

Universidade de Brasília

Instituto de Ciências Exatas  
Departamento de Ciência da Computação

**Análise da usabilidade da Conta gov.br para adoção  
pelo Senado Federal**

Demétrius de Almeida Jubé

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

Orientadora  
Prof.a Dr.a Letícia Lopes Leite

Brasília  
2025

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

J91a Jubé, Demétrius de Almeida  
Análise da usabilidade da Conta gov.br para adoção pelo  
Senado Federal / Demétrius de Almeida Jubé; orientador  
Letícia Lopes Leite. Brasília, 2025.  
219 p.

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

1. Teste de Usabilidade. 2. Login Único. 3. Conta gov.br.  
4. Serviços Públicos Digitais. I. Leite, Letícia Lopes,  
orient. II. Título.



# Dedicatória

À minha família, pelo alicerce.

À Lorena, pela parceria, pelo amor e por acreditar comigo em cada etapa.

Aos meus filhos, Eduardo e Sofia, por me lembrarem todos os dias do que realmente importa.

Esta conquista também é de vocês.

# Agradecimentos

A realização deste trabalho só foi possível graças ao apoio e à colaboração de muitas pessoas, às quais registro aqui minha sincera gratidão.

À minha orientadora, professora Letícia Lopes Leite, agradeço profundamente pela confiança, orientação cuidadosa e pela forma generosa com que compartilhou seu conhecimento ao longo de todo o processo. Suas contribuições foram fundamentais para o amadurecimento desta pesquisa e para minha formação acadêmica.

Agradeço também aos professores que compuseram a banca avaliadora, Márcia Moraes e Edison Ishikawa, pelas valiosas observações e sugestões, que enriqueceram significativamente o trabalho. E também à professora Thérèse Hofmann, que me guiou no caminho para a submissão ao Comitê de Ética em Pesquisa da UnB.

Ao Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília, deixo meu reconhecimento pela excelência da formação oferecida, assim como aos colegas da turma de 2022, pelo companheirismo durante a jornada.

Aos colegas do Senado Federal, em especial do Instituto DataSenado, Coordenação do Programa e-Cidadania e Serviço de Soluções Para Portais, meu agradecimento especial pelo apoio técnico e pela parceria que viabilizou parte essencial da pesquisa. Aos participantes dos testes de usabilidade, que gentilmente doaram seu tempo, deixo minha gratidão.

Por fim, agradeço à minha família e aos meus amigos, pelo suporte constante e pela paciência nos momentos de ausência. A você, Lorena, meu amor, obrigado por caminhar comigo com tanto afeto, incentivo e compreensão. Ao Eduardo e à Sofia, meus filhos, obrigado por compreenderem os momentos em que não pudemos brincar juntos, e por me inspirarem diariamente a alcançar este objetivo.

# Resumo

O Governo Federal do Brasil iniciou, em 2016, a criação da ferramenta de Login Único **Conta gov.br**, com o propósito de racionalizar o cadastro dos cidadãos em serviços públicos digitais e aprimorar sua experiência de uso. Nesse contexto, este trabalho avaliou os possíveis benefícios da integração dessa solução ao sistema e-Cidadania, do Senado Federal, com foco na usabilidade — fator que influencia diretamente a aceitação e o uso de novas funcionalidades. A pesquisa abrangeu o estudo de fundamentos teóricos sobre soluções de *Single Sign-On*, bem como das técnicas e métricas aplicadas na avaliação de usabilidade. Para subsidiar o desenvolvimento do protocolo de testes, foi conduzida uma Revisão Sistemática da Literatura (RSL) sobre estudos publicados nos últimos dez anos, cujos resultados destacaram a relevância de diretrizes éticas, roteiros estruturados de tarefas, aplicação de escalas do tipo Likert e oferta de compensações aos participantes. Com base nesses achados, foi elaborado e executado um protocolo experimental com 30 participantes de diferentes regiões do Brasil. Os testes revelaram que ambas as formas de autenticação (**Conta gov.br** e E-mail/Senha) apresentaram níveis semelhantes de usabilidade, com pontuações médias classificadas como *Best Imaginable* na *System Usability Scale* (SUS). A avaliação da facilidade de uso percebida (SEQ), cuja escala varia de 1 (Muito Difícil) a 7 (Muito Fácil), também apresentou médias próximas da graduação “Muito Fácil”. As diferenças entre os métodos não foram estatisticamente significativas nas métricas mencionadas, contudo o tempo de autenticação foi significativamente maior com a **Conta gov.br**, superando em mais do que o dobro o tempo necessário na autenticação por E-mail e Senha. Análises complementares identificaram correlações entre as métricas de usabilidade e fatores demográficos, como idade e familiaridade tecnológica, indicando que a compreensão do perfil do público-alvo pode mitigar riscos associados à adoção dessa integração. Além disso, a pesquisa resultou na elaboração de um Guia Prático que reúne orientações técnicas e dados de usabilidade para apoiar a adoção da **Conta gov.br** em sistemas públicos.

**Palavras-chave:** Login Único, Conta gov.br, e-Cidadania, Teste de Usabilidade, Revisão Sistemática da Literatura

# Abstract

In 2016, the Brazilian Federal Government launched the development of a Single Sign-On (SSO) platform—Conta gov.br—aiming to streamline user registration for digital public services and improve the overall user experience. This dissertation investigates the potential benefits and challenges of integrating *Conta gov.br* into the *e-Cidadania* platform of the Federal Senate, with a particular focus on usability, a critical factor influencing user acceptance and sustained engagement. The research involved a theoretical review of SSO solutions, including usability assessment techniques and metrics. To support the experimental design, a Systematic Literature Review (SLR) was conducted, analyzing studies from the past decade and identifying methodological patterns such as the importance of ethical compliance, structured task scenarios, Likert-type scales, and participant compensation. Based on this foundation, a usability test protocol was developed and applied to 30 participants from various regions of Brazil. The experiment compared *Conta gov.br* authentication with traditional email/password login, using the System Usability Scale (SUS) and Single Ease Question (SEQ) to measure perceived usability. Both methods achieved average SUS scores classified as Best Imaginable and SEQ ratings close to Very Easy, with no statistically significant differences between them. However, authentication time using *Conta gov.br* was more than twice as long. Additional analysis revealed correlations between usability metrics and participant characteristics such as age and technological familiarity, underscoring the importance of understanding user demographics when designing for adoption. As a practical contribution, the study produced a Technical Guide compiling usability findings and implementation recommendations to assist public institutions in evaluating the viability of *Conta gov.br* integration.

**Keywords:** *Single Sign-On, gov.br Account, e-Cidadania, Usability Testing, Systematic Literature Review*

# Sumário

<b>1</b>	<b>Introdução</b>	<b>1</b>
1.1	Problema de Pesquisa . . . . .	4
1.2	Justificativa . . . . .	4
1.3	Objetivos . . . . .	5
1.3.1	Objetivo Geral . . . . .	5
1.3.2	Objetivos Específicos . . . . .	5
1.4	Resultados Esperados . . . . .	5
1.5	Metodologia de Pesquisa . . . . .	6
1.6	Estrutura do Trabalho . . . . .	7
<b>2</b>	<b>Embasamento</b>	<b>8</b>
2.1	Autenticação e Autorização . . . . .	8
2.1.1	<i>Single Sign-On</i> . . . . .	11
2.1.2	Implementações de <i>Single Sign-On</i> . . . . .	12
2.1.3	Conta gov.br . . . . .	19
2.2	Interação Humano-Computador (IHC) . . . . .	27
2.2.1	Usabilidade . . . . .	28
2.2.2	Testes de usabilidade . . . . .	29
2.3	Métodos de Teste de Usabilidade . . . . .	29
2.3.1	Avaliação Heurística . . . . .	30
2.3.2	<i>Cognitive Walkthrough</i> . . . . .	30
2.3.3	<i>Contextual Inquiry</i> . . . . .	31
2.3.4	Avaliação de Usuários . . . . .	33
2.4	Métricas de Aferição de Usabilidade . . . . .	43
2.4.1	Eficácia . . . . .	44
2.4.2	Eficiência . . . . .	44
2.4.3	Satisfação . . . . .	45
2.5	Síntese do Capítulo . . . . .	46

<b>3</b>	<b>Revisão Sistemática de Literatura</b>	<b>48</b>
3.1	Planejamento . . . . .	49
3.1.1	Objetivo . . . . .	49
3.1.2	Questões de Pesquisa . . . . .	49
3.1.3	Definição da <i>String</i> de Busca . . . . .	50
3.1.4	Critérios de Seleção . . . . .	56
3.1.5	Bases de Pesquisa . . . . .	57
3.1.6	Estratégia de Pesquisa . . . . .	58
3.1.7	Mensuração da qualidade dos estudos e definição dos formulários de extração dos dados . . . . .	59
3.2	Condução . . . . .	60
3.2.1	Triagem do <i>Abstract</i> . . . . .	60
3.2.2	Triagem do arquivo da publicação . . . . .	65
3.2.3	Controle de qualidade . . . . .	66
3.2.4	Análise dos dados . . . . .	68
3.3	Síntese do Capítulo . . . . .	79
<b>4</b>	<b>Metodologia proposta</b>	<b>81</b>
4.1	Protocolo de Teste de Usabilidade . . . . .	81
4.2	Configuração do Estudo-Piloto . . . . .	85
4.3	Síntese do Capítulo . . . . .	92
<b>5</b>	<b>Análise dos Resultados</b>	<b>94</b>
5.1	Submissão ao Comitê de Ética . . . . .	94
5.2	Enquete do DataSenado . . . . .	96
5.3	Protocolo Final do Teste de Usabilidade . . . . .	99
5.3.1	Recrutamento . . . . .	99
5.3.2	Roteiro de aplicação . . . . .	100
5.4	Execução do teste de usabilidade . . . . .	107
5.4.1	Recrutamento dos participantes . . . . .	107
5.4.2	Análise Demográfica . . . . .	110
5.5	Resultados . . . . .	113
5.5.1	Usabilidade geral (SUS) . . . . .	113
5.5.2	Facilidade Percebida de Uso (SEQ) . . . . .	124
5.5.3	Tempo de Conclusão da Tarefa (TCT) . . . . .	127
5.6	Análise de Correlações . . . . .	136
5.7	Discussão . . . . .	147
5.8	Sugestões dos participantes . . . . .	151

5.9 Síntese do Capítulo . . . . .	153
<b>6 Conclusão</b>	<b>157</b>
<b>Referências</b>	<b>164</b>
<b>Apêndices</b>	<b>179</b>
<b>A Formulários de Pesquisa</b>	<b>180</b>
A.1 Formulário de Recrutamento . . . . .	180
A.2 Formulário de Avaliação da Sessão de Teste . . . . .	182
<b>B Termo de Consentimento Livre e Esclarecido</b>	<b>183</b>
<b>C Guia de Implantação da Conta gov.br</b>	<b>185</b>
C.1 Guia Prático para Adoção da <i>Conta gov.br</i> . . . . .	185

# Lista de Figuras

Figura 2.1	Fluxo de autenticação e autorização do <i>Single Sign-On</i> .. . . . .	11
Figura 2.2	Fluxo de autenticação do protocolo SAML.. . . . .	13
Figura 2.3	Fluxo de autenticação do protocolo OpenID.. . . . .	14
Figura 2.4	Fluxo de autenticação do protocolo OAuth.. . . . .	15
Figura 2.5	Fluxo de autenticação do protocolo <i>OpenID Connect</i> .. . . . .	17
Figura 2.6	Relação entre pares proporcionada pelo modelo de identidade des- centralizada.. . . . .	18
Figura 2.7	Catálogo de Confiabilidades da <b>Conta gov.br</b> , discriminando a relação entre os Níveis de Autenticação e os Selos de Confiabilidade.	20
Figura 2.8	Prerrogativas dos usuários da <b>Conta gov.br</b> por Nível de Auten- ticação. . . . .	21
Figura 2.9	Processo de avaliação de um serviço para integração com a <b>Conta gov.br</b> . . . . .	22
Figura 2.10	Fluxo de autenticação básico da <b>Conta gov.br</b> . . . . .	24
Figura 2.11	Autorização solicitada pelo sistema integrado para a <b>Conta gov.br</b> .	26
Figura 2.12	Processo de <i>Contextual Design</i> .. . . . .	32
Figura 2.13	Escala de adjetivos x pontuação SUS.. . . . .	41
Figura 2.14	O <i>Single Ease Question</i> - SEQ.. . . . .	46
Figura 3.1	Processo de RSL - Técnicas e Métricas de Usabilidade. . . . .	58
Figura 3.2	Tipos de conteúdo da base Springer Link . . . . .	61
Figura 3.3	Distribuição de resultados por base de pesquisa. . . . .	63
Figura 3.4	Estatística dos artigos excluídos X critério de exclusão. . . . .	64
Figura 3.5	Conferências com estudos de usabilidade e login por ano. . . . .	65
Figura 3.6	Evolução da triagem dos estudos da RSL. . . . .	68
Figura 3.7	Frequência de uso das técnicas de teste de usabilidade. . . . .	78
Figura 3.8	Frequência de métricas obtidas pela Revisão Sistemática de Lite- ratura. . . . .	78
Figura 5.1	Dados demográficos da enquete DataSenado.. . . . .	98

Figura 5.2	Resultado do envio do e-mail de recrutamento de participantes . . .	108
Figura 5.3	Dados de gênero e idade dos participantes . . . . .	111
Figura 5.4	Grau de instrução e habilidade com uso de tecnologia dos partici- pantes . . . . .	111
Figura 5.5	Região de nascimento e residência dos participantes . . . . .	112
Figura 5.6	Dados estatísticos da medição do SUS . . . . .	116
Figura 5.7	Comparação de percentis entre a <b>Conta gov.br</b> e o Email e Senha.	117
Figura 5.8	Impacto de cada pergunta para a avaliação de usabilidade da <b>Conta gov.br</b> e do Email e Senha. . . . .	119
Figura 5.9	Análise incremental do Alfa de Cronbach - E-mail e Senha. . . . .	123
Figura 5.10	Análise incremental do Alfa de Cronbach - <b>Conta gov.br</b> . . . . .	123
Figura 5.11	Média do SEQ para os cenários testados. . . . .	126
Figura 5.12	Tela de login - E-mail e Senha - Anterior . . . . .	127
Figura 5.13	Tela de login - E-mail e Senha - Atual . . . . .	127
Figura 5.14	Tela de login - <b>Conta gov.br</b> . . . . .	128
Figura 5.15	Tela de sucesso - E-mail e Senha - Anterior. . . . .	128
Figura 5.16	Tela de sucesso - E-mail e Senha - Atual. . . . .	128
Figura 5.17	Tela de sucesso - <b>Conta gov.br</b> - Anterior. . . . .	129
Figura 5.18	Tela de sucesso - <b>Conta gov.br</b> - Atual. . . . .	129
Figura 5.19	Diferença entre quadros no decorrer do tempo - Participante P1. . .	130
Figura 5.20	Distribuição dos tempos de conclusão da tarefa. . . . .	132
Figura 5.21	Tempo de conclusão mediano por cenário. . . . .	135
Figura 5.22	Correlação entre os resultados das métricas. . . . .	139
Figura 5.23	Correlação entre os dados demográficos e as métricas de usabilidade.	140
Figura 5.24	Dados de SEQ e TCT por gênero. . . . .	141
Figura 5.25	Dados de SUS e SEQ por faixa etária. . . . .	141
Figura 5.26	Dados de SEQ e TCT por grau de instrução. . . . .	142
Figura 5.27	Dados do SUS por nível de facilidade de uso de soluções de TI. . .	143
Figura 5.28	Dados do SEQ e TCT por nível de facilidade de uso de soluções de TI. . . . .	143
Figura 5.29	Resultado do SUS por região de nascimento e residência. . . . .	144
Figura 5.30	Resultado do SEQ por região de nascimento e residência. . . . .	144
Figura 5.31	Resultado do TCT por região de nascimento e residência. . . . .	145
Figura 5.32	Dados de Grau de instrução, Facilidade com tecnologia e Faixa etária por região. . . . .	146
Figura 5.33	Fluxo de páginas - Cenário <b>Conta gov.br</b> . . . . .	148
Figura 5.34	Fluxo de páginas - Cenário E-mail e senha. . . . .	149

