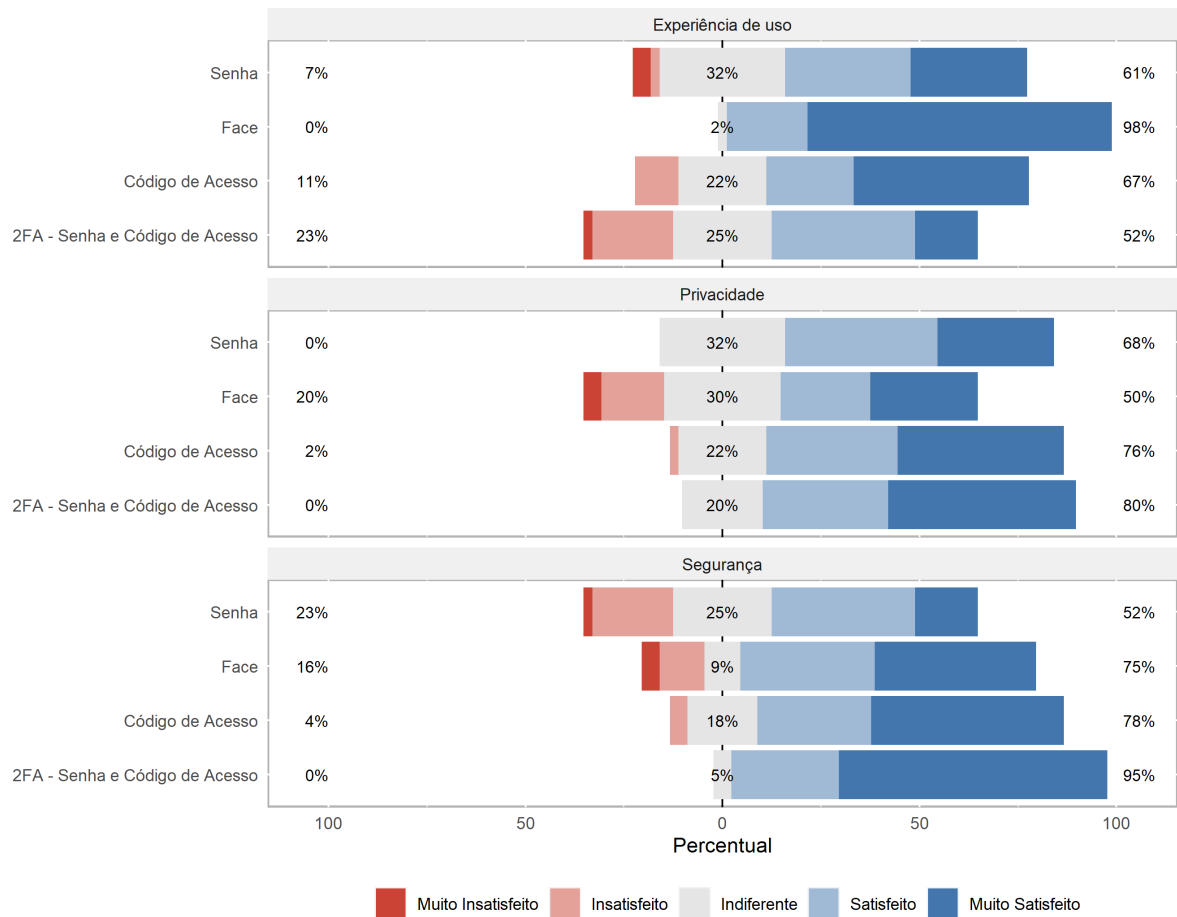


Figura 4.9: Resultados do experimento de autenticação.

Analisando cada um dos métodos de autenticação de forma isolada, ainda considerando os aspectos de experiência de uso, privacidade e segurança, é possível perceber que a abordagem baseada em código de acesso é a que apresenta o maior equilíbrio, apesar de não possuir o maior destaque em nenhum dos aspectos abordados. A Figura 4.10 apresenta uma visão isolada de cada um dos métodos de autenticação abordados neste trabalho.

A abordagem baseada em senha não apresenta nenhum destaque positivo e se configura como a pior abordagem do ponto de vista de segurança percebida pelos usuários.

A autenticação utilizando duplo fator de autenticação se destaca nos quesitos de segurança e privacidade, porém apresenta a pior avaliação dos usuários no que diz respeito à experiência de uso.

A abordagem baseada em biometria apresenta a melhor avaliação de experiência de uso e a pior avaliação com relação à privacidade.

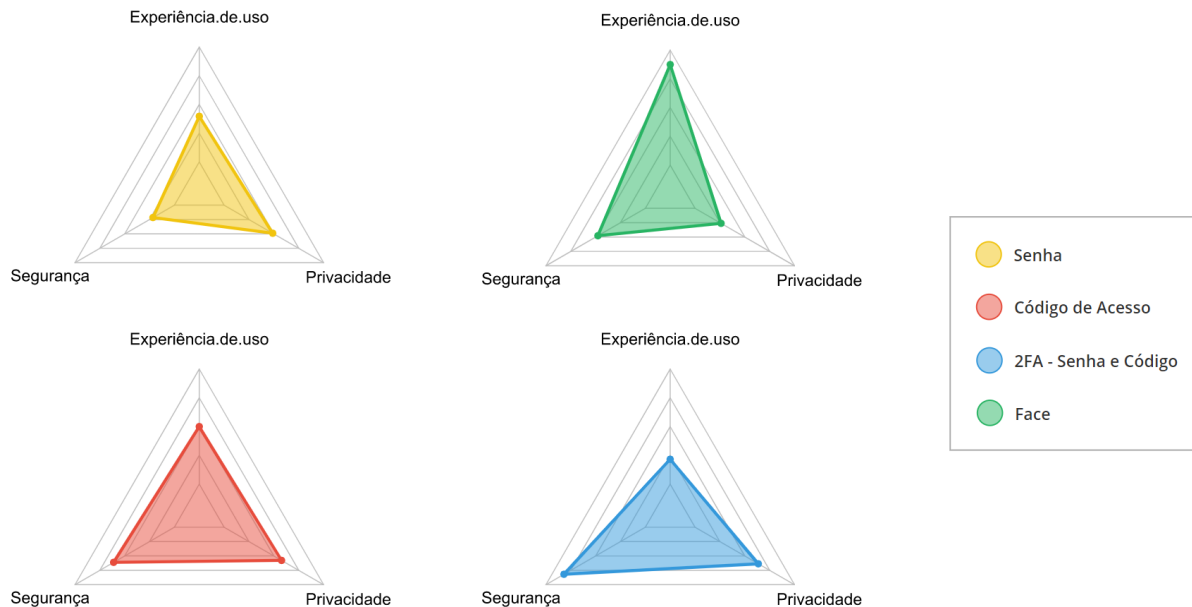


Figura 4.10: Diagrama de radar para cada um dos métodos de autenticação.