# Lista de Quadros

Quadro 2.1	Análise dos modelos de autenticação com base em fatores que afetam a segurança. . . . .	10
Quadro 2.2	Perguntas do questionário SUS. . . . .	40
Quadro 3.1	Questões de Pesquisa da revisão de literatura. . . . .	50
Quadro 3.2	Orientação utilizada para os aspectos do PICOC. . . . .	50
Quadro 3.3	PICOC inicial utilizado para o estudo. . . . .	51
Quadro 3.4	Primeira adequação dos critérios PICOC, para expandir os resultados da <i>String</i> de Busca. . . . .	52
Quadro 3.5	Sinônimos utilizados para aumento da abrangência dos estudos. . . . .	53
Quadro 3.6	Lista de sinônimos final. . . . .	55
Quadro 3.7	Critérios de exclusão - RSL de Usabilidade. . . . .	57
Quadro 3.8	Pontuação dos estudos no controle de qualidade. . . . .	67
Quadro 3.9	Resumo de Técnicas e Métricas encontradas nos estudos. . . . .	77
Quadro 4.1	Descrição do Cenário de Teste de usabilidade - E-mail e senha e <b>Conta gov.br</b> . . . . .	91
Quadro 4.2	Perguntas do questionário SUS e SEQ adaptadas para a autenticação de e-mail e senha. . . . .	92
Quadro 5.1	Descrição do Teste de usabilidade - E-mail e senha e <b>Conta gov.br</b> . . . . .	107
Quadro 5.2	Entrevistas organizadas por cenário. . . . .	109
Quadro 5.3	Dados demográficos dos participantes da pesquisa. . . . .	110
Quadro 5.4	Fatos atípicos que ocorreram durante o teste. . . . .	134

# Lista de Tabelas

Tabela 3.1	Pontuação do <i>checklist</i> de qualidade. . . . .	59
Tabela 4.1	Percentual da população por gênero X Faixas de idade. . . . .	86
Tabela 4.2	Distribuição sugerida para execução do teste-piloto. . . . .	86
Tabela 5.1	Respostas SUS - Cenário E-mail e Senha. . . . .	114
Tabela 5.2	Respostas SUS - Cenário <b>Conta gov.br</b> . . . . .	115
Tabela 5.3	Estatísticas descritivas do SUS por cenário. . . . .	116
Tabela 5.4	Contribuições por questão respondida para a <b>Conta gov.br</b> e E-mail. . . . .	118
Tabela 5.5	Respostas SUS com perguntas de viés negativo normalizadas - Cenário E-mail e Senha. . . . .	121
Tabela 5.6	Respostas SUS com perguntas de viés negativo normalizadas - Cenário <b>Conta gov.br</b> . . . . .	122
Tabela 5.7	Respostas à pergunta SEQ para aferição da Facilidade Percebida. . . . .	125
Tabela 5.8	Estatísticas descritivas do SEQ para <b>Conta gov.br</b> e E-mail e senha. . . . .	125
Tabela 5.9	Tempos de Conclusão das Tarefas (em milissegundos). . . . .	131
Tabela 5.10	Estatísticas descritivas das diferenças de tempo (ms) entre os métodos. . . . .	132
Tabela 5.11	Médias e Mediana dos Tempos de Conclusão (ms). . . . .	135
Tabela 5.12	Intervalo de Confiança dos Tempos de Conclusão (ms). . . . .	135
Tabela 5.13	Resultado Consolidado das Métricas por Participante. . . . .	137
Tabela 5.14	Dados do Teste de Shapiro-Wilk no conjunto de resultados. . . . .	138
Tabela 5.15	Número de participantes por região de nascimento e residência. . . . .	145

# Lista de Abreviaturas e Siglas

**API** *Application Programming Interface.*

**CAFe** Comunidade Acadêmica Federada.

**CDH** Comissão de Direitos Humanos e Legislação Participativa.

**CEP/CHS** Comitê de Ética em Pesquisa em Ciências Humanas e Sociais.

**CIC** Departamento de Ciência da Computação.

**CIN** Carteira de Identidade Nacional.

**CNH** Carteira de Habilitação.

**CSRF** *Cross-Site Request Forgery.*

**CSV** *Comma-Separated Values.*

**DOI** *Digital Object Identifier.*

**DPKI** *Decentralized Public Key Infrastructure.*

**ENGD** Estratégia Nacional de Governo Digital.

**GTMI** *GovTech Maturity Index.*

**HCI** *Human-Computer Interaction.*

**HTTP** *Hypertext Transfer Protocol.*

**ICP-Brasil** Infraestrutura de Chaves Públicas Brasileira.

**IdP** *Identity Provider.*

**IHC** Interação Humano-Computador.

**INSS** Instituto Nacional do Seguro Social.

**IRB** *Internal Revision Board.*

**IUIPC** *Internet Users' Information Privacy Concerns.*

**JSON** *JavaScript Object Notation.*

**LGPD** Lei Geral de Proteção de Dados.

**NFC** *Near Field Communication.*

**OASIS** *Organization for the Advancement of Structured Information Standards.*

**OCR** *Optical Character Recognition.*

**OIDC** *OpenId Connect.*

**OP** *OpenId Provider.*

**PICOC** *Population, Intervention, Comparison, Outcome, Context.*

**PIN** *Personal Identification Number.*

**PKCE** *Proof Key for Code Exchange.*

**PPCA** Programa de Pós-Graduação em Computação Aplicada.

**QP** Questão de Pesquisa.

**REST** *Representational State Transfer.*

**RIS** *Research Information Systems.*

**RP** *Relying Party.*

**RQ** *Research Question.*

**RSL** Revisão Sistemática de Literatura.

**SAML** *Security Assertion Markup Language.*

**Senatran** Secretaria Nacional de Trânsito.

**SEQ** *Single Ease Question.*

**SGD** Secretaria de Governo Digital.

**SP** *Service Providers*.

**SSI** *Self-Sovereign Identity*.

**SSO** *Single Sign-On*.

**SUS** *System Usability Scale*.

**TCLE** Termo de Consentimento Livre e Esclarecido.

**TCT** Tempo de Conclusão da Tarefa.

**UnB** Universidade de Brasília.

**UX** *User Experience*.

**XML** *eXtensible Markup Language*.

**YOLO** *You Only Look Once*.

# Capítulo 1

## Introdução

Nos últimos anos, o Brasil tem passado por um processo crescente de digitalização de serviços públicos, adotando novas tecnologias e plataformas para facilitar o acesso dos cidadãos a esses serviços. Dados do *GovTech Maturity Index* (GTMI) de 2022, um indicador que o Banco Mundial utiliza para medir aspectos críticos de modernização de governos, mostram que o Brasil está no seletor grupo de *GovTech Leaders* [1]. Os países que fazem parte desse agrupamento têm uma grande maturidade em quatro áreas principais [2]:

1. Sistemas centrais do governo e plataformas digitais compartilhadas: essa área aborda a infraestrutura tecnológica básica, incluindo sistemas e plataformas que facilitam a comunicação, coordenação e integração entre diferentes órgãos e entidades governamentais.
2. Entrega de serviços on-line: o foco dessa área é a disponibilidade e qualidade dos serviços públicos oferecidos por meio de canais digitais, tais como portais governamentais e aplicativos móveis, permitindo que os cidadãos acessem informações e serviços de forma rápida e eficiente.
3. Engajamento digital do cidadão: abrange os mecanismos e ferramentas que permitem aos cidadãos participarem e colaborarem com o governo, como consultas públicas e fóruns de discussão, aprimorando a transparência, a responsabilização e a inclusão no processo decisório.
4. Facilitadores de GovTech: inclui políticas, regulamentações, investimentos e capacitações que promovem e incentivam o desenvolvimento e a adoção de soluções de GovTech, como políticas de dados abertos, investimentos em pesquisa e desenvolvimento, e formação de profissionais especializados.

É possível que a boa performance brasileira no GTMI esteja relacionada com a implantação da Estratégia de Governança Digital, que define objetivos e diretrizes para a trans-

formação digital do setor público no Brasil. Ela foi instituída pelo Decreto nº 8.638/2016 [3], e atualizada pelos Decretos nº 10.332/2020 [4], 10.996/2022 [5] e 11.260/2022 [6], quando passou a ser conhecida como Estratégia Nacional de Governo Digital - ENGD [7].

O principal objetivo de ENGD é melhorar a eficiência, a eficácia e a transparência dos serviços públicos, tornando-os mais acessíveis e amigáveis aos cidadãos e, como consequência, oferecer uma jornada de usuário mais agradável [4]. A estratégia abrange várias áreas de atuação, como: modernização e integração dos sistemas de governo; expansão e melhoria dos serviços públicos digitais; promoção da participação e engajamento dos cidadãos; garantia da segurança da informação e proteção de dados; e fomento à inovação e adoção de novas tecnologias.

A modernização e integração dos sistemas de governo, conforme previsto na ENGD, têm contribuído para melhorar a infraestrutura tecnológica do Brasil. O desenvolvimento de plataformas digitais compartilhadas, como o Portal de Serviços do Governo Federal (Gov.br), tem facilitado a coordenação e comunicação entre diferentes órgãos e entidades governamentais. Isso se alinha com a primeira área do GTMI, que aborda sistemas centrais do governo e plataformas digitais compartilhadas.

No que diz respeito à prestação de serviços governamentais, a ENGD tem impulsionado a expansão e a melhoria dos serviços públicos digitais. Essa transformação digital de serviços, aliada à criação de soluções centradas no cidadão resultam em melhoria da acessibilidade, simplicidade e transparência. Esses avanços estão em consonância com a segunda área do GTMI, que enfoca a entrega de serviços on-line.

A ENGD também promove a participação e o engajamento dos cidadãos, com ênfase no desenvolvimento de ferramentas e mecanismos de interação entre o governo e a população, como explicitado no Objetivo 14 do Decreto 10.332/2020 [4]. Essa abordagem está alinhada com a terceira área do GTMI, que abrange o engajamento digital do cidadão.

Por fim, a ENGD fomenta a capacitação de servidores públicos, a segurança da informação, a proteção de dados e a promoção de inovação e novas tecnologias. Esses aspectos estão em sintonia com a quarta área do GTMI, que se concentra nos facilitadores de GovTech citados anteriormente.

Nesse contexto de integração de serviços digitais, um dos passos foi criar um mecanismo de acesso digital único para essas múltiplas soluções tecnológicas. O projeto dessa plataforma de autenticação foi instituído pelo Decreto 8.936, de 19 de dezembro de 2016 [3], e criou a base do que é hoje o Login Único do Governo Federal, também conhecido por *Conta gov.br* [8].

Inicialmente utilizada apenas pelo Poder Executivo Federal, atualmente a *Conta gov.br* está sendo adotada por outros órgãos públicos, nos níveis estadual e municipal [9]. Dentre as principais vantagens da *Conta gov.br* estão: a facilidade de acesso a

diversos serviços públicos on-line com uma única conta de usuário e senha, o canal de atendimento on-line para suporte aos usuários e a personalização da experiência de uso. Outro benefício importante é sua conformidade com a Lei Geral de Proteção de Dados (LGPD), garantindo que as informações pessoais dos cidadãos brasileiros sejam tratadas com a privacidade e segurança prescritas pela legislação [10].

Criada em 14 de agosto de 2018, através da Lei nº 13.709 [11], e em vigor desde 18 de setembro de 2020, a LGPD estabelece regras para a coleta, uso, armazenamento e compartilhamento de dados pessoais de indivíduos, incluindo dados pessoais sensíveis. Ela também especificou sanções administrativas, civis e penais para as empresas e organizações que descumprirem suas disposições. Tais penalidades variam desde uma advertência, passando por multas que podem chegar a até R\$ 50 milhões por infração, e chegando até à proibição parcial ou total do exercício das atividades relacionadas ao tratamento de dados pessoais [12].

As vantagens de se ter um login único, juntamente com uma infraestrutura já adequada à LGPD, levaram o Senado Federal do Brasil a considerar a incorporação da **Conta gov.br** nos serviços digitais que são prestados aos cidadãos, uma vez que sua adoção sugere uma melhoria tanto na questão da usabilidade, quanto na proteção de dados pessoais dos usuários. Diversos serviços legislativos, como a proposição de matérias legislativas e a inscrição em cursos oferecidos pela Casa Legislativa, poderiam ser disponibilizados por meio da **Conta gov.br**, ampliando o acesso e a participação dos cidadãos.

Dentre as soluções oferecidos pelo Senado Federal, o Portal e-Cidadania provavelmente seria o mais beneficiado por essa melhoria. Criado em 2012 pela equipe de desenvolvimento do Senado, o portal tem como objetivo promover e viabilizar uma maior participação dos cidadãos nas atividades legislativas, orçamentárias, fiscalizatórias e representativas do Senado [13]. O portal oferece três ferramentas principais de participação:

1. Ideia Legislativa: permite o envio e apoio a ideias legislativas para aprimoramento da legislação ou criação de novas leis, onde as ideias que alcançam 20 mil apoios são encaminhadas à Comissão de Direitos Humanos e Legislação Participativa (CDH);
2. Evento Interativo: possibilita a participação em audiências públicas, sabatinas e outros eventos abertos, com páginas específicas que contêm transmissão ao vivo, espaço para comentários e informações relevantes ao evento; e
3. Consulta Pública: os cidadãos são convidados a opinar sobre proposições legislativas em tramitação no Senado Federal até a deliberação final.

A premissa utilizada para inferir um ganho na utilização da **Conta gov.br** no e-Cidadania vem de seus números de utilização: dados de abril de 2023 apontam que, apenas para o tipo Ideia Legislativa, mais de 100 mil ideias foram recebidas, oriundas de

quase 64 mil autores, gerando mais de 10 milhões de registros de apoio desde a implantação em 2012 [14]. Essas estatísticas mostram que há uma utilização considerável da aplicação por parte dos cidadãos, e supõe-se que facilitar o registro dessas informações pode causar um impacto positivo na prestação do serviço público.

Ao mesmo tempo, ter a custódia dessas milhares de informações pessoais pode apresentar riscos para a organização, uma vez que o vazamento ou o mau uso desses dados podem acarretar alguma das penalidades previstas na LGPD. Esse cenário exige que as organizações observem a gestão dos dados pessoais de seus usuários com mais apuro, até com a instituição de processos como o proposto por Canedo et al. [15]. O estabelecimento desses protocolos exige treinamento de pessoal e criação de políticas, o que gera custo para a instituição e, utilizar uma solução que já está aderente a essas práticas reduzirá, em teoria, o impacto.

Dessa forma, o presente trabalho se propõe a verificar os benefícios que a **Conta gov.br** pode trazer para os órgãos que a utilizam, principalmente no que diz respeito à usabilidade. O estudo será feito em um órgão do Poder Legislativo, no caso, o Senado Federal, e espera-se que sejam obtidos dados concretos sobre as reais vantagens da integração com o Login Único do Governo Federal. Ao final, será proposto um guia prático que facilite o uso da **Conta gov.br** por outros órgãos, informando sobre as vantagens identificadas nessa pesquisa.

## 1.1 Problema de Pesquisa

Existe algum impacto ou benefício na adoção da **Conta gov.br** pelo Senado Federal do Brasil em seus sistemas acessados pelo público em geral, no que tange à experiência dos usuários?

## 1.2 Justificativa

A pesquisa deste problema é justificada pela necessidade de aprimorar os serviços públicos on-line oferecidos pelo Senado Federal do Brasil, garantindo acessibilidade, eficiência e segurança para os cidadãos. A adoção da **Conta gov.br** pode proporcionar benefícios em termos de usabilidade, o que deve ser investigado em profundidade para avaliar o impacto dessa implementação. Sendo assim, uma vez que há custos operacionais na implantação do serviço, o estudo se justifica para obter dados claros sobre a relação de custo-benefício existente na integração com esse sistema.

## 1.3 Objetivos

### 1.3.1 Objetivo Geral

O objetivo deste trabalho é **avaliar o impacto do uso da *Conta gov.br* pelo Senado Federal em relação à usabilidade e propor um guia para que outros poderes, além do Executivo, utilizem a plataforma.** A intenção é oferecer dados concretos para que outros órgãos públicos possam avaliar se há vantagem na integração com a *Conta gov.br*.

### 1.3.2 Objetivos Específicos

Com base no objetivo geral do trabalho, podemos listar os seguintes objetivos específicos:

- Descrever o funcionamento da *Conta gov.br* de forma a apresentar aos possíveis utilizadores questões arquiteturais que devem ser consideradas em sua implantação.
- Realizar uma revisão de literatura para:
  - Identificar as formas de testar a usabilidade de soluções de login único, a fim de subsidiar a avaliação da *Conta gov.br* pelo Senado Federal.
  - Definir quais são as métricas mais utilizadas em testes desse tipo, para ter um conjunto de informações embasado em estudos sólidos.
- Criar um protocolo de teste de usabilidade, baseado nos achados da revisão.
- Desenvolver um estudo de caso prático no sistema e-Cidadania, para comparar a usabilidade da forma de autenticação atual, que utiliza e-mail e senha, e avaliar se existe impacto na incorporação da *Conta gov.br* em relação à usabilidade, utilizando o protocolo de avaliação criado.
- Propor um guia prático para que órgãos públicos de outros Poderes da Administração Pública possam utilizar a *Conta gov.br*, sintetizando os dados encontrados e os possíveis benefícios da integração.

Descreveremos na próxima seção quais são as entregas práticas a que o trabalho se propõe.

## 1.4 Resultados Esperados

Com o intuito de possibilitar a conferência, ao final do trabalho, do sucesso da pesquisa, espera-se que os seguintes resultados sejam produzidos:

- Identificação das técnicas e métricas do estado-da-arte para aferição da usabilidade de um sistema com login único.
- Criação de um protocolo do teste de usabilidade, gerado pelas técnicas identificadas.
- Catalogação dos benefícios da adoção da plataforma gov.br pelo Senado Federal em relação à usabilidade dos usuários.
- Confecção do Guia Prático para Adoção da *Conta gov.br*, contendo diretrizes e boas práticas para que outros órgãos públicos possam utilizar a *Conta gov.br*.

O processo que fornecerá a base teórica e estruturará as abordagens necessárias para que esses produtos sejam feitos será visto na próxima seção.

## 1.5 Metodologia de Pesquisa

Para alcançar os resultados esperados desta pesquisa, foi adotada uma abordagem metodológica estruturada em quatro etapas principais:

1. **Revisão Sistemática da Literatura (RSL):** a primeira etapa consistiu na realização de uma RSL, cujo objetivo foi mapear estudos relacionados à avaliação de usabilidade em sistemas de autenticação digital, especialmente os baseados em login único. A revisão foi conduzida com o apoio da ferramenta *Parsifal* [16], uma ferramenta on-line projetada para direcionar pesquisadores na execução de RSL no contexto da Engenharia de Software. Os resultados dessa etapa forneceram a base teórica para os passos seguintes, especialmente quanto às métricas e técnicas a serem utilizadas.
2. **Elaboração do Protocolo de Teste:** a partir dos achados da RSL, foi elaborado um protocolo de teste de usabilidade adaptado ao contexto do sistema e-Cidadania. Esse protocolo definiu os cenários a serem avaliados, as tarefas executadas pelos participantes e como as métricas seriam coletadas e avaliadas.
3. **Execução dos Testes com Usuários:** a terceira etapa correspondeu à aplicação dos testes com usuários reais, realizada em ambiente de homologação, com simulação de acesso ao sistema e-Cidadania por meio de dois métodos de autenticação: o tradicional, que usa E-mail e Senha, e com a *Conta gov.br*. A coleta de dados considerou tanto variáveis quantitativas quanto observações qualitativas, permitindo uma análise comparativa sobre a experiência de uso, a facilidade percebida e o desempenho em cada cenário.

4. **Elaboração do Guia Prático:** por fim, os achados da pesquisa foram consolidados em um Guia Prático para Adoção da Conta gov.br, produzido em formato *markdown* com vistas à sua ampla disseminação. O guia reúne fundamentos técnicos, orientações estratégicas, dados empíricos e representações gráficas, servindo como ferramenta de apoio para outros órgãos públicos que desejem adotar a Conta gov.br de forma segura e fundamentada.

Com a metodologia definida, a próxima seção apresenta a estrutura do trabalho, detalhando como cada capítulo contribui para alcançar os objetivos da pesquisa.

## 1.6 Estrutura do Trabalho

Este trabalho tem o total de seis capítulos, sendo que o primeiro foi esta introdução. O conteúdo dos demais é descrito a seguir:

- **Capítulo 2:** Apresenta os conceitos necessários para o melhor entendimento da pesquisa.
- **Capítulo 3:** Descreve a metodologia da Revisão Sistemática de Literatura, define suas etapas e mostra resultados obtidos.
- **Capítulo 4:** Apresenta o protocolo de teste de usabilidade derivado dos achados da RSL, e esquematiza o estudo-piloto que seria realizado, mas que foi cancelado em razão de ajustes no cronograma decorrentes da submissão ao Comitê de Ética em Pesquisa e das demais exigências institucionais ao longo da preparação do estudo principal.
- **Capítulo 5:** Lista as atividades que foram executadas para coletar os dados da pesquisa, ao mesmo tempo que interpreta e discute estes resultados.
- **Capítulo 6:** Analisa o resultado geral desta pesquisa e direciona os trabalhos futuros.

# Capítulo 2

## Embasamento

### 2.1 Autenticação e Autorização

O uso de soluções digitais, como redes sociais e comércio eletrônico, nos dias de hoje tem uma dimensão gigantesca. Dados de janeiro de 2024 [17] mostram que existem 5,35 bilhões de usuários de internet, o que corresponde a 66,2% da população global. Estudos como o realizado por Dwivedi et al. [18] abordam o impacto e os desafios que essa massa de pessoas impõem em áreas como o marketing digital, através de desenvolvimentos tecnológicos como Inteligência Artificial, Realidade Aumentada, análise de Big Data e *Blockchain*.

Um aspecto comum a todas as tecnologias mencionadas é a necessidade de os usuários se autenticarem para acessar os serviços oferecidos por elas. Conforme Lim et al. [19], a autenticação e a autorização são os processos que impactam diretamente na confiabilidade e segurança de um serviço em nuvem.

A autenticação é o procedimento que confirma a identidade do usuário, sendo a primeira linha de defesa que ele tem para manter a confidencialidade e a integridade de suas informações, segundo Almuairfi et al. [20]. O primeiro conceito assegura que apenas pessoas autorizadas possam acessar uma informação, enquanto o segundo garante que os dados não são modificados de forma não autorizada.

Já a autorização determina as prerrogativas de acesso dos usuários, ou seja, o que ele pode fazer depois de obter acesso, afirmam Lim et al. [19]. Eles acrescentam que os dados envolvidos vão além da identidade do usuário, englobando atributos adicionais como papéis e títulos.

Barkadehi et al. [21] acrescentam que as estratégias utilizadas para autenticação se baseiam em quatro modelos principais:

1. Baseado em conhecimento: algo que o usuário *sabe*, como a tradicional combinação de usuário e senha, um *Personal Identification Number* (PIN) ou um padrão de bloqueio de tela de *smartphone*.

2. Baseado em propriedade: algo que o usuário *tem*, como os *tokens* criptográficos, *smartcards*, dispositivos de segurança com *Near Field Communication* (NFC) e aparelhos celulares.
3. Baseado em características inerentes: algo que o usuário *é*. Nesse modelo estão as impressões digitais, palma, íris e voz.
4. Modelo misto: dois (*Two factor*) ou mais (*Multifactor*) fatores dos modelos acima são utilizados para autenticar o usuário.

Grabatin et al. [22] fizeram uma análise das características dos principais modelos citados, considerando cinco fatores: Confiabilidade, Segurança, Privacidade, Usabilidade, Ambiente e Interoperabilidade. O resultado está sintetizado no Quadro 2.1:

<b>Fator</b>	<b>Clássico (Senha/PIN)</b>	<b>Físico (Tokens, NFC)</b>	<b>Biometria</b>
Confiabilidade	Confiável, não tem falsos positivos nem negativos. Suscetível a <i>phishing</i> .	Alta, não sujeito a adivinhações.	Muito alta, usa características únicas. Afetada por mudanças físicas.
Segurança	Vulnerável a <i>phishing</i> , <i>cracking</i> , <i>shoulder surfing</i> , análise de calor e marcas de dedos.	Mais seguro contra <i>phishing</i> e ataques on-line, mas vulnerável se roubado. Aumenta a segurança se usado como segundo fator. Possíveis vulnerabilidades na implementação.	Biometrias comportamentais são difíceis de imitar. Acurácia de autenticação menor. Vulnerável se informações biométricas forem roubadas.
Privacidade	Permite pseudônimos, protegendo identidade.	Boa, não vinculada diretamente a informações pessoais.	Baixa, ligada ao indivíduo e não alterável. Risco de violação de privacidade se comprometida.

<b>Fator</b>	<b>Clássico (Senha/PIN)</b>	<b>Físico (Tokens, NFC)</b>	<b>Biometria</b>
Usabilidade	Baixa caso a política seja rigorosa e exija a lembrança de senhas complexas, além de consumirem tempo.	Alta, elimina necessidade de memorizar senhas. Pode ser afetada em ambientes lotados.	Muito alta, não requer memorização ou posse. Opção mais acessível para usuários com deficiências.
Ambiental	Suscetível a erros e lento, especialmente em ambientes que tenham algumas limitações, como por exemplo, ambientes de saúde.	Limitações em ambientes que exigem vestuário de proteção, podendo dificultar o transporte de dispositivos eletrônicos.	Pode falhar ou ser pouco confiável em condições extremas (frio, calor, umidade) e com uso de máscaras ou luvas.
Interoperabilidade	Amplamente implementado e considerado um padrão de fato, embora possa ser impossível ou incômodo em muitas situações.	Uso limitado a sistemas que suportam dispositivos físicos específicos. Planejamento cuidadoso necessário para integração.	Uso restrito a sistemas que suportam biometria. Desafios na integração com sistemas que não permitem métodos de autenticação intercambiáveis.

Quadro 2.1: Análise dos modelos de autenticação com base em fatores que afetam a segurança. (Fonte: O Autor.)

De todos os modelos de autenticação apresentados anteriormente, Krawiecka et al. [23] afirmam que as senhas são o mecanismo de autenticação primária mais utilizado na Web, mesmo com a apresentação de esquemas alternativos. Os pesquisadores creditam essa predominância ao fato das senhas serem fáceis de entender, eficientes de usar e não exigirem que o usuário carregue dispositivos ou *tokens* adicionais. Além disso, são compatíveis com praticamente todos os servidores e navegadores web e têm um custo mínimo para quem a utiliza.

Há, porém, um efeito colateral do uso frequente desse meio de autenticação. Com a proliferação dos serviços utilizados, a quantidade de credenciais que um usuário tem que gerenciar se tornou muito grande. Isso gerou um fenômeno descrito por Sasse et al. [24] como a Grande Fadiga da Autenticação. Essa pesquisa discutiu como a autenticação

pode ser demorada, onerosa, interromper tarefas primárias e reduzir a produtividade, afetando a percepção e a atitude das pessoas em relação à segurança, o que muitas vezes compromete esse aspecto.

Sun et al. [25] sugerem que uma alternativa para reduzir esse problema é a utilização do *Single Sign-On* (SSO), uma abordagem que permite que os usuários da Web utilizem uma conta única para acessar múltiplos sites não relacionados. Veremos mais detalhes sobre esse assunto na próxima seção.

### 2.1.1 *Single Sign-On*

Soluções de *Single Sign-On*, ou de Login Único, operam com base em um conceito de serviço centralizado, permitindo que o usuário seja autenticado usando um único conjunto de credenciais de login, segundo Pandey e Nisha [26]. Por meio de *cookies* gerados e controle de sessão, essas credenciais podem ser usadas para acessar múltiplas aplicações. Plataformas como Facebook e Google exemplificam o uso de SSO social, facilitando o acesso a diversos serviços de terceiros.

A arquitetura básica de uma solução de Login Único possui dois atores, conforme afirmam Sun et al. [25]: um Provedor de Identidade (*Identity Provider* - IdP), responsável por manter as informações de identidade dos usuários e também por autenticá-los; e uma Parte Confiante (*Relying Party* - RP), que se baseia nas identidades autenticadas para tomar decisões sobre a autorização e customizar a experiência do usuário. O fluxo de uso da arquitetura está ilustrado na Figura 2.1:

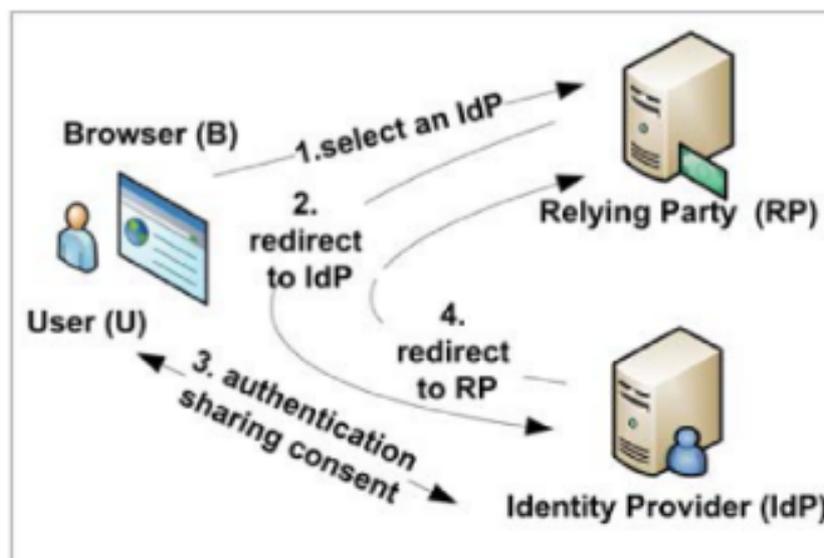


Figura 2.1: Fluxo de autenticação e autorização do *Single Sign-On*. (Fonte: Sun et al. [25]).

A descrição dos passos executados na autenticação por uma solução de *Single Sign-On* é a seguinte:

1. O usuário seleciona um IdP por meio de um formulário de login apresentado pela RP, que tipicamente combina campos de login tradicionais (nome de usuário, senha) com uma lista de ícones de IdP para escolha.
2. A RP redireciona o usuário para o IdP visando a autenticação.
3. O usuário se autentica no IdP inserindo seu nome de usuário e senha. Este passo pode ser omitido se o usuário já estiver autenticado pelo IdP na sessão do navegador. Após a autenticação, o IdP apresenta um formulário de consentimento para compartilhamento de perfil, autorizando a liberação de suas informações de perfil.
4. O IdP redireciona o usuário de volta à RP com os atributos de perfil solicitados. Antes de conceder acesso, a RP pode solicitar ao usuário que complete um formulário de registro para coletar informações adicionais do perfil ou vincular a uma conta existente. Para um usuário que retorna, apenas os passos de 1 a 3 são necessários para fazer login no site da Parte Confiante.