Um outro ponto de observação derivado do experimento é relacionado ao tempo necessário para que o usuário consiga efetuar um processo de autenticação. A realização do experimento mostrou que, no grupo estudado, as autenticações baseadas em biometria facial são as que necessitaram de menor tempo gasto por parte dos usuários, seguido pelos métodos baseados em código de acesso, senha e 2FA, respectivamente. Sendo que a autenticação baseada em 2FA apresentou duração consideravelmente maior.

O tempo de duração das autenticações baseadas em senha se justifica pelas falhas de autenticação observadas e posterior redefinição da credencial. O quantitativo de redefinições de senha aponta para a dificuldade de recordar a senha definida pelo usuário, mesmo em um experimento com duração de apenas quatro dias. A Figura 4.11 ilustra o tempo gasto em cada um dos métodos de autenticação.

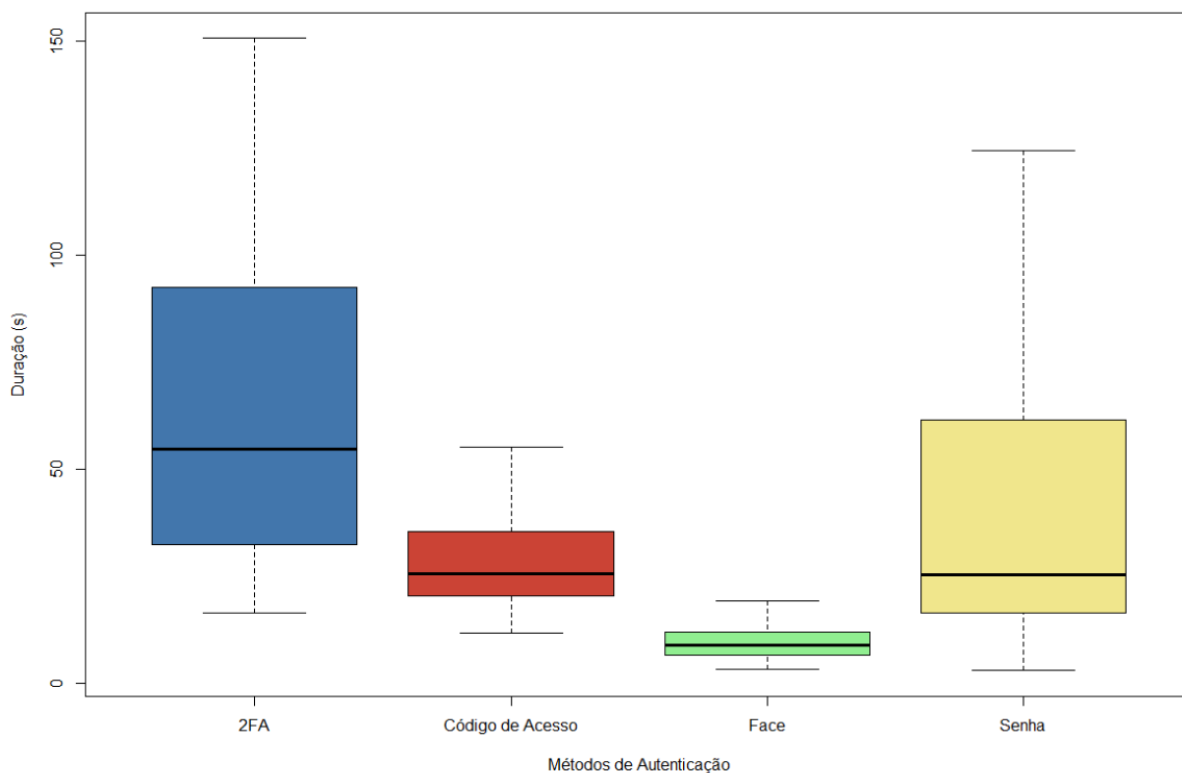


Figura 4.11: Duração dos processos de autenticação.

Com a análise dos tempos gastos em cada um dos métodos de autenticação do experimento e, observando a avaliação dos usuários sobre os aspectos de experiência de uso, privacidade e segurança, se configuraram algumas correlações entre as variáveis envolvidas. A duração do processo de autenticação possui correlação negativa com a experiência de uso percebida pelos usuários, ou seja, quanto mais demorado é o processo de autenticação, menos os usuários avaliam de forma positiva o método de autenticação. A Figura 4.12 apresenta um disgrama de correlação entre variáveis do experimento.

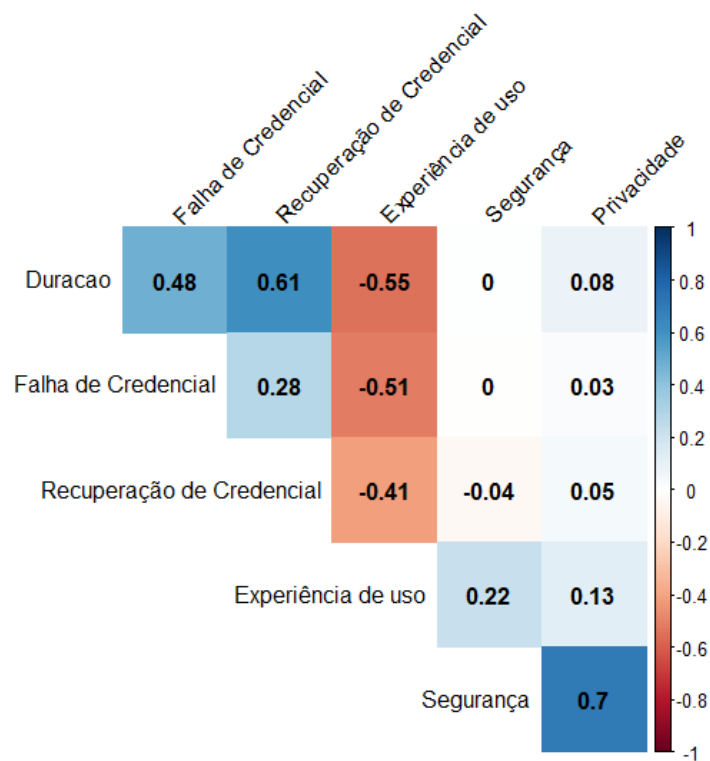


Figura 4.12: Matriz de correlação entre as variáveis do experimento.

Ainda analisando a duração das autenticações, se percebeu que o tempo elevado se correlaciona positivamente com o processo de recuperação e falha de credencial. Outro ponto que chamou atenção foi o fato de existir uma correlação positiva considerável entre a percepção de privacidade e de segurança, sendo o maior índice de correlação observado no ensaio.

O observado no experimento é que os usuários demonstraram ter uma boa percepção dos aspectos inspecionados neste trabalho, com indicação de satisfação baseada na duração do processo de autenticação e no esforço requerido, seja de memorização, aquisição de um código único ou apresentação de um dado biométrico. As limitações do experimento realizado são apresentadas na Seção 4.3.

4.3 Limitações e Ameaças ao Experimento

O experimento foi realizado a partir de uma amostra aleatória e, assim como observado no Capítulo 3, sofre com algum grau de viés, o que compromete a generalização dos resultados encontrados. Estudos baseados em questões de opinião podem apresentar resultados diferentes quando realizados em outro período de tempo ou que sejam aplicados a grupos de indivíduos diferentes.

4.4 Síntese do Capítulo

Este Capítulo apresentou o método, resultados e limitações da realização de um experimento com usuários finais de sistemas de IdM, especificamente na parte de autenticação. Foi apresentada uma aplicação que implementa quatro métodos distintos de autenticação, sendo eles: senha, código de acesso, duplo fator (senha e código de acesso) e biometria facial. Ao final do método de autenticação, o usuário foi convidado a indicar sua satisfação sobre o método de autenticação em questão, nos aspectos de experiência de uso, privacidade e segurança, podendo realizar a avaliação em cinco níveis: de muito insatisfeito até muito satisfeito.

Os resultados apresentados indicam que a autenticação baseada em código de acesso é a que apresenta maior equilíbrio entre os métodos de autenticação observados, sendo a autenticação baseada em biometria facial a que apresenta melhor avaliação com relação à experiência de uso. Os resultados indicaram que o tempo gasto durante a autenticação é um fator relevante no processo de satisfação do usuário com relação à experiência de uso.

Capítulo 5

Conclusão

O modelo de atendimento baseado em balcão presencial ainda contribui de forma significativa na prestação de serviços aos cidadãos, porém o custo elevado e a necessidade de expansão na prestação de serviços faz com que novas formas sejam exploradas. Assim, o processo de digitalização de serviços se torna opção capaz de ofertar serviços em maior escala, com maior qualidade e com custo reduzido.

A pandemia provocada pela Covid-19 acelerou o processo de virtualização e ocasionou a redefinição de serviços para o mundo digital. Em geral, a oferta de um serviço digital requer que o provedor do serviço conheça o seu usuário para que o atendimento seja realizado maneira correta e, neste ponto, é fundamental que os serviços on-line possam contar com um sistema de gerenciamento de identidades e que este sistema possua um método de autenticação seguro, com boa experiência de uso e que respeite a privacidade dos seus usuários.

No contexto dos processos de autenticação de usuário e de sistemas de gerenciamento de identidade, é importante que as soluções tenham a percepção de que a experiência de uso é muito valorizada, e que os usuários buscam aplicações rápidas, práticas e fáceis de usar. Aspectos de segurança e privacidade, apesar de percebidos pelos usuários, são considerados pelos usuários finais como sendo secundários em relação à experiência de uso, o que reforça a necessidade de que os provedores de identidade apresentem soluções projetadas para a proteção do usuário, uma vez que são pilares importantes no estabelecimento de um efetivo sistema de IdM [19].

Este trabalho apresentou um questionário aplicado à usuários de sistemas on-line com o intuito de perceber o comportamento destes usuários quando deparados com sentenças a respeito de métodos de autenticação. O resultado do questionário revelou que, mesmo em cenários em que os usuários reconhecem que determinada abordagem é arriscada em termos de segurança, eles ainda a utilizam em prol de uma maior comodidade durante a identificação. Um exemplo se deu na sentença que se refere ao processo de repetição

de uma mesma senha em mais de um serviço. Outra situação que chama atenção é que os usuários ainda se sentem confortáveis com o uso de senhas, mesmo estas apresentando uma série de problemas. Um exemplo que reforça essa observação é a observação de que cerca de 88% das contas ativas do serviço Gov.br utilizam como meio de autenticação apenas usuário e senha [20]. Atualmente, o Gov.br conta com mais de um milhão de contas ativas.

Com larga margem foi observado que, do ponto de vista dos entrevistados no questionário, o uso de biometria é considerado um processo mais simples e conveniente, frente aos métodos de autenticação baseados em senha, código de acesso e duplo fator de autenticação (senha e código de acesso). Se por um lado a adoção de biometria nos processos de autenticação de usuário torna o processo com ótima experiência de uso, por outro, a utilização de biometria requer controles eficientes no que diz respeito à proteção e à privacidade dos usuários. Métodos de autenticação puramente baseados em biometria ainda correm o risco de vazamentos de dados inviabilizarem por completo o sistema, uma vez que não é possível a redefinição de um dado biométrico.

Foi apresentado também um experimento realizado com usuários de sistemas on-line onde estes usuários foram apresentados a uma aplicação de software e convidados a se autenticarem, sendo que, ao final de cada processo de autenticação, o usuário indica a sua avaliação a respeito da experiência de uso, sensação de segurança e privacidade. O resultado do experimento indica que o método de autenticação baseado em código de acesso foi o que melhor equilibrou as dimensões de experiência de uso, privacidade e segurança. Apesar de não se apresentar como a melhor abordagem do ponto de vista de usabilidade, a utilização de código de acesso não requer esforço do usuário para memorização de senha e também não requer que o usuário faça exposição de uma informação pessoal sensível, como alguma forma de biometria, ou que ele necessite portar algum dispositivo físico, como o caso dos *tokens* ou cartões inteligentes. Foi observado também que o tempo despendido no processo de autenticação contribui diretamente para a manifestação de satisfação por parte do usuário final.

Encontrar o correto equilíbrio entre segurança, proteção de privacidade e usabilidade é o desafio posto e é esperado que uma gama de soluções se apresentem como candidatas a solucionar esta questão. É esperado também que os temas de segurança e privacidade de dados sejam cada vez mais abordados e que os cidadãos passem a valorizar e exigir que o tratamento dos seus dados pessoais sejam realizados de forma segura, protegida e respeitando a privacidade.

A evolução dos métodos de autenticação é constante e o futuro indica como uma boa perspectiva o surgimento e adoção de métodos de autenticação baseados em risco (*Risk Based Authentication*). Nesta abordagem, uma combinação de fatores e técnicas criam um

contexto de confiança que habilita o processo de autenticação com maior ou menor fluidez com relação à experiência de uso. Um exemplo de aplicação deste conceito ocorre quando um processo de autenticação é constituído, além de credenciais, de uma análise prévia do comportamento do usuário, envolvendo situações como a verificação se o acesso parte de uma localização ou dispositivo habitual. Um desafio desta abordagem é o respeito à privacidade dos usuários, evitando o perigo de uma situação de vigilância e rastreabilidade. Para encarar este desafio, soluções baseadas em identificadores descentralizados e credenciais verificáveis são promissoras e pretendem cada vez mais empoderar os usuários e fomentar a criação de estruturas de IdM auto-soberanas, com o usuário sendo o real detentor do seu dado e podendo informar apenas subconjuntos dos seus dados de identificação de acordo com o contexto de cada serviço, promovendo uma inversão do controle, saindo do provedor de identidade e indo para o usuário final.

5.1 Contribuições

As principais contribuições apresentadas neste trabalho são:

1. Análise e apresentação de diferentes abordagens para a estruturação de um sistema de IdM. As abordagens apresentadas (isolada, centralizada, federada, centrada no usuário e auto-soberana) possibilitam que os responsáveis pela elaboração de um sistema de IdM tenham um panorama dos principais prós e contras de cada abordagem.
2. Apresentação de um questionário sobre a percepção dos usuários a respeito de métodos de autenticação em sistemas de IdM. Com uma melhor compreensão e diagnóstico das crenças dos usuários é possível a construção e entrega de uma solução que esteja alinhada com os anseios e necessidades destes usuários.
3. Método para a realização de um experimento de autenticação com usuários finais de sistemas de IdM. Capturar a avaliação de um usuário de sistema on-line logo após uma experiência prática de uso pode apresentar uma noção mais fiel do comportamento deste usuário, contribuindo assim na construção de soluções de autenticação mais eficientes e com maior possibilidade de adoção.
4. Disponibilização de um software para a realização de experimento de autenticação com usuários finais. O software disponibilizado é passível de incremento de novos métodos de autenticação e da seleção de quais métodos devem ser aplicados a cada realização do experimento. O código fonte está disponível em <https://github.com/araujoronald/uauth>.