Wang et al. [27] acrescentam que um SSO deve atender a pelo menos três requisitos básicos de segurança: resistência à falsificação (*unforgeability*), privacidade de credenciais (*credential privacy*) e solidez (*soundness*). A resistência à falsificação exige que apenas a autoridade confiável seja capaz de fornecer uma credencial válida para um novo usuário, e nem mesmo um conluio entre usuários e provedores de serviços consiga forjar uma comprovação desse tipo. A privacidade de credenciais garante que provedores de serviços desonestos coludidos não consigam recuperar completamente a credencial de um usuário e, então, se passar por ele para fazer login em outros provedores de serviços. Finalmente, solidez significa que um usuário não registrado e sem credencial não deve ser capaz de acessar os serviços oferecidos pelos provedores de serviços.

Como o conceito de *Single Sign-On* é abstrato, foi necessário criar uma forma de desenvolvê-lo para uso no mundo real. Veremos na próxima seção um apanhado das implementações mais importantes que constam na literatura.

### 2.1.2 Implementações de *Single Sign-On*

As primeiras soluções de Login Único foram oriundas de empresas e agências governamentais, segundo Beltran [28]. A intenção dessas corporações era que seus empregados pudessem ter acesso transparente aos mais variados serviços disponibilizados em sua infraestrutura. Para atingir esse objetivo, foram usados dois protocolos principais: Kerberos e *Security Assertion Markup Language* (SAML).

O Kerberos é definido por Neuman e TS'o [29] como um serviço de autenticação distribuída, desenvolvido no âmbito do Projeto Athena do MIT na metade dos anos 80. Ele permite que um cliente, atuando em nome de um usuário, possa provar sua identidade a um verificador (um servidor de aplicação) sem transmitir dados pela rede. Isso tem como objetivo evitar que um agente malicioso ou o próprio verificador se passem posteriormente pelo usuário. Seu sistema de autenticação utiliza uma série de mensagens criptografadas para comprovar ao verificador que um cliente está operando em nome de um usuário específico.

Já Bazaz e Khaliq [30] descrevem o SAML como um protocolo baseado em XML, desenvolvido pela *Organization for the Advancement of Structured Information Standards* (OASIS). Sua função principal é permitir a comunicação entre domínios com diferentes mecanismos de autenticação. Gross [31] acrescenta que, por ser um padrão aberto e muito extensível, se tornou uma opção atraente para o desenvolvimento de protocolos como o *Liberty Alliance Project* e o *Shibboleth Project*.

As entidades envolvidas no SAML, segundo Bazaz e Khaliq [30], incluem o usuário, o Provedor de Identidade (IdP) e o Provedor de Serviço (*Service Provider* - SP). O IdP faz “afirmações” sobre a identidade e os atributos do usuário para os SPs, enquanto o Provedor de Serviço oferece um serviço específico ou hospeda uma aplicação. O fluxo de autenticação do protocolo é apresentado na Figura 2.2:

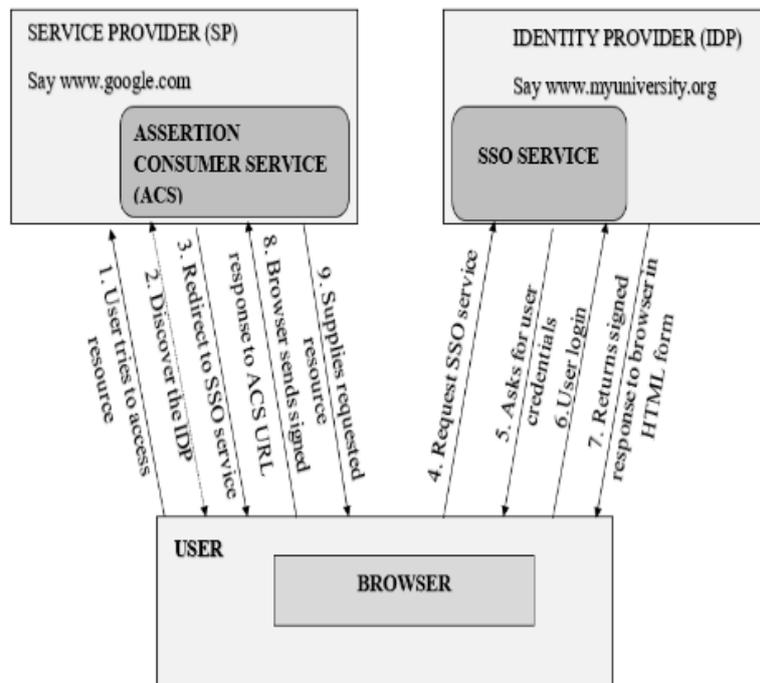


Figura 2.2: Fluxo de autenticação do protocolo SAML. (Fonte: Bazaz e Khaliq [30]).

Beltran [28] aponta que, apesar das vantagens de interoperabilidade que apresenta, o SAML encontrou problemas para se firmar no ambiente da Internet. Isso se deve ao fato de não existir um servidor de segurança centralizado, e sim, várias aplicações que se comunicam através de trocas básicas por meio do *Hypertext Transfer Protocol* (HTTP), usando representação *JavaScript Object Notation* (JSON) ou *eXtensible Markup Language* (XML). Neste sentido, foram privilegiados dois protocolos que se baseiam na arquitetura *Representational State Transfer* (REST) e possuem uma federação de identidade de baixo acoplamento: OpenID e OAuth2.0.

O OpenID, que foi desenvolvido em 2005 e finalizado em 2007, é descrito por Sun et al. [25] como um protocolo leve de SSO e que oferece uma capacidade única de descoberta dinâmica de Provedores de Identidade (IdPs). Essa fase se denomina Descoberta, e permite que as Partes Confiantes (RPs) descubram qual *endpoint* utilizar para se comunicar com o IdP e solicitar a autenticação do usuário (fase de Autenticação).

Uma vez que ela seja bem sucedida, Radha e Reddy [32] acrescentam que se inicia a fase da Associação. Nessa fase, o IdP e a RP estabelecem uma conexão direta utilizando um segredo compartilhado, que será usado para assinar a comunicação entre ambos, permitindo que as mensagens sejam verificadas quanto à sua autenticidade. Finalmente, é iniciada a fase de Verificação, onde o IdP envia uma mensagem para a RP informando que o usuário é quem diz ser. Essa mensagem é verificada com base no segredo compartilhado na fase de Associação, evitando que um impostor possa forjar uma resposta de autenticação falsa sobre um usuário. A Figura 2.3 ilustra o fluxo.

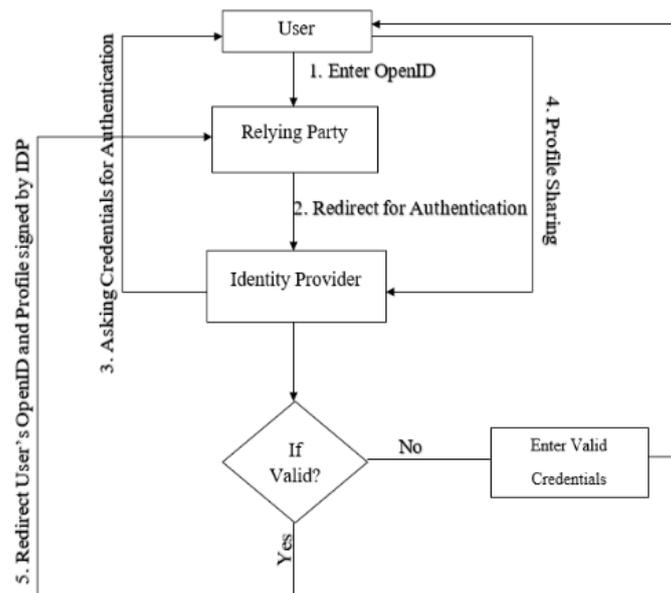


Figura 2.3: Fluxo de autenticação do protocolo OpenID. (Fonte: Bazaz e Khalique [30]).

O protocolo OAuth, de acordo com Beltran [28], é um protocolo genérico de autorização delegada que fornece um *token* de acesso a um cliente permitindo que ele acesse um recurso protegido com base na permissão do proprietário do recurso. Ele, porém, não é um protocolo de *Single Sign-On* típico, apesar de ser usado de forma ampla para desenvolver soluções de autenticação e identidade.

Um exemplo clássico desse uso, segundo Siriwardena [33], é quando queremos delegar para uma aplicação de terceiros o acesso à nossa página do Facebook. O fluxo desse processo está ilustrado na Figura 2.4.

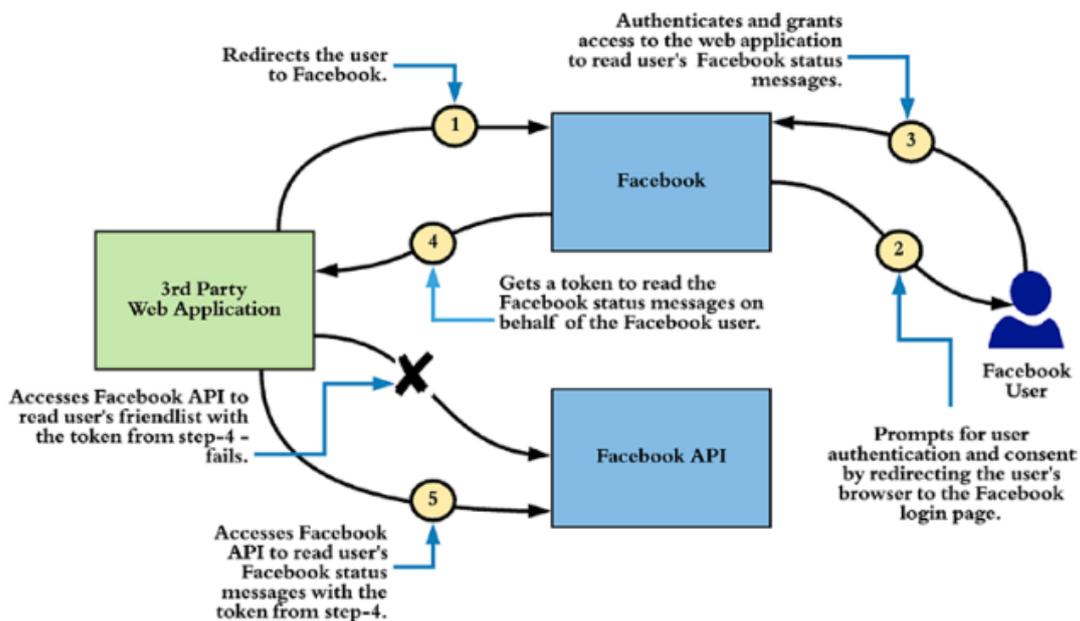


Figura 2.4: Fluxo de autenticação do protocolo OAuth. (Fonte: Siriwardena [33]).

A descrição detalhada dos passos que estão ilustrados é a seguinte:

1. O usuário visita uma aplicação web de terceiros e deseja permitir que a aplicação publique mensagens em seu mural do Facebook. Para isso, a aplicação precisa de um *token* do Facebook e redireciona o usuário para a rede social;
2. O Facebook solicita que o usuário se autentique (caso ainda não esteja autenticado) e pede seu consentimento a fim de dar permissões à aplicação para publicar mensagens em seu mural;
3. O usuário se autentica e dá seu consentimento ao Facebook, permitindo que ele compartilhe um *token* com a aplicação. Esse *token* permite apenas a publicação de mensagens no mural por um período limitado e não pode realizar outras ações,

como enviar solicitações de amizade, deletar mensagens de status, fazer upload de fotos, etc;

4. A aplicação web recebe um *token* do Facebook;
5. A aplicação web acessa a *Application Programming Interface* (API) do Facebook com o *token* fornecido no passo 4. A API garante que apenas solicitações com um *token* válido possam acessá-la.

Há, no entanto, um problema de interoperabilidade e segurança no protocolo, aponta Beltran [28]. A pesquisadora afirma que a falta de padronização de como as informações de autenticação e identidade são transmitidas resulta em implementações vulneráveis, já que cada Provedor de Identidade define a sua camada de identidade. Essas questões levaram ao surgimento do *OpenID Connect* (OIDC), uma especificação que fornece uma estrutura de autenticação e identidade interoperável baseada no OAuth.

Siriwardena [33] explica que o *OpenID Connect* foi desenvolvido sobre o OAuth2.0, introduzindo uma camada de identidade sobre este último. Ele devolve um *token* de ID (ID\_TOKEN) para o cliente, representando a identidade do usuário final, deixando que o OAuth2.0 fique concentrado na autorização, que é realizada através do retorno de um *token* de acesso (ACCESS\_TOKEN) para recursos em nome do usuário. O autor completa a análise informando que Provedores de Identidade como Yahoo! e Google descontinuaram o suporte ao OpenId e migraram para essa nova arquitetura em torno de 2015.

Wilson e Hingnikar [34] definem três papéis principais na arquitetura:

1. Usuário Final: o sujeito a ser autenticado.
2. Provedor OpenID (*OpenId Provider* - OP): um servidor de autorização OAuth 2.0 que implementa OIDC, capaz de autenticar um usuário e retornar declarações sobre o usuário autenticado e o evento de autenticação para uma Parte Confiante (aplicação).
3. Parte Confiante (RP): um cliente OAuth 2.0 que delega a autenticação do usuário a um Provedor OpenID e solicita declarações sobre o usuário do Provedor OpenID. Geralmente, é uma aplicação, mas uma Parte Confiante pode ser outro provedor de identidade em casos de uso mais avançados.

Os autores também apresentaram um fluxo para ilustrar como o processo de autenticação ocorre. Ele é apresentado na Figura 2.5 e descrito na sequência:

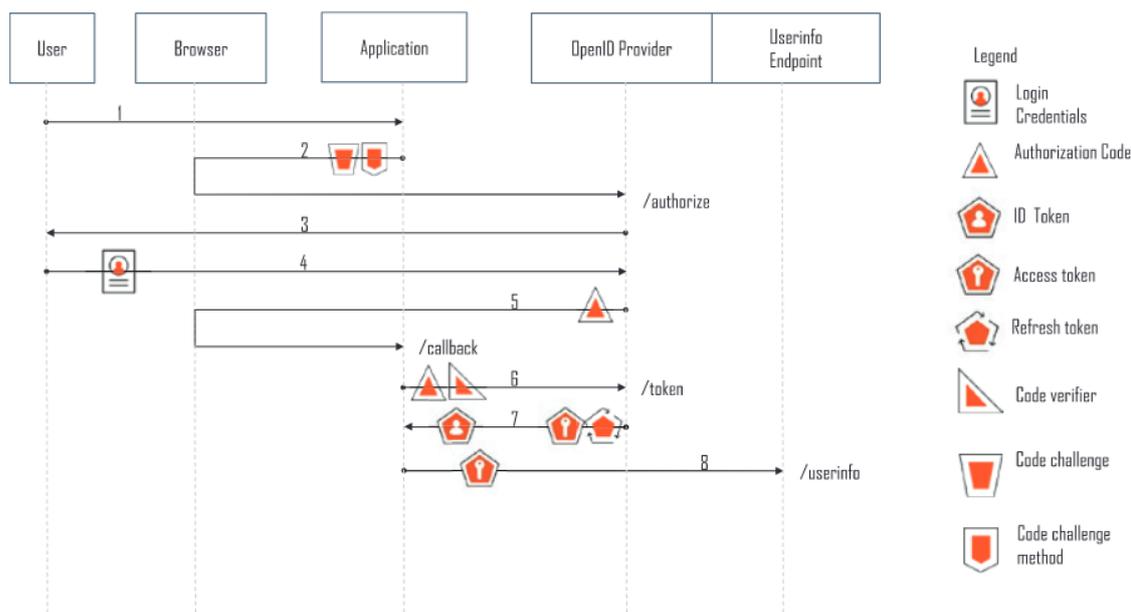


Figura 2.5: Fluxo de autenticação do protocolo *OpenID Connect*. (Fonte: Wilson e Hingnikar [34]).