5. Apresentação dos resultados de um experimento realizado com usuários de sistemas de autenticação, onde foi possível perceber o comportamento e a avaliação dos usuários quando deparados com diferentes formas de autenticação. Os resultados apresentados contribuem no entendimento do comportamento dos usuários e apontam para preferências de usuário que podem ser consideradas na construção de um sistema de IdM.

5.2 Trabalhos Futuros

Para trabalhos futuros são vislumbradas as seguintes ações:

1. Acompanhamento de indicadores de efetividade de um processo de autenticação sem uso de senha (*passwordless*). O indicador utilizado poderá ser a quantidade de solicitações de nova credencial acompanhada do volume de acionamentos de suporte relacionados a autenticação. A efetividade desta abordagem poderá encorajar o uso deste método de autenticação.
2. Inclusão de suporte a outros métodos de autenticação no software utilizado no experimento. Em particular, métodos biométricos como voz e padrão de digitação, abrindo margem para a experimentação de diferentes formas de autenticação que se aproximem do considerado ideal pelos usuários finais.
3. Experimentação de método de autenticação baseado em marcações de pontos específicos em trechos de músicas, como forma de fornecer um mecanismo de autenticação com suporte para portadores de deficiência visual. O método de autenticação se apresenta como a escolha de um música por parte do usuário e a marcação de pontos específicos durante a execução da música escolhida de forma a construir um padrão que possa ser utilizado para identificar este usuário.
4. Implementação de autenticação baseada em risco, com utilização de diferentes métodos de autenticação a depender do contexto, sendo sugeridos métodos como código de acesso, biometria facial, identificador de hardware do dispositivo de acesso e IP do usuário. Conjuntamente, implementação de mecanismo de identificador descentralizado (DID), de forma a mitigar o problema da rastreabilidade, onde o provedor de serviço tenha limitada a sua capacidade de rastrear os movimentos de um determinado usuário.

Referências

- [1] UNITED NATIONS. *United Nations E-Government Survey 2018*. 2018. 298 p. Disponível em: <<https://www.un-ilibrary.org/content/publication/d54b9179-en>>. Acesso em: 10 out. 2021. 1, 2
- [2] PEDROSA, G. V. et al. A systematic review of indicators for evaluating the effectiveness of digital public services. *Information*, v. 11, n. 10, 2020. ISSN 2078-2489. Disponível em: <<https://www.mdpi.com/2078-2489/11/10/472>>. 1
- [3] UNITED NATIONS. *United Nations E-Government Survey 2020*. 2020. Disponível em: <<https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey>>. Acesso em: 10 out. 2021. 1, 2
- [4] ALLEN, C. *The Path to Self-Sovereign Identity*. 2016. Disponível em: <<http://www.lifewithalacrity.com/previous/2016/04/the-path-to-self-sovereign-identity.html>>. Acesso em: 16 jun. 2021. 2, 13, 14, 16, 17, 18, 20
- [5] CAMERON, K. The laws of identity. 2005. Disponível em: <<https://www.identityblog.com/?p=352>>. Acesso em: 11 maio. 2020. 2, 4, 5, 10, 28, 29
- [6] LEÃO, H. A. T.; CANEDO, E. D. Best practices and methodologies to promote the digitization of public services citizen-driven: A systematic literature review. *Information*, v. 9, n. 8, 2018. ISSN 2078-2489. Disponível em: <<https://www.mdpi.com/2078-2489/9/8/197>>. Acesso em: 12 jul. 2020. 2
- [7] FILHO, W. P.; RIBEIRO, C.; ZEFFERER, T. An ontology-based interoperability solution for electronic-identity systems. In: *2016 IEEE International Conference on Services Computing (SCC)*. [S.l.: s.n.], 2016. p. 17–24. 2, 8, 9
- [8] GARTNER. *What Government CIOs Should Know About Digital IDs*. 2019. Disponível em: <<https://www.gartner.com/smarterwithgartner/what-government-cios-should-know-about-digital-ids/>>. Acesso em: 02 nov. 2021. 2
- [9] BRASIL. Receita federal esclarece sobre situações de fraude no auxílio emergencial. *Ministério da Economia*, 2021. Disponível em: <<https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2021/junho/receita-federal-esclarece-sobre-situacoes-de-fraude-no-auxilio-emergencial>>. Acesso em: 14 nov. 2021. 3
- [10] BONNEAU, J. et al. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: *2012 IEEE Symposium on Security and Privacy*. [S.l.: s.n.], 2012. p. 553–567. 3, 25, 34

- [11] WORLD BANK. *ID4D Data: Global Identification Challenge by the Numbers*. 2018. Disponível em: <<https://id4d.worldbank.org/global-dataset>>. Acesso em: 10 out. 2021. 4
- [12] CAVE, J. et al. Once-only principle for citizens and businesses policy options and their impacts. In: *European Commission DG Communications Networks, Content Technology*. [S.l.: s.n.], 2017. 4
- [13] UNITED NATIONS. The 17 goals - sustainable development. 2020. Disponível em: <<https://sdgs.un.org/goals>>. Acesso em: 15 dez. 2020. 4
- [14] WORLD BANK. G20 digital identity onboarding. *Global Partnership for Financial Inclusion*, 2018. Disponível em: <<https://openknowledge.worldbank.org/handle/10986/30484>>. Acesso em: 10 out. 2021. 4
- [15] MCKINSEY. Digital identification: A key to inclusive growth. mckinsey global institute. 2019. Disponível em: <<https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>>. Acesso em: 15 dez. 2020. 4
- [16] KUTNJAK, A. Covid-19 accelerates digital transformation in industries: Challenges, issues, barriers and problems in transformation. *IEEE Access*, v. 9, p. 79373–79388, 2021. 4
- [17] GABRYELCZYK, R. Has covid-19 accelerated digital transformation? initial lessons learned for public administrations. *Information Systems Management*, Taylor Francis, v. 37, n. 4, p. 303–309, 2020. 4
- [18] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD), Presidência da República*, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.html>. Acesso em: 24 maio. 2021. 4, 9, 21, 32
- [19] CAVOUKIAN, A. *7 Laws of Identity - The Case for Privacy-Embedded Laws of Identity in the Digital Age*. Ontario, Canada, 2006. Disponível em: <<http://www.ipc.on.ca/index.asp?navid=46fid1=470>>. 4, 10, 29, 57
- [20] BRASIL. Acesso gov.br. *Secretaria de Governo Digital*, s.n, 10 2021. 5, 22, 58
- [21] GARCÍA, S. S.; OLIVA, A. G. Solving identity management and interoperability problems at pan-european level. In: MEERSMAN, R.; HERRERO, P.; DILLON, T. (Ed.). *On the Move to Meaningful Internet Systems: OTM 2009 Workshops*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. p. 805–809. ISBN 978-3-642-05290-3. 8
- [22] ITU-T. *Baseline capabilities for enhanced global identity management and interoperability*. [S.l.], 2009. 8, 15

- [23] BERBECARU, D.; LIOY, A.; CAMERONI, C. Providing digital identity and academic attributes through european eid infrastructures: Results achieved, limitations, and future steps. *Software: Practice and Experience*, v. 49, n. 11, p. 1643–1662, 08 2019. 8, 13
- [24] LIPS, S. et al. Designing an effective long-term identity management strategy for a mature e-state. In: KÓ, A. et al. (Ed.). *Electronic Government and the Information Systems Perspective*. Cham: Springer International Publishing, 2019. p. 221–234. ISBN 978-3-030-27523-5. 8
- [25] BERBECARU, D. et al. Towards stronger data security in an eid management infrastructure. In: *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. [S.l.: s.n.], 2017. p. 391–395. 8
- [26] RATH, C.; NIEDERMAIR, T.; ZEFFERER, T. Towards a personal security device. In: BARTHE, G.; MARKATOS, E.; SAMARATI, P. (Ed.). *Security and Trust Management*. Cham: Springer International Publishing, 2016. p. 1–16. ISBN 978-3-319-46598-2. 8
- [27] SHEHU, A.-s.; PINTO, A.; CORREIA, M. E. On the interoperability of european national identity cards. In: NOVAIS, P. et al. (Ed.). *Ambient Intelligence – Software and Applications – 9th International Symposium on Ambient Intelligence*. Cham: Springer International Publishing, 2019. p. 338–348. ISBN 978-3-030-01746-0. 8
- [28] FILHO, W. P.; RIBEIRO, C.; ZEFFERER, T. Privacy-preserving attribute aggregation in eid federations. *Future Generation Computer Systems*, v. 92, 09 2018. 8, 9
- [29] PRŭŠA, J. E-identity: Basic building block of e-government. In: *2015 IST-Africa Conference*. [S.l.: s.n.], 2015. p. 1–10. 8
- [30] NIELSEN, M. M. Tackling identity management, service delivery, and social security challenges: Technology trends and partnership models. In: *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*. New York, NY, USA: Association for Computing Machinery, 2019. (ICEGOV2019), p. 1–5. ISBN 9781450366441. Disponível em: <<https://doi.org/10.1145/3326365.3326366>>. 8, 13, 28
- [31] Yuan Cao; Lin Yang. A survey of identity management technology. In: *2010 IEEE International Conference on Information Theory and Information Security*. [S.l.: s.n.], 2010. p. 287–293. 9, 13, 15, 28
- [32] LI, J. et al. Survey of research on identity management. *Computer Engineering and Design*, v. 6, 2009. 9, 13, 15
- [33] LEE, S. *An Introduction to Identity Management*. 2017. Disponível em: <<https://www.csoonline.com/article/2122096/an-introduction-to-identity-management.html>>. Acesso em: 2020-08-03. 9
- [34] WU, X. et al. Research of eid mobile identity authentication method. In: YUEMING, L.; XU, W.; XI, Z. (Ed.). *Trustworthy Computing and Services*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015. p. 350–358. ISBN 978-3-662-47401-3. 9

- [35] PARK, N.; LEE, D. Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. *Personal and Ubiquitous Computing*, v. 22, 03 2017. 9
- [36] WORLD BANK. Privacy by design : Current practices in estonia, india, and austria. 2018. Disponível em: <<https://openknowledge.worldbank.org/handle/10986/31053>>. Acesso em: 29 jul. 2020. 9
- [37] CALO, M. Digital market manipulation. *SSRN Electronic Journal*, v. 82, 01 2013. 9
- [38] ZARSKY, T. Privacy and manipulation in the digital age. *Theoretical Inquiries in Law*, v. 20, p. 157–188, 03 2019. 9
- [39] BLANCO, A. G. *Personal data theft: How can I protect myself?* 2017. Disponível em: <<https://www.bbva.com/en/personal-data-theft-can-protect/>>. Acesso em: 14 out. 2020. 9
- [40] PARLIAMENT, E.; UNION, C. of the E. Regulation (eu) 2016/679. *General Data Protection Regulation, European Union*, 2016. Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>. Acesso em: 06 jun. 2021. 9, 21, 32
- [41] IETF. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. *Internet Engineering Task Force*, 2008. Disponível em: <<https://tools.ietf.org/html/rfc5280>>. Acesso em: 06 jun. 2020. 11
- [42] CHANDRA, S. et al. A comparative survey of symmetric and asymmetric key cryptography. In: . [S.l.: s.n.], 2014. 11
- [43] ALBARQI, A. et al. Public key infrastructure: A survey. *Journal of Information Security*, v. 06, p. 31–37, 01 2015. 11
- [44] IETF. The secure sockets layer (ssl) protocol version 3.0. *Internet Engineering Task Force*, 2011. Disponível em: <<https://tools.ietf.org/html/rfc6101>>. Acesso em: 06 jun. 2020. 11
- [45] IETF. The transport layer security (tls) protocol version 1.3. *Internet Engineering Task Force*, 2018. Disponível em: <<https://tools.ietf.org/html/rfc8446>>. Acesso em: 06 jun. 2020. 11
- [46] BRASIL. Medida provisória nº 2.200-2. *Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, Presidência da República*, 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/MPV/Antigas2001/2200-2.htm>. Acesso em: 24 maio. 2021. 11
- [47] ITI, I. N. de Tecnologia da I. *ITI em Números*. 2020. Disponível em: <<https://numeros.iti.gov.br/>>. Acesso em: 02 jun. 2021. 12
- [48] IBGE. Projeção da população. *Instituto Brasileiro de Geografia e Estatística*, 2021. Disponível em: <<https://www.ibge.gov.br/apps/populacao/projecao/index.html>>. Acesso em: 16 mar. 2021. 12