1. O usuário acessa a aplicação (Parte Confiante).
2. O navegador do usuário é redirecionado para o Provedor OpenID com uma solicitação de autenticação.
3. O Provedor OpenID interage com o usuário para autenticação e para obter consentimento para o escopo da solicitação de informações do mesmo.
4. O usuário se autentica, dá consentimento, e o Provedor OpenID cria ou atualiza uma sessão de autenticação para o usuário.
5. O navegador do usuário é redirecionado de volta para a aplicação com um código de autorização.
6. A aplicação envia uma solicitação de *token* ao Provedor OpenID, com o código de autorização.
7. O Provedor OpenID responde com um `ID_TOKEN`, `ACCESS_TOKEN` e, opcionalmente, um *token* de atualização.
8. A aplicação pode usar o `ACCESS_TOKEN` no *endpoint* `/userinfo` do Provedor OpenID, que é responsável por fornecer informações sobre o usuário.

Finalizando, todos os protocolos aqui apresentados se baseiam no modelo de Identidade Federada, onde a figura do Provedor de Identidade (IdP) tem a maior importância

na autenticação dos usuários. A título de informação, convém mencionar que existe um paradigma diferente, que surgiu em 2015, denominado modelo de Identidade Descentralizada (*Decentralized Identity*). Também conhecida como Identidade Autossobrerana (*Self-Sovereign Identity - SSI*), Preukschat e Reed [35] descrevem que essa solução foi inspirada pela *Blockchain* e, diferente dos provedores de identidade centralizados, esse modelo é fundamentalmente difuso, incorporando avanços em criptografia, bancos de dados distribuídos e redes descentralizadas.

Os autores enfatizam que a principal diferença desse modelo é que ele não é baseado em contas, mas sim em uma relação direta entre pares, semelhante às relações no mundo real, onde nenhuma das partes “fornece”, “controla” ou “possui” a relação. Em uma conexão ponto a ponto, as partes compartilham uma conexão sem que nenhuma delas a possua completamente, conforme ilustrado na Figura 2.6.

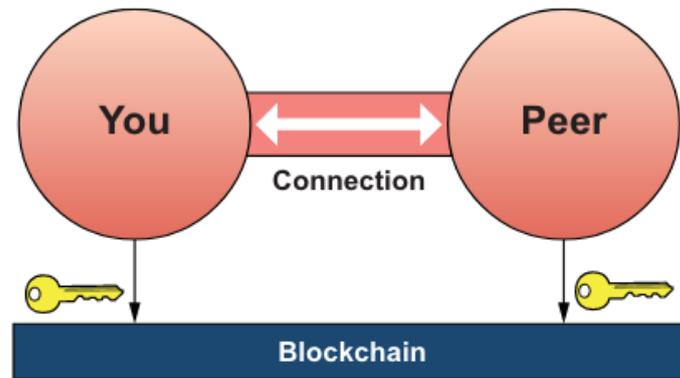


Figura 2.6: Relação entre pares proporcionada pelo modelo de identidade descentralizada. (Fonte: Preukschat e Reed [35]).

Os pesquisadores mencionam que, em linhas gerais, a tecnologia *Blockchain* é utilizada para criar uma Infraestrutura de Chave Pública Descentralizada (*Decentralized Public Key Infrastructure - DPKI*). Essa arquitetura permite a troca direta de chaves públicas para formar conexões privadas e seguras e o armazenamento de algumas dessas chaves em *Blockchains* públicos para validar assinaturas em credenciais de identidade digitais verificáveis, que se assemelha à maneira como provamos nossa identidade no mundo real.

Concluindo, verificamos de forma sintética alguns conceitos relacionados à implementação do Login Único na prática. Com esse conteúdo, estamos habilitados para ver os detalhes que envolvem a autenticação da *Conta gov.br*.

### 2.1.3 Conta gov.br

O mecanismo de acesso digital único de usuários a serviços públicos do Governo Federal do Brasil, conhecido como **Conta gov.br**, foi instituído pelo Decreto 8.936/2016 [3]. Foi essa norma que estabeleceu as diretrizes para oferta de soluções digitais fornecidas pelo Poder Público, como a convergência autoritativa e a federação dos processos de autenticação desses serviços [36].

As questões que levaram a Secretaria de Governo Digital a optar por esse caminho foram problemas identificados na prestação dos serviços existentes à época, como a duplicidade e inconsistência de informações cadastrais, a falta de integração entre diferentes bases de dados, e as múltiplas contas de acesso e diversas formas de autenticação que existiam dentro do ecossistema de soluções digitais do Governo Federal.

Além de atacar o problema de autenticação dos usuários, fornecendo uma solução de Login Único que diminui a Fadiga de Autenticação mencionada por Sasse et al. [24], a **Conta gov.br** também proporciona uma solução de autorização, já que a plataforma permite que as prerrogativas dos usuários variem de acordo com o método utilizado por eles para se autenticarem. A premissa é: quanto mais confiável for o método de autenticação, maior a quantidade de serviços disponíveis para uso, uma vez que o grau de certeza de que o usuário é quem diz ser fica maior.

Para tal, a **Conta gov.br** define os seguintes conceitos [36]:

- Selo de Confiabilidade: dado que varia de acordo com a segurança do processo de verificação, indicando se o procedimento foi feito por uma instituição bancária ou pela Justiça Eleitoral, por exemplo.
- Níveis de Autenticação: informação que indica o grau de validação dos dados de quem possui a conta. É determinado de acordo com o Selo de Confiabilidade do responsável pela verificação dessas informações. Quanto mais seguro for o Selo, maior o Nível.
- Catálogo de Confiabilidades: estrutura que permite que o sistema que está utilizando a **Conta gov.br** para autorização customize a experiência do usuário. É composto pelos Níveis de Autenticação e Selos de Confiabilidade.

A Figura 2.7 ilustra como esses conceitos se relacionam e apresenta uma síntese dos passos para obtenção de cada Selo:



Figura 2.7: Catálogo de Confiabilidades da **Conta gov.br**, discriminando a relação entre os Níveis de Autenticação e os Selos de Confiabilidade. (Fonte: O Autor.)

O detalhamento de como obter cada Nível de Autenticação é o seguinte [37]:

- Bronze
  - Cadastro via formulário on-line para validação dos dados na Receita Federal
  - Cadastro via formulário on-line para validação dos dados no Instituto Nacional do Seguro Social (INSS)
  - Cadastro via atendimento presencial nas Agências do INSS
  - Validação dos dados via atendimento presencial nos postos da Secretaria Nacional de Trânsito (Senatran)
  
- Prata
  - Reconhecimento facial pelo aplicativo Gov.br para conferência da sua foto nas bases da Carteira de Habilitação (CNH)
  - Validação dos seus dados via *internet banking* de um banco credenciado
  - Validação dos dados com usuário e senha do Sistema de Gestão de Pessoas (Sigepe), se o interessado for servidor público federal do Executivo

- Ouro

- Reconhecimento facial pelo aplicativo Gov.br para conferência da foto nas bases da Justiça Eleitoral
- Validação dos dados utilizando o aplicativo Gov.br para ler o QR Code da Carteira de Identidade Nacional (CIN)
- Validação dos seus dados com Certificado Digital de pessoa física compatível com Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

Em síntese, podemos afirmar que, quando o cidadão cria uma conta, a forma como esses dados serão validados definirá o Nível de Autenticação associado àquela conta. E, com base nesse nível, os tipos de serviços públicos que podem ser acessados e as transações digitais disponíveis também variarão, conforme mostra a Figura 2.8.

	BRONZE	PRATA	OURO
Uma única conta para acessar diversos serviços digitais	✓	✓	✓
Fazer o login em qualquer serviço gov.br sem precisar de senha, usando apenas a biometria do celular	✓	✓	✓
Gerenciar as autorizações de uso dos seus dados	✓	✓	✓
Realizar a prova de vida utilizando o reconhecimento facial	✓	✓	✓
Visualizar e compartilhar seus dados e documentos digitais	✗	✓	✓
Utilizar serviços gratuitos de assinatura eletrônica no site assinador.iti.br	✗	✓	✓
Acessar serviços públicos que exigem o maior grau de confiabilidade da conta gov.br	✗	✓	✓
Habilitar a autenticação em duas etapas para ter mais segurança no uso da sua conta	✗	✓	✓
Nível máximo de segurança da conta gov.br	● Básico	●● Alto	●●● Máximo

Figura 2.8: Prerrogativas dos usuários da **Conta gov.br** por Nível de Autenticação (Fonte: Governo Federal do Brasil [37]).

Note que, a partir do nível Prata, é possível habilitar a Autenticação em Duas Etapas. Essa opção faz com que o usuário, ao logar na sua conta, tenha que informar um código de desafio que é gerado pela **Conta gov.br** e enviado através do aplicativo de celular Gov.br. O resultado é um aumento de segurança, pois mistura dois modelos de autenticação (Seção

2.1): baseado em conhecimento (login e senha) e baseado em propriedade (o código é enviado apenas para aquele celular).

Após a contextualização de como a **Conta gov.br** funciona, verificaremos a seguir os aspectos técnicos que possibilitam sua integração a um serviço que queira usá-la como alternativa de autenticação/autorização.

### Integração da **Conta gov.br** com uma aplicação

Para utilização da **Conta gov.br** como solução de Login Único, é necessário submeter uma proposta para a Secretaria de Governo Digital (SGD), descrevendo, dentre outras informações, quais serviços o cidadão terá acesso após a disponibilização. Com isso, tem-se início um processo de avaliação da solução, que está ilustrado na Figura 2.9 e detalhado na sequência:

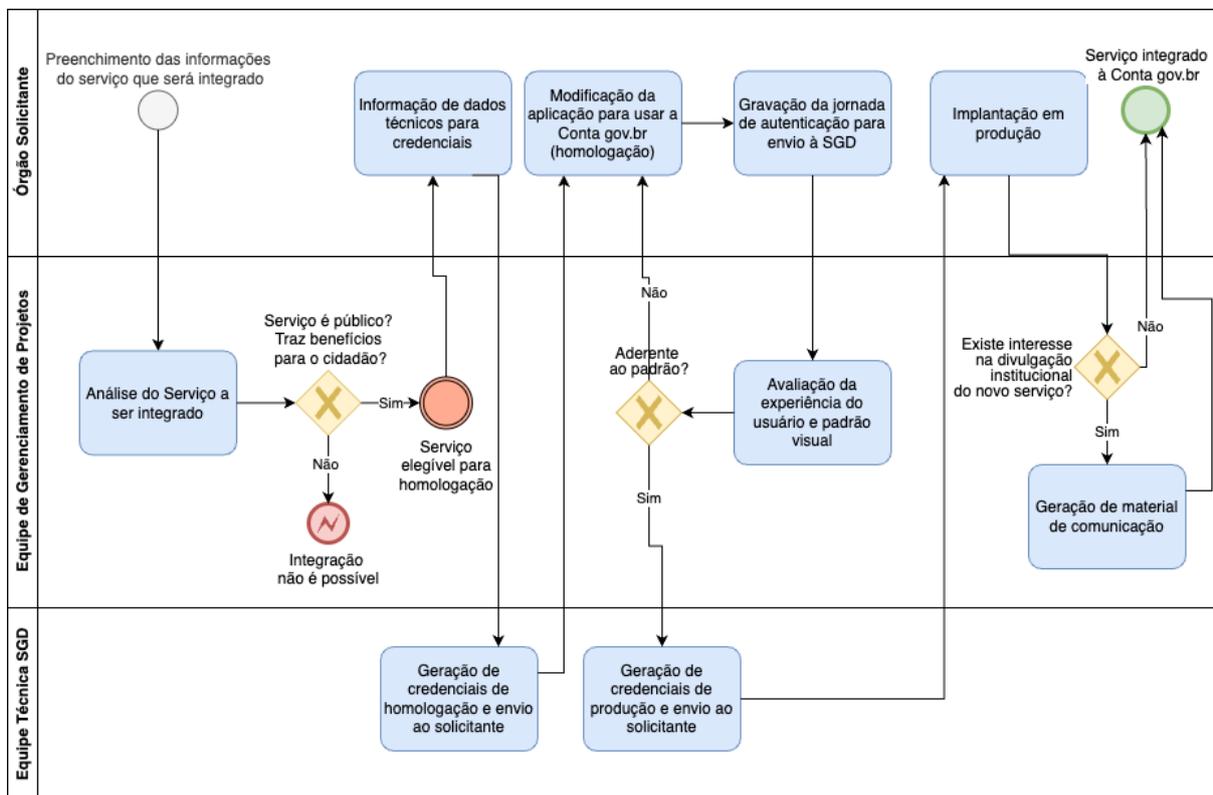


Figura 2.9: Processo de avaliação de um serviço para integração com a **Conta gov.br**. (Fonte: O Autor.)

A primeira análise que é feita é para verificar se o serviço candidato à integração é completamente público, e se vai trazer algum benefício para os cidadãos brasileiros. Dessa forma, serviços integralmente administrativos ou que não tenham uma interface com o cidadão não estão habilitados para uso da solução [38].

Caso a solicitação seja aprovada, dados do Responsável Técnico e também do sistema que será integrado serão solicitados para dar encaminhamento ao processo. Dentre as informações requeridas, estão a previsão do número de acessos por dia, as URLs de retorno e *logout* e um certificado digital que contenha uma Chave Pública do Representante Legal do Órgão e do Representante Técnico. Esta última tem como objetivo garantir que a credencial seja enviada criptografada para o Responsável Técnico, preservando o sigilo da informação e assegurando que apenas ele consiga acessá-la.

De posse desses dados, a Equipe Técnica da SGD gera as credenciais necessárias para que a aplicação utilize a ***Conta gov.br*** no ambiente de homologação. Tais dados, requeridos no processo de autenticação e autorização, são o `CLIENT_ID` e o `SECRET`.

O órgão ou entidade solicitante realiza as modificações no código-fonte da aplicação que será integrada, seguindo o Roteiro de Integração [36]. Os detalhes técnicos dessas alterações serão abordados na próxima seção. Quando a integração estiver concluída, o órgão realiza a gravação de toda a jornada de autenticação proposta e envia para a SGD.

A Equipe de Gerenciamento de Projetos da SGD vai verificar se a solução está aderente com o *design system* [39] estabelecido para manter a identidade visual das soluções integradas. Além disso, eles analisam toda a experiência do usuário ao fazer o login. Caso esteja dentro dos padrões estabelecidos, é autorizada a criação das credenciais de produção, que são enviadas ao solicitante.

O órgão implanta a solução integrada e, caso seja do interesse dele e da SGD, um material de divulgação institucional é confeccionado e propagado nos meios de comunicação dos órgãos envolvidos.

## Arquitetura da integração com a ***Conta gov.br***

Analisaremos nesse momento a forma que a autenticação e a autorização ocorrem quando uma aplicação é integrada à ***Conta gov.br***. Esperamos com isso esclarecer o motivo de algumas informações serem necessárias no momento do cadastro dessas soluções na plataforma. A Figura 2.10 exibe uma representação do fluxo que acontece durante o processo.