- [49] BRASIL. Lei nº 14.063. *Uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos*, , *Presidência da República*, 2020. Disponível em: <<https://www.in.gov.br/en/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931>>. Acesso em: 24 maio. 2021. 12
- [50] BRASIL. Lei nº 14.129. *Princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública*, *Presidência da República*, 2021. Disponível em: <<https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132>>. Acesso em: 24 maio. 2021. 12
- [51] JøSANG, A.; POPE, S. User centric identity management. *AusCERT Conference 2005*, 01 2005. 14, 15, 16, 17
- [52] Ahn, G.; Ko, M. User-centric privacy management for federated identity management. In: *2007 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2007)*. [S.l.: s.n.], 2007. p. 187–195. 15
- [53] JENSEN, J. Federated identity management challenges. *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*, p. 230–235, 08 2012. 15, 16
- [54] CHADWICK, D. Federated identity management. *IEEE Computer - COMPUTER*, v. 38, p. 96–120, 08 2009. 16
- [55] OPENID. What is openid? 2021. Disponível em: <<https://openid.net/what-is-openid/>>. Acesso em: 22 set. 2021. 17
- [56] OAUTH. Oauth 2.0. 2021. Disponível em: <<https://oauth.net/2/>>. Acesso em: 22 set. 2021. 17
- [57] ALLIANCE, F. How fido works. 2021. Disponível em: <<https://fidoalliance.org/how-fido-works/>>. Acesso em: 22 set. 2021. 17
- [58] MÜHLE, A. et al. A survey on essential components of a self-sovereign identity. *Computer Science Review*, v. 30, p. 80–86, 11 2018. 17, 18, 19
- [59] TOBIN, A.; REED, D. The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, v. 29, n. 2016, 2016. 18
- [60] ISIROVA, K.; POTIL, O. Decentralized public key infrastructure development principles. In: . [S.l.: s.n.], 2018. p. 305–310. 19
- [61] W3C. *Verifiable Credentials Data Model 1.0*. 2019. Disponível em: <<https://www.w3.org/TR/vc-data-model/>>. Acesso em: 17 fev. 2021. 19
- [62] EVERNYM. A gentle introduction to verifiable credentials. 2019. Disponível em: <<https://www.evernym.com/blog/gentle-introduction-verifiable-credentials>>. Acesso em: 29 jul. 2020. 19

- [63] PWNEED, H. I. B. Have i been pwned: Check if your email has been compromised in a data breach. 2021. Disponível em: <<https://haveibeenpwned.com>>. Acesso em: 22 set. 2021. 20
- [64] AXUR. Has your password been leaked? 2021. Disponível em: <<https://mypwd.io>>. Acesso em: 22 set. 2021. 20
- [65] LEAKCHECK. Make sure your credentials haven't been compromised. leakcheck security services. 2021. Disponível em: <<https://leakcheck.net>>. Acesso em: 22 set. 2021. 20
- [66] IETF, I. E. T. F. A one-time password system. 1998. Disponível em: <<https://datatracker.ietf.org/doc/html/rfc2289>>. Acesso em: 24 maio. 2021. 20
- [67] LAMPORT, L. Password authentication with insecure communication. *Communications of the ACM*, ACM New York, NY, USA, v. 24, n. 11, p. 770–772, 1981. 20
- [68] YEH, T.-C.; SHEN, H.-Y.; HWANG, J.-J. A secure one-time password authentication scheme using smart cards. *IEICE Transactions on Communications*, The Institute of Electronics, Information and Communication Engineers, v. 85, n. 11, p. 2515–2518, 2002. 20
- [69] M'RAIHI, D. et al. Hotp: An hmac-based one-time password algorithm. *The Internet Society, Network Working Group. RFC4226*, 2005. 20, 21
- [70] M'RAIHI, D. et al. Totp: Time-based one-time password algorithm. *Internet Request for Comments*, 2011. 20, 21
- [71] GRASSI, P. et al. *Digital Identity Guidelines: Authentication and Lifecycle Management*. [S.l.: s.n.], 2017. 21
- [72] JAIN, A. K.; FLYNN, P.; ROSS, A. A. *Handbook of biometrics*. [S.l.]: Springer Science & Business Media, 2007. 21
- [73] MILKA, G. Anatomy of account takeover. In: *Enigma 2018 (Enigma 2018)*. Santa Clara, CA: USENIX Association, 2018. Disponível em: <<https://www.usenix.org/node/208154>>. 22
- [74] GOOGLE. A simpler and safer future — without passwords. *Safety Security*, 2021. Disponível em: <<https://blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords>>. Acesso em: 03 jun. 2021. 22
- [75] FERENHOF, H. A.; FERNANDES, R. F. Desmistificando a revisão de literatura como base para redação científica: método ssf. *Revista ACB*, Biblioteconomia em Santa Catarina Florianópolis, v. 21, n. 3, p. 550–563, 2016. 22
- [76] MARIANO, A.; SANTOS, M. Revisão da literatura: Apresentação de uma abordagem integradora. 09 2017. 23
- [77] PETERSEN, K. et al. Systematic mapping studies in software engineering. In: . Swindon, GBR: BCS Learning amp; Development Ltd., 2008. (EASE'08), p. 68–77. 23

- [78] KITCHENHAM, B. A.; BUDGEN, D.; BRERETON, O. P. The value of mapping studies: A participantobserver case study. In: . Swindon, GBR: BCS Learning amp; Development Ltd., 2010. (EASE'10), p. 25–33. 23
- [79] STATISTA. Smartphone users worldwide 2020. 2020. Disponível em: <<https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>>. Acesso em: 17 jul. 2020. 23
- [80] ANATEL. Relatório de acompanhamento do setor de telecomunicações. *Agência Nacional de Telecomunicações*, 2019. Disponível em: <<https://www.anatel.gov.br/dados/relatorios-de-acompanhamento/2019>>. Acesso em: 17 jul. 2020. 23
- [81] STEINBOCK, D. Tagcrowd: create your own word cloud from any text. 2021. Disponível em: <<https://tagcrowd.com>>. Acesso em: 22 set. 2021. 24
- [82] FERDOUS, M. S.; POET, R. A comparative analysis of identity management systems. In: *2012 International Conference on High Performance Computing Simulation (HPCS)*. [S.l.: s.n.], 2012. p. 454–461. 25, 30, 34
- [83] DUTSON, J. et al. Don't punish all of us: Measuring user attitudes about two-factor authentication. In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. [S.l.: s.n.], 2019. p. 119–128. 26
- [84] DUO. Two-factor authentication endpoint security. 2021. Disponível em: <<https://duo.com>>. Acesso em: 07 jul. 2021. 26, 43
- [85] YUBICO. Discover yubikey 5 | strong authentication for secure login. 2021. Disponível em: <<https://www.yubico.com/products/yubikey-5-overview/>>. Acesso em: 07 jul. 2021. 26
- [86] GOOGLE. Security key. 2021. Disponível em: <<https://cloud.google.com/titan-security-key>>. Acesso em: 07 jul. 2021. 26
- [87] CHEN, L. et al. Continuous authentication based on user interaction behavior. In: *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. [S.l.: s.n.], 2019. p. 1–6. 26
- [88] SHAN, C. P. et al. Automated login method selection in a multi-modal authentication system: Login method selection based on user behavior. In: *2019 IEEE 9th Symposium on Computer Applications Industrial Electronics (ISCAIE)*. [S.l.: s.n.], 2019. p. 120–124. 26
- [89] SAE-BAE, N. et al. Emerging nui-based methods for user authentication: A new taxonomy and survey. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, v. 1, n. 1, p. 5–31, 2019. 26
- [90] DAS, S. et al. Evaluating user perception of multi-factor authentication: A systematic review. *arXiv preprint arXiv:1908.05901*, 2019. 28