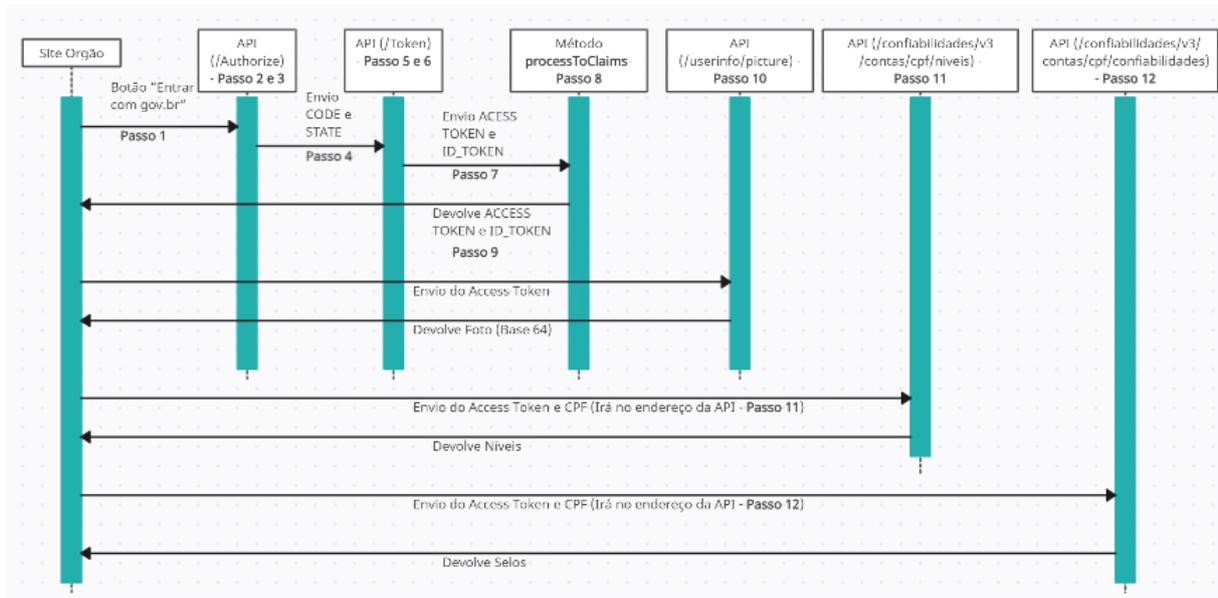


Figura 2.10: Fluxo de autenticação básico da **Conta gov.br** (Fonte: Secretaria de Governo Digital [36]).

Antes de descrevermos o processo, é importante notar a semelhança do diagrama apresentado aqui com aquele ilustrado pela Figura 2.5. Essa similaridade não é ao acaso, uma vez que ela acontece porque a **Conta gov.br** utiliza a arquitetura do *OpenID Connect* como solução de autenticação e autorização.

Os passos do procedimento apresentado são os seguintes:

1. O acionamento do botão **Entrar com gov.br** solicita uma nova autenticação.
2. O *endpoint* `/authorize` é sensibilizado, e o Provedor OpenId da **Conta gov.br** verifica se o usuário está logado. Caso não esteja, redireciona para a página de login.
3. A página de login faz uma requisição `GET` para o *endpoint* `/authorize`. Nesse passo há algumas considerações específicas da **Conta gov.br**: os parâmetros `state`, `code_challenge` e `code_challenge_method` devem ser usados.

Conforme Wilson e Hingnikar [34] e Siriwardena [33], a especificação do OpenID Connect tem as seguintes definições para os parâmetros:

- **state** - Um número aleatório ou *string* que é enviado para o provedor OpenID, que deve retornar exatamente o mesmo parâmetro de estado e valor em uma resposta de sucesso. Busca evitar ataques de *token injection* e *Cross-Site Request Forgery* (CSRF). Essa proteção acontece porque um link malicioso que tenha sido enviado a uma vítima não terá o valor de **state** gerado e anexado à

sessão dela, ao mesmo tempo que um atacante é incapaz de replicar o valor ao acaso. A aplicação cliente, ao receber um valor diferente daquele que passou quando iniciou a sessão, deve rejeitar a resposta e encerrar a conexão.

- `code_challenge` - Código de desafio derivado do uso do *Proof Key for Code Exchange* (PKCE), um mecanismo que garante que a aplicação que solicitou um código de autorização é a mesma que obtém o `ACCESS_TOKEN`. Essa proteção é oriunda do seguinte fluxo:
  - A aplicação gera uma *string* aleatória e criptograficamente segura, chamada de `code verifier`.
  - Calcula um valor derivado, o `code challenge`, a partir do `code verifier`.
  - Inclui o `code challenge` e o método de derivação na solicitação de autorização.
  - Envia o `code verifier` ao servidor de autorização quando solicitar o `ACCESS_TOKEN`.
  - O servidor de autorização transforma o `code verifier` usando o método recebido na solicitação de autorização.
  - O resultado é comparado com o `code challenge` enviado para verificar a autenticidade da solicitação. Como apenas a aplicação legítima conhece o `code verifier`, um agente malicioso não poderia usar um código de autorização roubado, já que não conseguiria replicar a informação.
- `code_challenge_method` - O método utilizado para derivar o `code challenge` do `code verifier`. Pode ser `plain` ou `S256`. Na prática, deve usar a opção `S256`, que utilizará um *hash* SHA256 codificado em URL base64 do `code verifier` para protegê-lo, uma vez que a opção `plain` usa os mesmos valores tanto para o `code verifier` quanto para o `code challenge`, não havendo qualquer proteção em um eventual comprometimento do valor. O uso de `S256` é obrigatório na integração com a *Conta gov.br*.

4. Com a autenticação bem-sucedida, é gerado um Código de Autorização (*Authorization Code*) que é retornado para a aplicação utilizando o parâmetro `redirect_uri`, passado na requisição para o *endpoint* `/authorize`. Esse endpoint que vai permitir que a aplicação envie uma nova requisição para o Provedor OpenId, dessa vez para recuperar os *tokens* de ID (`ID_TOKEN`) e de Acesso (`ACCESS_TOKEN`). O `state` também é enviado na resposta, possibilitando que a aplicação possa verificar se é uma resposta legítima para a requisição que iniciou anteriormente.
5. O provedor redireciona para a página de autorização, onde os recursos requeridos pela aplicação são mostrados para o usuário, conforme exemplo da Figura 2.11.

Ele então pode avaliar e decidir se vai autorizar ou não o compartilhamento de informações com a aplicação.

## Autorização de uso de dados pessoais

### Serviço: e-Cidadania

Este serviço precisa utilizar as seguintes informações pessoais do seu cadastro:

- Identidade gov.br
- Nome e foto
- Endereço de e-mail

A partir da sua aprovação, a aplicação acima mencionada e a plataforma gov.br utilizarão as informações listadas acima, respeitando [os termos de uso e o aviso de privacidade](#).



Figura 2.11: Autorização solicitada pelo sistema integrado para a *Conta gov.br*. (Fonte: O Autor.)

6. Caso o usuário autorize o acesso, será feita a chamada ao endpoint `/token` para obtenção do `ACCESS_TOKEN` e `ID_TOKEN`. É nesse momento que as credenciais fornecidas pela Equipe Técnica da SGD entram em cena, pois devem ser usadas na requisição `POST` que será feita. Além deste dado, a URL de retorno cadastrada na solicitação de integração também deve ser enviada no corpo do *request*, além do `code` e `code_verifier`, que vão proteger a requisição de ataques, como visto anteriormente.
7. Os *tokens* de Acesso e de ID retornam para a aplicação consumidora, que pode utilizá-los para consultar dados de recursos protegidos.
8. Uma verificação de autenticidade dos *tokens* é feita antes de seu uso, com base na chave pública da *Conta gov.br*. Ela é recuperada por meio de um serviço disponibilizado pela infraestrutura do Login Único chamado `processToClaims`, e cabe à aplicação realizar essa validação.
9. O `ACCESS_TOKEN` e o `ID_TOKEN` validados ficam à disposição da aplicação, que pode ter acesso às informações como o CPF ou CNPJ do usuário que se autenticou e qual o meio de autenticação utilizado (instituição bancária, certificado digital, etc).
10. Esse passo é executado caso a aplicação queira obter a foto de perfil do usuário, acessando o *endpoint* `/userinfo/picture` usando o `ACCESS_TOKEN`, que é retornada em formato Base64.

11. Essa etapa serve para verificar os Níveis de Autenticação do usuário que está logado. Dessa forma, ela contém dados que serão usados pela lógica de autorização do sistema cliente, já que ele pode modificar seu comportamento de acordo com o Nível retornado (Bronze, Prata ou Ouro). Eles são obtidos através de uma chamada GET para o endpoint `/confiabilidades/v3/contas/cpf/niveis?response-type=ids`
12. Os Selos de Confiabilidade da conta logada podem ser verificados através da chamada ao endpoint `/confiabilidades/v3/contas/cpf/confiabilidades?response-type=ids`, permitindo que a aplicação tenha uma granularidade maior na customização da experiência do usuário, se assim desejar.

Concluindo a análise técnica, cabe ressaltar que existem várias bibliotecas que encapsulam a lógica das aplicações que são clientes de um provedor de identidade OpenId Connect, como cita Wilson e Hingnikar [34]. Uma breve pesquisa no repositório de códigos GitHub retornou 277 resultados nas mais variadas linguagens como, por exemplo, Go, PHP e Java [40].

## 2.2 Interação Humano-Computador (IHC)

A invenção do computador teve impactos consideráveis na sociedade como um todo. Porém, segundo Shneiderman e Plaisant [41], os computadores iniciais eram utilizáveis apenas por pessoas que dedicavam esforço para dominar a tecnologia, característica que era uma barreira na democratização desse recurso. Conforme os autores citados, para tentar sanar o problema, entraram em ação os designers, combinando entendimento tecnológico com a sensibilidade às capacidades e necessidades humanas, lançando as bases de uma linha de conhecimento intitulada Interação Humano-Computador (*Human-Computer Interaction*).

Segundo Barbosa e da Silva [42], a IHC é uma área que está interessada na qualidade de uso dos sistemas e no impacto na vida de seus usuários. Os autores enfatizam que a construção do software clássica prioriza a concepção de artefatos técnicos, como algoritmos e representações dos dados, não se importando com a forma como o sistema será utilizado. A Interação Humano-Computador muda essa abordagem, investigando os atores envolvidos, seus interesses, objetivos e atividades, entre outros aspectos, para depois verificar como essas características influenciarão a interface do usuário, e como o sistema viabilizará essa forma de intervenção.

Grudin [43] relata que o primeiro trabalho sistemático dessa área foi feito por especialistas da área de Fatores Humanos e Ergonomia, o que já delineava a natureza multidisciplinar da IHC. Publicado em 1959 por Brian Shackel, o artigo “*Ergonomics for a*

*Computer*” [44] descrevia o redesign do computador EMIAC e abria caminho para estudos semelhantes.

Desde então, a Interação Humano-Computador veio ganhando destaque e, em 1997, Carrol [45] descreve as razões: tecnicamente, por evocar problemas complexos e soluções elegantes na história recente da computação; culturalmente, por abranger as opiniões e ideias do público não especializado sobre a tecnologia da informação e seu impacto em suas vidas, tornando-se a parte visível da ciência da computação; e comercialmente, à medida que as tecnologias básicas da computação se tornam *commodities*, o que tem sido considerado um fator diferencial nesse campo é o design de aplicações e interfaces de usuário, dando importância à IHC. O autor conclui definindo a Interação Humano-Computador como uma ciência do design que busca entender e apoiar seres humanos interagindo com e através da tecnologia. Olson e Olson [46] completam a definição ao sintetizar um objetivo para a área como: produzir software e hardware que é útil, esteticamente agradável e *usável*. Esta última característica é importante, pois se relaciona com um campo específico da IHC que é a *Usabilidade*, a qual será vista com mais detalhes na próxima seção.

### 2.2.1 Usabilidade

Usabilidade, no contexto de produtos interativos, pode ser descrita como a característica que garante que eles sejam fáceis de aprender, eficazes de usar e agradáveis do ponto de vista do usuário, segundo Preece et al. [47]. Eles também enumeram os objetivos que compõem essa área:

1. Eficácia: um objetivo amplo, que busca descrever se o sistema está cumprindo o propósito no qual foi concebido.
2. Eficiência: se refere a como o sistema apoia os usuários no cumprimento das suas tarefas, afetando sua produtividade.
3. Segurança: envolve a proteção que o sistema oferece para que o usuário se mantenha a salvo de situações perigosas ou condições indesejadas.
4. Utilidade: aborda o quanto o sistema provê a funcionalidade correta para que os usuários façam o que precisam fazer.
5. Aprendizagem: refere-se à facilidade com que um sistema pode ser aprendido para uso.
6. Memorabilidade: trata-se da facilidade com que um sistema pode ter seu uso lembrado, uma vez que já tenha sido aprendido.

Uma das formas dos sistemas melhorarem os aspectos acima é através da Engenharia de Usabilidade, segundo Lecerof e Paterno [48]. Nesse campo da Interação Humano-Computador (IHC), o objetivo é tornar os sistemas mais usáveis por meio da aplicação de métodos em diferentes etapas do processo de design e desenvolvimento, de maneira estruturada e sistemática. Eles destacam que uma das ferramentas que a Engenharia da Usabilidade lança mão é a execução de avaliações de usabilidade. Esses testes devem ser feitos, se possível, nos estágios iniciais do desenvolvimento e, geralmente, têm uma meta específica entre as seguintes: validar se o design é bom o suficiente; comparar designs alternativos; avaliar o impacto do design no mundo real; e, finalmente, checar se o design adere a padrões especificados. Verificaremos na próxima seção detalhes desse tipo de avaliação.

### **2.2.2 Testes de usabilidade**

De acordo com Lewis [49], o teste de usabilidade é uma metodologia que visa observar os usuários enquanto eles realizam tarefas específicas no uso de alguma ferramenta, dentro de um ambiente de teste. O objetivo é verificar o quão bem as pessoas conseguem usar aquela solução para o propósito ao qual ela se destina. Lazar [50] acrescenta que o teste de usabilidade não se limita à pesquisa com usuários, se concentrando também na interface do sistema quando aplicado a soluções computacionais. O objetivo é reunir informações para melhor satisfazer as necessidades e expectativas dos usuários e entender como eles interagem com estas soluções.

Segundo Ghasemifard et al. [51], a melhoria do design é o propósito primário dos testes de usabilidade. Esses testes envolvem a coleta sistemática das informações de usabilidade, sendo que os dados obtidos através das sessões de teste criam parâmetros claros que devem ser melhorados ou suprimidos na solução. Por fim, os autores ainda ponderam que a observação dos usuários tendo problemas com a solução contribui para que os desenvolvedores tenham empatia pelos clientes.

Apresentaremos, nas próximas seções, exemplos de técnicas e métricas de usabilidade que podem ser utilizadas na implementação de uma avaliação.

## **2.3 Métodos de Teste de Usabilidade**

Uma metodologia pode ser descrita como um corpo de métodos, procedimentos e regras empregadas por uma ciência ou disciplina [52]. Dentro desse contexto, podemos afirmar que há diversas metodologias de teste de usabilidade, cada uma com sua sequência de passos e objetivos. Esses métodos, segundo Rubin [53], funcionam como uma sinopse

de como a seção de teste funcionará, provendo uma visão geral do que será feito pelos participantes.

Veremos a seguir alguns exemplos de metodologias que foram encontradas na literatura, descrevendo o funcionamento geral e seus objetivos principais.

### **2.3.1 Avaliação Heurística**

A avaliação heurística foi um método informal proposto por Nielsen e Molich [54], que consiste em solicitar que um grupo de avaliadores inspecione a interface de um produto e indique, na sua opinião, o que está bom e o que pode apresentar problemas. Neste estudo os autores conseguiram verificar que uma avaliação individual não traz resultados significativos, mas ao agregar as respostas de vários avaliadores, era possível ter um retorno mais confiável sobre as questões de usabilidade. Posteriormente o próprio Nielsen [55] sugeriu características para que a análise heurística fosse mais objetiva, formando o conjunto que é conhecido hoje como Heurísticas de Nielsen.

Com o tempo, a técnica está sendo refinada para que se torne mais robusta e produza respostas melhores. Abulfaraj e Steele são autores que investigaram dois aspectos desse método: o primeiro estudo [56] identificou o “Efeito da Experiência”, estabelecendo a correlação entre a qualidade da avaliação e a experiência do avaliador; já a segunda pesquisa [57] teve como objetivo simplificar as Heurísticas de Nielsen para avaliadores novatos, buscando, assim, aumentar a efetividade dos testes feitos por esse público, através da criação de um passo-a-passo de como fazer a análise.

As principais vantagens do método são o custo baixo, a facilidade de compreensão da aplicação e a ausência de necessidade de um planejamento avançado para aplicá-lo. O objetivo é identificar problemas antes que se tenha avançado muito no desenvolvimento da solução, uma vez que ele pode ser aplicado nos estágios iniciais da implementação.

### **2.3.2 *Cognitive Walkthrough***

A técnica do *Cognitive Walkthrough* (Percurso Cognitivo, em tradução livre), foi proposta por Polson et al. [58], e tem como objetivo principal assegurar a facilidade no aprendizado do produto que está sendo desenvolvido. Baseado na Teoria da Aprendizagem Exploratória [59], o método considera que os usuários aprendem a usar o sistema através da exploração e interação com o mesmo.

Sua aplicação, conforme Lazar [50], é feita por especialistas que simulam ser usuários, percorrendo uma série de tarefas na interface que está sendo avaliada. Ghasemifard et al. [51] explicam que formulários são utilizados para guiar o processo de avaliação, que é baseado em quatro passos:

1. Definição de Objetivos: O usuário define um objetivo que deseja alcançar com o sistema;
2. Busca por Opções de Ação: O usuário examina a interface em busca de opções de ação disponíveis que possam ajudá-lo a progredir em direção ao seu objetivo;
3. Seleção de Ação: O usuário seleciona a ação que parece mais provável de fazer progresso em direção ao objetivo estabelecido;
4. Execução e Avaliação: O usuário executa a ação escolhida e avalia o *feedback* do sistema para determinar se a ação o ajudou a se aproximar do objetivo.

Como vantagens do seu uso, Jeffries et al. [60] indicaram que a metodologia ajuda a definir os objetivos e assunções dos usuários, e que os próprios desenvolvedores de software poderiam utilizá-la. Porém, para isso é necessário que eles tenham experiência na definição das tarefas que serão realizadas, além de sua execução ser tediosa. Estudos conduzidos por Jacobsen [61] mostraram que essa desvantagem poderia ser diminuída com a simplificação do processo, sem perder a eficácia. Todavia, os mesmos estudos perceberam que pode haver uma variação significativa dos resultados por diferentes avaliadores, inspirando cuidados ao escolher a técnica.

### **2.3.3 Contextual Inquiry**

A técnica do *Contextual Inquiry*, ou Inquérito Contextual, foi introduzida por Beyer e Holtzblatt em 1998 [62] como parte do *Contextual Design*, um processo centrado no usuário que tem como objetivo entender como as pessoas executam seu trabalho, de forma que seja possível descobrir um padrão ótimo para esse trabalho. Segundo os autores, a premissa básica do método é simples: ir até o local de trabalho do cliente, observar como ele desenvolve esse trabalho e falar com ele sobre como ele trabalha. Dessa forma, eles afirmam, o entendimento do ambiente do cliente se torna inevitável. É possível ter uma noção geral do processo na Figura 2.12.

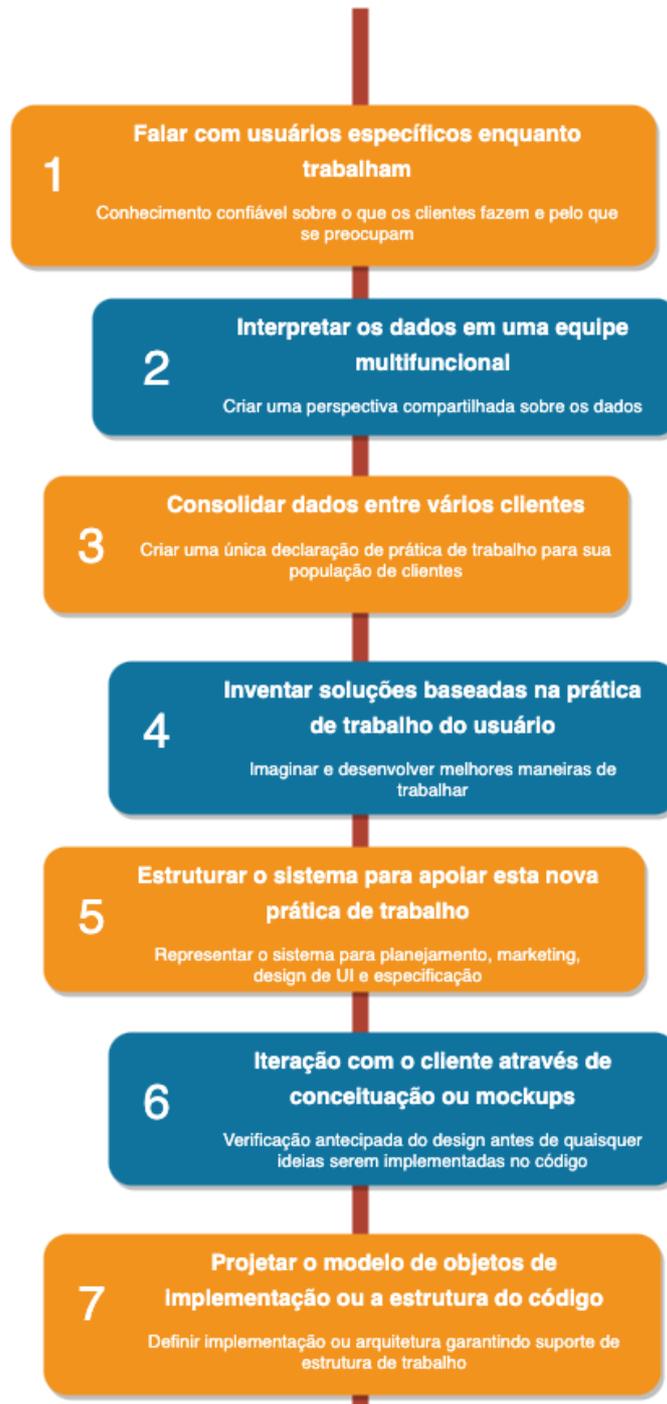


Figura 2.12: Processo de *Contextual Design*. (Fonte: Beyer e Holtzblatt (Adaptado) [63]).

Preece et al. [47] conceituam o método como uma abordagem onde o designer atua como aprendiz do usuário. Para isso, os autores afirmam, é utilizada a entrevista contextual, que combina observação, discussão e reconstrução de eventos passados e se baseia em quatro princípios:

1. Contexto: Este princípio enfatiza a importância de ir ao local de trabalho para observar o que acontece diretamente.
2. Parceria: Afirma que o desenvolvedor e o usuário devem colaborar para entender o trabalho. Diferentemente de entrevistas ou *workshops* tradicionais, onde o entrevistador ou líder do *workshop* está no controle, o inquérito contextual promove uma parceria onde o entendimento é desenvolvido cooperativamente.
3. Interpretação: Observações devem ser interpretadas para serem utilizadas no design, e essa interpretação deve ser obtida em uma cooperação entre o usuário e o desenvolvedor.
4. Foco: É importante que a discussão permaneça relevante para o design que está sendo desenvolvido. Para isso, um foco de projeto é estabelecido para guiar o entrevistador, que será complementado pelo foco individual que surge da perspectiva e do *background* do entrevistado.

Devido ao seu caráter imersivo, o uso do Inquérito Contextual na avaliação de usabilidade se mostra útil principalmente para verificar propostas de melhoria no design apresentado, uma vez que a observação *in loco* da utilização do sistema permite a identificação desses pontos. Como Holtzblatt e Beyer [64] afirmam, é possível identificar características como emoções, motivações e como o sistema se encaixa na vida do usuário, permitindo que o projetista incorpore a perspectiva deste na solução que está sendo feita.

### 2.3.4 Avaliação de Usuários

Testes de usabilidade feitos por avaliação de usuários (*User-based evaluations*) são testes que contam com a participação direta de pessoas, buscando criar uma amostra representativa dos potenciais utilizadores da solução, realizando tarefas típicas da mesma [51]. Lazar et al. [50] acrescentam que esses testes podem ser realizados em qualquer tempo do desenvolvimento, apesar de que, quanto mais cedo forem feitos, maior influência terão no design, além de diminuir os custos de alguma alteração.

Bastien [65] sugere que os testes de usuários sigam as seguintes etapas:

1. Definição dos objetivos do teste: Estabelecer claramente o que se espera alcançar com o teste.
2. Qualificação e recrutamento dos participantes: Identificar e selecionar os participantes adequados para o teste.
3. Seleção das tarefas: Escolher as tarefas específicas que os participantes executarão durante o teste.

4. Criação e descrição dos cenários das tarefas: Desenvolver e detalhar os cenários em que as tarefas selecionadas serão realizadas.
5. Escolha do que será medido e registro dos dados: Definir quais métricas serão coletadas e como os dados serão capturados.
6. Preparação dos materiais e do ambiente de teste: Organizar todos os recursos necessários e preparar o local onde o teste ocorrerá.
7. Escolha do testador e design do protocolo de teste: Selecionar quem conduzirá o teste e elaborar o conjunto de instruções e procedimentos a serem seguidos.
8. Design/seleção de questionários de satisfação e procedimentos de análise de dados: Preparar ou escolher questionários para avaliar a satisfação dos usuários e definir como os dados coletados serão analisados.
9. Apresentação e comunicação dos resultados: Consolidar os resultados do teste e comunicá-los às partes interessadas.

Dessa lista, daremos ênfase aos pontos que subsidiam à consecução de um dos nossos objetivos de pesquisa, que é a implementação do protocolo de testes de usabilidade. São eles: Recrutamento dos participantes; Seleção das tarefas e criação dos seus cenários; design e seleção de questionários e procedimentos de análise; e escolha do que será medido. Esse último tópico será visto em detalhes na Seção 2.4, enquanto os três primeiros serão vistos nas sequências.

### **Recrutamento dos participantes**

Os pontos principais na seleção dos participantes de uma avaliação de usabilidade são: custo, disponibilidade, adequação e objetivos do estudo, segundo Tullis e Albert [66]. Eles também enfatizam a importância dos participantes refletirem adequadamente o público-alvo do sistema que será testado.

Hass [67] acrescenta que uma das formas de garantir a referida fidelidade é com a criação de um conjunto de perguntas para qualificar ou desqualificar os potenciais participantes do estudo. As questões devem diferenciar de forma precisa e justa os participantes e os não-participantes. O autor adiciona que o pagamento de honorários para os participantes é juridicamente legal, muito embora faça ponderações sobre o valor a ser empregado nessa prática, uma vez que um pagamento muito alto pode ser considerado coerção financeira, se mostrando inadequado.

Hass [67] ainda aborda a importância da criação de um formulário de consentimento, que faça uma descrição geral sobre os parâmetros de participação no estudo e que contenha:

- Conteúdo do Formulário
  - Descrição dos riscos associados à participação
  - Explicação de como os riscos foram abordados pelos designers do estudo
  - Detalhes sobre os tipos de dados que serão coletados
  - Informações sobre quem terá acesso aos dados coletados.
- Responsáveis pelo Estudo
  - Identificação de quem está encarregado do estudo
  - Instruções de como contatar os responsáveis
- Compartilhamento de Experiências
  - Esclarecimento sobre se os participantes podem ou não compartilhar suas experiências do estudo com outros
- Processo de Consentimento
  - Oportunidade para os participantes indicarem seu consentimento, confirmando que entenderam e concordam com as informações fornecidas

Esse formulário é uma das bases para um princípio que deve nortear qualquer teste que envolva seres humanos, que é a utilização de Diretrizes Éticas. Blomberg e Burrell [68] afirmam que esses estudos exigem o desenvolvimento de confiança entre os pesquisadores e os participantes, caso contrário estes não compartilharão abertamente suas experiências. Isso demanda que o pesquisador reflita sobre as consequências do estudo na vida das pessoas que participaram da investigação, e como protegê-las de qualquer dano. Essas questões são endereçadas através de um balizamento ético abrangente.

Preece et al.[47] esclarecem que organizações profissionais, universidades, órgãos governamentais e escritórios de pesquisa geralmente exigem que os pesquisadores informem as atividades que serão feitas envolvendo participantes humanos. Eles também apontam que deve-se priorizar a proteção da privacidade dos indivíduos. Isso é feito assegurando que seus nomes não sejam vinculados aos dados coletados ou divulgados em relatórios escritos sem o seu consentimento, e também tratando informações pessoais detalhadas sobre saúde, emprego, educação, situação financeira e residência dos participantes como confidenciais.

Concluindo, em termos da quantidade de participantes do teste, Albert e Tullis [69] sugerem duas opções de dimensionamento:

1. Cenários de menor risco: onde é aceitável não capturar todos os problemas de usabilidade.
  - Número recomendado de participantes: 5 a 10.
  - Uma equipe de UX é suficiente.
  - Condições:
    - Foco em capturar problemas grandes para iteração no design.
    - Apenas um grupo principal de usuários com visões semelhantes sobre o design e tarefas.
    - Escopo do design limitado com número gerenciável de telas, páginas ou tarefas.
  
2. Cenários críticos: nos quais há a necessidade de capturar a maioria dos problemas de UX.
  - Número recomendado de participantes: 10 a 25.
  - Múltiplos pesquisadores de UX para identificação independente de problemas de usabilidade.
  - Condições:
    - Importante capturar o máximo possível de problemas de UX.
    - Consequências negativas significativas ao perder problemas maiores.
    - Comparação estatística necessária (por exemplo, entre designs ou com uma linha de base).
    - Múltiplos grupos de usuários ou usuários particularmente diversos.
    - Escopo do design amplo, recomendando-se um conjunto abrangente de tarefas.

Em suma, os autores recomendam ajustar esse número de acordo com o objetivo do teste, os recursos disponíveis e a criticidade dos resultados para o desenvolvimento do produto.

### **Confecção de roteiros para testes de usabilidade**

Criar um roteiro das tarefas que o usuário deve fazer em uma avaliação de usabilidade é um dos aspectos mais desafiadores dentro do teste, segundo Lazar [50]. Isso porque as tarefas precisam ter algumas características para que sejam exploradas em todo seu potencial:

- Devem direcionar para um objetivo claro.
- Ser claras e inequívocas, para que não precisem de explicações adicionais.
- Possuir uma resposta ou solução evidentes, para que os participantes saibam que completaram a tarefa.
- Ter relação com os recursos-chave da interface.
- Não solicitar informações que os usuários já possam saber de antemão, uma vez que podem ignorar o uso da interface para isso.
- Baseada em fatores como frequência, centralidade nos objetivos do usuário ou criticidade.

Preece et al. [47] acrescentam que uma lista de tarefas permite obter medidas de desempenho quantitativas, como o tempo de conclusão, número e tipo de erros por tarefa, e quantos usuários completaram-na com sucesso. Eles prosseguem na análise afirmando que essas tarefas podem ter uma variação de complexidade bem ampla, podendo ser algo simples como encontrar uma informação, até algo mais difícil, como criar um design. O importante é que seja possível caracterizar o nível de usabilidade atual, e identificar os limites mínimos aceitáveis e o patamar que sugere um nível alto de desempenho.

Além de todos esses indicadores, um estudo conduzido por Lindgaard e Chattratchart [70] identificou uma correlação forte entre a quantidade de tarefas e o número de novos problemas de usabilidade encontrados, sugerindo que a confecção dessa lista pode aumentar a probabilidade de detecção de erros durante a fase de design, evitando problemas após o lançamento da solução.

Uma forma de potencializar o uso das tarefas em uma avaliação de usabilidade é através da descrição das mesmas através de cenários. Isso porque, segundo Kwang Bok Lee e Grice [71], cenários de tarefas descrevem atividades típicas que os desenvolvedores esperam dos usuários. Por estarem alinhados aos objetivos do plano de teste, fornecem mais precisão ao que se quer avaliar. Ademais, a inclusão de contexto e motivação para as tarefas provida pelo cenário remove a artificialidade do teste.