- [91] DAS, S.; WANG, B.; CAMP, L. J. Mfa is a waste of time! understanding negative connotation towards mfa applications via user generated content. In: *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*. [S.l.: s.n.], 2019. 28
- [92] LINÁKER, J. et al. *Guidelines for Conducting Surveys in Software Engineering*. [S.l.: s.n.], 2015. 29
- [93] JOSHI, A. et al. Likert scale: Explored and explained. *British Journal of Applied Science Technology*, v. 7, p. 396–403, 01 2015. 29
- [94] KASUNIC, M. Designing an Effective Survey. 9 2005. Disponível em: <https://kilthub.cmu.edu/articles/journal_contribution/Designing_an_Effective_Survey/6573062>. Acesso em: 10 out. 2020. 29
- [95] CAVOUKIAN, A. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, v. 5, 2009. 29
- [96] LOGMELN. Lastpass. *Gerenciador de senhas*, 2021. Disponível em: <<https://www.lastpass.com>>. Acesso em: 24 jul. 2021. 30
- [97] 1PASSWORD. 1password. *Password Manager for Families, Businesses, Teams*, 2021. Disponível em: <<https://1password.com>>. Acesso em: 24 jul. 2021. 30
- [98] DASHLANE, S. Dashlane. *Aplicativo de gerenciador de senhas para casa, dispositivos móveis, empresa*, 2021. Disponível em: <<https://www.dashlane.com>>. Acesso em: 24 jul. 2021. 30
- [99] UNB. Avaliação das atividades letivas do 1/2020. *Universidade de Brasília*, 2020. Disponível em: <<https://questionarios.unb.br/index.php/358886>>. Acesso em: 15 abr. 2020. 32
- [100] MCCANDLESS, T. E. D. *World's Biggest Data Breaches Hacks*. 2021. Disponível em: <<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks>>. Acesso em: 16 out. 2021. 36
- [101] AXUR. *Relatório de vazamento de dados no Brasil*. 2021. Disponível em: <<https://conteudo.axur.com/pt-br/vazamento-de-dados-no-brasil-2021>>. Acesso em: 16 out. 2021. 36
- [102] STACK OVERFLOW. Developer survey. 2021. Disponível em: <<https://insights.stackoverflow.com/survey/2021most-popular-technologies-language-prof>>. Acesso em: 12 set. 2021. 40
- [103] DOCKER. Empowering app development for developers. *Docker Inc.*, 2021. Disponível em: <<https://www.docker.com/>>. Acesso em: 24 out. 2021. 42
- [104] AUTH0. Auth0: Secure access for everyone. but not just anyone. *Auth0 Inc.*, 2021. Disponível em: <<https://auth0.com/>>. Acesso em: 24 out. 2021. 43

- [105] KASPERSKY. Password check. *Kaspersky Lab*, 2021. Disponível em: <<https://password.kaspersky.com/pt/>>. Acesso em: 22 set. 2021. 44
- [106] SECURITY.ORG. How secure is my password? 2021. Disponível em: <<https://www.security.org/how-secure-is-my-password/>>. Acesso em: 22 set. 2021. 44
- [107] MY1LOGIN. Password strength meter. 2021. Disponível em: <<https://www.my1login.com/resources/password-strength-test>>. Acesso em: 22 set. 2021. 44

Apêndice A

Termo de Consentimento Livre e Esclarecido do Questionário

Esta pesquisa faz parte do trabalho de conclusão do curso de mestrado no Programa de Pós-Graduação em Computação Aplicada do Departamento de Ciência da Computação, da Universidade de Brasília (UnB).

O objetivo principal desta pesquisa é investigar o seu comportamento em relação a soluções que permitem que você se identifique para acessar serviços on-line. Serão inspecionados aspectos como segurança, privacidade e experiência de uso.

O respeito a sua privacidade é fundamental. Assim, as respostas serão tratadas de forma anônima e confidencial, sendo utilizadas estritamente para fins da realização da pesquisa acadêmica. Você poderá deixar de participar da pesquisa a qualquer momento, sem prejuízos. Para mais informações, sugestões ou comentários, envie um e-mail para: ronald.ecomp@gmail.com.

Apêndice B

Formulário do Questionário

Pesquisa acadêmica sobre o processo de identificação em serviços online

Olá,

esta pesquisa faz parte do trabalho de conclusão do curso de mestrado no Programa de Pós-graduação em Computação Aplicada da Universidade de Brasília (UnB).

O tempo aproximado para as respostas é de 5 minutos.

O objetivo principal desta pesquisa é investigar o seu comportamento em relação a soluções que permitem que você se identifique para acessar serviços online. Serão inspecionados aspectos como segurança, privacidade e experiência de uso.

O respeito a sua privacidade é fundamental. Assim, as respostas aqui informadas são anônimas e desta forma a sua identidade é preservada. Solicitamos que leia e aceite o Termo de Consentimento Livre e Esclarecido disponível no link <https://bit.ly/3pJclZU>.

Ao clicar no botão Próxima, estou de acordo em participar da pesquisa.

***Obrigatório**

Informações sobre você

1. Qual a sua faixa etária? *

Marcar apenas uma oval.

- 18 a 24 anos
- 25 a 39 anos
- 40 a 59 anos
- Acima de 60 anos

2. Com qual gênero você mais se identifica? *

Marcar apenas uma oval.

- Masculino
- Feminino
- Gostaria de me identificar de outra forma

3. Qual seu nível de formação? *

Marcar apenas uma oval.

- Ensino fundamental
- Ensino médio
- Ensino superior
- Pós-graduação

4. Qual a sua área de atuação? *

Marcar apenas uma oval.

- Tecnologia da Informação
- Outras áreas

Sua relação com processos de login

5. Você se sente confortável com o processo de login utilizando nome de usuário e senha *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Concordo fortemente

6. Frequentemente esqueço das minhas senhas nos serviços online *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Concordo fortemente

15. Me preocupo mais com o vazamento de um cadastro de impressões digitais e reconhecimento facial do que com o vazamento de uma senha *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Concordo fortemente

Este conteúdo não foi criado nem aprovado pelo Google.

Google Formulários

Apêndice C

Termo de Consentimento Livre e Esclarecido do Experimento

Você está sendo convidado a participar da pesquisa “Autenticação em sistemas de gerenciamento de identidades sob a perspectiva dos usuários finais”, de responsabilidade de Ronald Carvalho Ribeiro de Araujo, estudante de mestrado da Universidade de Brasília. O objetivo desta pesquisa é investigar sua satisfação em relação a diferentes métodos de autenticação. Assim, gostaria de consultá-lo/a sobre seu interesse e disponibilidade de cooperar com a pesquisa.

O respeito a sua privacidade é fundamental. Assim, suas respostas serão utilizadas estritamente para fins da realização da pesquisa acadêmica. Você receberá todos os esclarecimentos necessários antes, durante e após a finalização da pesquisa, e lhe asseguro que o seu nome não será divulgado, sendo mantido o mais rigoroso sigilo mediante a omissão total de informações que permitam identificá-lo/a. Os dados provenientes de sua participação na pesquisa ficarão sob a guarda do pesquisador responsável pela pesquisa.

A coleta de dados será realizada por meio de um experimento que envolve diferentes tipos de autenticação em sistemas on-line. É para estes procedimentos que você está sendo convidado a participar. Sua participação na pesquisa não implica em nenhum risco identificado.

Espera-se, com esta pesquisa, entender o comportamento dos usuários quando deparados com diferentes métodos de autenticação e, desta forma, apresentar caminhos para a elaboração de soluções que possam ser mais eficientes no atendimento das necessidades dos usuários finais.

Sua participação é voluntária e livre de qualquer remuneração ou benefício. Você é livre para recusar-se a participar, retirar seu consentimento ou interromper sua participação a qualquer momento. A recusa em participar não acarretará qualquer penalidade ou perda de benefícios.

Se você tiver qualquer dúvida em relação à pesquisa, você pode me contatar através do telefone 61 98221-3620 ou pelo e-mail ronald.ecomp@gmail.com.

Apêndice D

Documentação da API do Experimento

uAUTH Experimento

Experimento de autenticação que investiga o comportamento dos usuários quando deparados com diferentes métodos de autenticação. São observados os comportamentos relativos a experiência de uso, segurança e privacidade.

/ hello

verificação da disponibilidade da API

Method: GET
Type:
URL: localhost:3000/auth/hello/

/ info

Recupera informações sobre um determinado link de autenticação

Method: GET
Type:
URL: localhost:3000/auth/info/:codigoLink

Parâmetros:

Nome	Descrição
codigoLink	código que identifica uma solicitação de autenticação

/ inicializar-usuario

Indica o usuário como inicializado no experimento.

Method: PUT
Type:
URL: localhost:3000/auth/usuario/inicializar/:idUserario

Parâmetros:

Nome	Descrição
idUserario	identificador do usuário

/ notificacao

Notifica os usuários que possuem autenticações pendentes para o turno informado. As notificações são realizadas via SMS e contém o a URL para acesso a uma determinada autenticação.

Method: GET

Type:

URL: localhost:3000/auth/notificacao/:turnoEnvio

Parâmetros:

Nome	Descrição
turnoEnvio	Turno de envio da mensagem. Assume os valores MANHA e TARDE

/ notificar-usuario

Notifica os usuários via SMS que o experimento esta próximo de ser iniciado. Os usuários só serão notificados uma única vez.

Method: PUT

Type:

URL: localhost:3000/auth/usuario/notificar

/ usuario-config

Efetua o cadastro de um usuário no experimento e gera entradas na tabela de autenticações de acordo com a configuração de tipos de autenticações e quantidade.

Method: POST

URL: localhost:3000/auth/usuario/config

Cabeçalhos:

Nome	Descrição
Authorization	token de autorização para realizar a ação

Corpo:

```
{
  "usuario": {
    "nome": "Brasiliano Ficticio da Silva",
    "cpf": "48379975030",
    "celular": "99999999999",
    "area_atuacao": "TI",
    "autenticacoes": {
      "tipos": ["SENHA", "CODIGO_ACESSO", "FACE", "SENHA_CODIGO_ACESSO"],
      "quantidade": 2
    }
  }
}
```

/ auth-2fa-1-password

Realiza a primeira parte da autenticação com duplo fator de autenticação. A primeira validação é realizada utilizando senha

Method: PUT

URL: localhost:3000/auth/2fa/password/:idUsuario/:idAutenticacao

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário
idAutenticacao	Identificador da autenticação em curso

Corpo:

```
{
  "cpf": "48379975030",
  "senha": "Abcd1234@"
}
```

/ auth-2fa-2-otp

Realiza a segunda parte da autenticação com duplo fator de autenticação. A segunda validação é realizada utilizando código de acesso

Method: PUT

URL: localhost:3000/auth/2fa/otp/:idUsuario/:idAutenticacao

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário
idAutenticacao	Identificador da autenticação em curso

Corpo:

```
{  
  "otp": "823915"  
}
```

/ auth-facial

Realiza a autenticação utilizando a face do usuário

Method: PUT

URL: localhost:3000/auth/facial/:idUsuario

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário

Corpo:

```
{  
  "cpf": "00801812526"  
}
```

/ auth-otp

Realiza a autenticação do usuário utilizando código de acesso

Method: PUT

URL: localhost:3000/auth/otp/:idUsuario/:idAutenticacao

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário
idAutenticacao	Identificador da autenticação em curso

Corpo:

```
{  
  "otp": "823915"  
}
```

/ auth-password

Realiza a autenticação de um usuário utilizando senha

Method: PUT

URL: localhost:3000/auth/password/:idUsuario/:idAutenticacao

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário
idAutenticacao	Identificador da autenticação em curso

Corpo:

```
{  
  "cpf": "48379975030",  
  "senha": "Abcd1234@"  
}
```

/ config-password

Define/Redefine a senha do usuário em questão

Method: PUT

URL: localhost:3000/auth/config/password/:idUsuario/:idAutenticacao

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário
idAutenticacao	Identificador da autenticação em curso

Corpo:

```
{  
  "password": "Abcd1234@"  
}
```

/ enviar-otp

Gera o código de acesso para o usuário e encaminha via SMS

Method: GET
URL: localhost:3000/auth/otp/:idUsuario/:cpf

Parâmetros:

Nome	Descrição
idUsuario	Identificador do usuário
cpf	CPF do usuário

/ feedback

Registra a avaliação do usuário com relação a autenticação. A duração é registrada em milissegundos

Method: PUT
URL: localhost:3000/auth/feedback/:idAutenticacao

Parâmetros:

Nome	Descrição
idAutenticacao	Identificador da autenticação em curso

Corpo:

```
{  
  "avaliacao": "5",  
  "duracao": "10000"  
}
```

Apêndice E

Dicionário de Dados das Tabelas do Experimento

TABELA: usuarios

COLUNA	DESCRIÇÃO
id	Identificador único
nome	Nome do participante
cpf	CPF do participante
celular	Celular do participante
senha	Senha definida pelo participante na primeira interação que envolva senha ou na redefinição de senha. Pode ser uma autenticação do tipo SENHA ou CODIGO_ACESSO_SENHA
area_atuacao	Área de atuação do participante: TI OUTRAS
inicializado	Indica que o participante já iniciou sua participação com aceitação do TCLA
notificado	Indica que o participante já foi notificado da proximidade do início do experimento

TABELA: autenticacoes

COLUNA	DESCRIÇÃO
Nome da coluna	Comentário
id	Identificador único
tipo	Método de autenticação utilizado: SENHA CODIGO_ACESSO SENHA_CODIGO_ACESSO FACE
codigo_link	Código aleatório composto por 6 caracteres e sufixo do link de acesso para autenticação
avaliacao	Avaliação do usuário final com relação a experiência de uso
data	Momento em que foi realizada a autenticação
id_usuario	Identificador do usuário que realizou a autenticação
pendente	Autenticação ainda não realizada
duracao	Duração em milisegundos do processo de autenticação
turno_preferencial	Turno preferencial para notificação automática: MANHA TARDE
qtd_falha_credencial	Quantidade de falhas de acesso devido a credencial incorreta
qtd_recuperacao_credencial	Quantidade de vezes que o usuário acionou o mecanismo de recuperação da credencial
avaliacao_seguranca	Avaliação do usuário final com relação a segurança
avaliacao_privacidade	Avaliação do usuário final com relação a privacidade