Há cinco diretrizes para a confecção desses cenários, como indica Rubin [53]:

1. Descrever cenários realistas, completando-os com motivações para sua execução: cenários próximos da realidade aumentam a confiabilidade dos testes e ajudam participantes a se manterem no papel, superando hesitações. Incluir contexto e razões realistas para as tarefas ajudam a avaliar o design do produto.
2. Criar uma ordem para os cenários: sequenciar cenários de tarefas na ordem mais provável de execução ajuda a manter autenticidade, guiar participantes como aprenderiam na prática, e revelar efeitos acumulados de erros. Se a ordem sequencial não

for crucial, a variação na apresentação dos cenários (contra-balanceamento) pode evitar vieses e fornecer *insights* sobre sequências e prioridades naturais.

3. Alinhar os cenários com a experiência do participante: nem todos os participantes devem explorar os mesmos aspectos do produto. Recursos, telas ou seções do manual que são avançados demais não devem ser acessados por participantes novatos, pois esses elementos são complexos para eles. Ao mesmo tempo, participantes mais experientes podem ignorar as funcionalidades básicas.
4. Evitar o uso de jargões ou dicas: é importante não incluir nos enunciados nomes de botões, itens de menu ou títulos de telas, para não fornecer pistas não intencionais aos participantes que eles não encontrariam fora do ambiente de teste.
5. Prover cenários de trabalho substanciais: é recomendado apresentar um objetivo claramente definido em linguagem simples e permitir que os participantes executem as tarefas por conta própria. A meta é observar se os participantes conseguem realizar todas as etapas intermediárias necessárias para alcançar o objetivo final, o que revela sua compreensão conceitual do produto e destaca quaisquer mal-entendidos sobre seu uso.

O atendimento a esses princípios não apenas contribui para testes eficazes, mas também se torna peça fundamental para o design centrado no usuário.

## Questionários

Uma das formas de executar as avaliações de usuários é com o uso de questionários. Com eles, é possível que os participantes respondam perguntas quantitativas ou qualitativas enquanto executam as tarefas dos testes [71]. Além disso, questionários conseguem resumir o *feedback* dos usuários após a navegação em um site ou aplicativo de celular [72].

E, no que diz respeito aos meios de responder aos questionários, uma possibilidade é o uso da Escala Likert, que é uma escala ordinal de 5 ou 7 pontos utilizada para aferir atitudes, e que medem o quanto o respondente concorda ou discorda com o que foi questionado [73]. As respostas às perguntas variam entre afirmações como “Discordo Totalmente” a “Concordo Totalmente”, e podem ser usadas para diagnosticar problemas de usabilidade, assim como para medir o grau de satisfação do usuário imediatamente após completar uma tarefa [74].

Outra possibilidade é a estruturação de questionários com uma finalidade específica. Um exemplo desse caso foi a proposta de Wijayarathna et al. [75], que apresentaram um Questionário de Dimensões Cognitivas (*Cognitive Dimension Questionnaire*) a ser aplicado em desenvolvedores que usavam uma API de segurança. As perguntas foram

ajustadas pra verificar qual o nível de dificuldade que esses programadores tinham em aprender e usar as ferramentas.

Um caso adicional de questionário especializado é o *System Usability Scale* (SUS). Proposto por Brooke [76], é um método que buscou resolver o problema da falta de praticidade existente na avaliação de usabilidade de diferentes soluções. Como a análise de contexto e a seleção de métricas adequadas pode ser um processo oneroso, geralmente esse custo inviabilizava a execução de avaliações. Diante de tal cenário, o pesquisador procurou uma medida rápida e simples de examinar a usabilidade, ao mesmo tempo que fosse confiável o suficiente para identificar mudanças entre versões de um produto de software.

Para isso, construiu-se um questionário com dez itens, baseado na Escala Likert, para fornecer uma visão global das avaliações subjetivas de usabilidade. A escolha dos itens para compor o teste procurou identificar exemplos que provocassem unanimidade em termos de concordância ou discordância extrema, evitando ambiguidades. O processo resumido de confecção foi o seguinte:

- Dois sistemas de software, um considerado muito fácil, e outro, muito difícil, foram escolhidos para avaliação;
- Um questionário com 50 perguntas potenciais foi respondido por um conjunto de 20 pessoas de diferentes ocupações e graus de expertise em tecnologia;
- As respostas eram medidas em uma Escala Likert de 5 pontos;
- Os itens que geraram respostas mais extremas foram selecionados para a escala final;
- Uma alternância entre itens positivos e negativos foi feita para estimular a resposta consciente de cada um deles

A escala final resultante abrange diversos aspectos da usabilidade, como necessidade de suporte, treinamento e complexidade, e sugeria ter uma validade aparente para medir a usabilidade de um sistema. Mais tarde, essa premissa foi confirmada por outros estudos [77] [78] [79]. O modelo do questionário está descrito no Quadro 2.2, contendo a pergunta original em inglês, a tradução para o português do Brasil proposta por Lourenço et al. [80] e o viés da pergunta (positivo ou negativo):

Número	Pergunta original	Tradução - Português do Brasil	Viés
1	<i>I think that I would like to use this system frequently.</i>	Eu acho que gostaria de usar esse sistema frequentemente.	Positivo
2	<i>I found the system unnecessarily complex.</i>	Eu achei esse sistema desnecessariamente complexo.	Negativo
3	<i>I thought the system was easy to use.</i>	Eu achei esse sistema fácil de usar.	Positivo
4	<i>I think that I would need the support of a technical person to be able to use this system.</i>	Eu achei que precisaria de ajuda de uma pessoa técnica para ser capaz de usar esse sistema.	Negativo
5	<i>I found the various functions in this system were well integrated.</i>	Eu achei que as várias funções desse sistema foram bem integradas.	Positivo
6	<i>I thought there was too much inconsistency in this system.</i>	Eu acho que o sistema apresenta muita inconsistência.	Negativo
7	<i>I would imagine that most people would learn to use this system very quickly.</i>	Eu imagino que a maioria das pessoas pode aprender a usar esse sistema rapidamente.	Positivo
8	<i>I found the system very cumbersome to use.</i>	Eu achei esse sistema muito pesado para usar.	Negativo
9	<i>I felt very confident using the system.</i>	Eu me senti muito seguro usando o sistema.	Positivo
10	<i>I needed to learn a lot of things before I could get going with this system.</i>	Eu precisei aprender muitas coisas antes que pudesse utilizar esse sistema.	Negativo

Quadro 2.2: Perguntas do questionário SUS. (Fonte: O Autor.)

Cada uma dessas perguntas pode ser respondida por uma escala de cinco pontos, que vai de “Discordo fortemente” até “Concordo fortemente”, onde o primeiro corresponde a 0 pontos. Esse valor é incrementado em 1 ponto por cada item da escala, fazendo com que o último valha 4 pontos. Para obter o valor numérico da avaliação, deve-se executar as seguintes ações:

1. Identificar qual o valor marcado na resposta (V);
2. Caso a pergunta tenha um viés positivo, subtrai-se 1 ponto do valor obtido (V-1);

3. Se o viés for negativo, a forma do cálculo muda, e deve-se subtrair o valor posicional do número 5 (5-V);
4. Soma-se todos os itens e multiplica-se por 2,5.

Esse algoritmo fornecerá um valor que varia de 0 a 100 pontos. Esse número por si só já permite a comparação de dois sistemas. Porém, Bangor et al. [81] resolveram aprimorar o trabalho ao determinar uma escala de adjetivos para o valor obtido na avaliação do SUS. A Figura 2.13 ilustra o resultado:

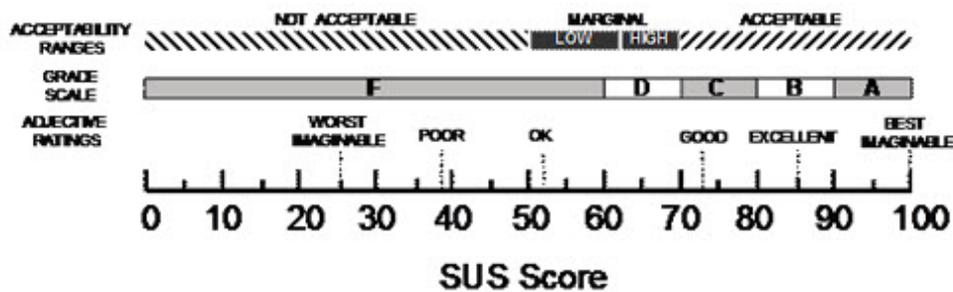


Figura 2.13: Escala de adjetivos x pontuação SUS. (Fonte: Bangor et al. [81]).

Essa escala permite que valores obtidos com a aplicação do questionário possam ter interpretações individuais, fornecendo também uma forma mais amigável de reportar o resultado do trabalho para pessoas que não são especialistas. Podemos verificar que o valor mínimo aceitável, pela escala, seria o total de 70 pontos. Uma Boa experiência seria algo em torno de 73 pontos, enquanto um *score* de 85 pontos já seria considerada uma solução com Excelente usabilidade.

Finalizando, um ponto importante ao utilizar questionários é a verificação da sua consistência interna, ou seja, o quão as respostas expressadas por eles são confiáveis ao ponto de permitir fazer algum tipo de previsão, segundo Wadkar et al.[82]. Uma das formas de assegurar essas características, segundo Heo et al.[83] é através do cálculo do Coeficiente *Alfa de Cronbach*, um índice que varia de 0 a 1 e é obtido através da média das correlações dos itens do questionário. Streiner [84] afirma que o valor mínimo aceitável para seu resultado é de 0,70, pois um número abaixo desse limite indica que as respostas do questionário estão inconsistentes.

## Entrevistas

Entrevistas constituem uma ferramenta de avaliação de usabilidade que é melhor utilizada em situações que exigem informações detalhadas de um número pequeno de respondentes, conforme afirmam Dumas e Salzman [85]. Nessa situação, elas são realizadas no final dos

testes, para revisar eventos-chave e coletar impressões finais dos participantes sobre a usabilidade do produto.

Preece et al. [47] também as descrevem como conversas com um propósito, e pontuam que a similaridade delas com uma conversa ordinária varia conforme as perguntas a serem respondidas e o tipo de entrevista utilizada, que são basicamente quatro:

1. Abertas ou não estruturadas - As perguntas feitas são abertas, permitindo que o formato e o conteúdo das respostas não sejam predeterminados, e o entrevistado tem liberdade para responder de forma tão extensa ou breve quanto desejar;
2. Estruturadas - Utilizam perguntas predeterminadas (fechadas), semelhantes às de um questionário, e as respostas envolvem a escolha de opções pré-definidas;
3. Semiestruturadas - Integra elementos das entrevistas estruturadas e não estruturadas, ao empregar perguntas fechadas e abertas. O entrevistador inicia com perguntas pré-planejadas para orientar a conversa, e depois incentiva o entrevistado a elaborar as respostas em busca de maior profundidade;
4. Entrevistas em grupo - Dinâmica que normalmente envolve de três a dez pessoas, selecionadas de forma a representar uma amostra de usuários típicos. Permite discutir questões diversas ou sensíveis que poderiam ser ignoradas.

Dumas e Salzman [85] concluem que a efetividade da entrevista está diretamente ligada à habilidade do entrevistador, que deve buscar um treinamento específico para essa situação e fazer um preparo cuidadoso de como conduzirá as sessões.

### ***Think Aloud Protocol***

A técnica do “Pensar em Voz Alta” (*Think Aloud*) consiste em instruir que os participantes verbalizem suas ações e pensamentos durante a execução de uma determinada tarefa, segundo Lewis [49]. Ele também pontua que as verbalizações confiáveis são aquelas produzidas durante a execução da tarefa, e que não exigem processamento cognitivo adicional além do necessário para realizar a ação e falar sobre o que se está fazendo.

O processo de coleta de dados utilizando o método *Think Aloud* pode ser descrito nos seguintes tópicos principais, segundo Fonteyn et al. [86]:

- Ambiente de Coleta de Dados - Sessões individuais em um ambiente tranquilo que facilite o pensamento em voz alta;
- Registro de Dados - Sessões gravadas em áudio e posteriormente transcritas para gerar dados verbais;

- Instruções aos Participantes - Após assinar o consentimento, os participantes são instruídos a verbalizar seus pensamentos enquanto resolvem tarefas simuladas;
- Lembrete Contínuo - Se os participantes pausarem por mais de alguns segundos, são lembrados pelo investigador para continuar pensando em voz alta;
- Minimização da Interação - Interações entre o participante e o investigador são mantidas no mínimo para não interferir no fluxo de pensamentos;
- Notas do Investigador - O investigador toma notas sobre o conteúdo verbalizado, incluindo pontos que precisam de esclarecimento;
- Entrevista de Acompanhamento - Após a coleta de dados, uma breve entrevista de acompanhamento pode ser conduzida para esclarecer o pensamento dos participantes e identificar suas estratégias de raciocínio;
- Coleta de Dados Demográficos - Dados demográficos são coletados para fornecer informações descritivas sobre os participantes.

Há uma variação do método, descrita por Albert e Tullis[69], que consiste em capturar os pensamentos dos participantes após a execução da tarefa, mostrando a eles um lembrete do que fizeram através de um vídeo ou replay de rastreamento ocular. Intitulada *Retrospective Think-Aloud*, ela se ancora em evidências de que a carga cognitiva do *Think Aloud* Simultâneo pode reduzir o sucesso dos participantes na tarefa. Porém, eles também pontuam que outro estudo indicou que a detecção de problemas de usabilidade era maior usando a técnica tradicional.

## 2.4 Métricas de Aferição de Usabilidade

Uma métrica é uma maneira de medir ou avaliar um fenômeno particular ou um item, e existem em diversas áreas da vida cotidiana, segundo Albert e Tullis [69]. Os autores afirmam, também, que na área de Experiência do Usuário (*User Experience - UX*) elas são responsáveis por indicar a experiência pessoal de um ser humano ao utilizar um produto ou sistema.

Bevan e Macleod [87] afirmam que as medidas de usabilidade refletem a qualidade de uso de um sistema, e que podem ser aferidas como o resultado da interação em um contexto, considerando: Eficácia, Eficiência e Satisfação.

Descreveremos nas próximas seções as características gerais de cada um desses tipos, e daremos alguns exemplos práticos de métricas estabelecidas na literatura.

### 2.4.1 Eficácia

Índices de eficácia medem a extensão em que os objetivos pretendidos de uso do sistema são alcançados. Dois aspectos-chave podem ser considerados nessa dimensão: *completude*, aferida pela proporção do conteúdo completado em relação ao total pretendido; e *precisão*, indicada pela exatidão com que o usuário atinge seus objetivos. Como um exemplo prático, se considerarmos a transcrição de um documento de duas páginas em um formato específico, a precisão seria medida pelos erros de ortografia e desvios de formato, enquanto a completude seria proporção de palavras transcritas em relação ao total no documento original [87].

Um exemplo claro de métrica desse tipo é a Precisão do Usuário (*User Accuracy*), que também pode ser interpretada como a Taxa de Sucesso de um usuário ao realizar uma determinada tarefa. Sauro e Lewis [88] ressaltam que essa é uma das métricas de usabilidade mais fundamentais, e são coletadas como uma medida binária, onde o sucesso da tarefa é codificado como 1 e a falha como 0. Por conta dessa característica, são reportadas como porcentagem ou proporção.

Rubin [53] sugere três estatísticas que podem ser derivadas da observação do sucesso da tarefa:

1. Porcentagem de Participantes com Sucesso (Incluindo Assistência): registra todos os participantes que concluíram a tarefa com êxito, independentemente de terem finalizado dentro do prazo estabelecido ou precisado de assistência.
2. Porcentagem de Participantes com Sucesso (Sem Assistência): indica a porcentagem de participantes que conseguiram completar a tarefa com sucesso por conta própria.
3. Porcentagem de Participantes com Sucesso dentro de um Tempo Estabelecido: reflete a eficiência e o desempenho correto, mostrando quantos participantes completaram a tarefa com sucesso dentro de um tempo pré-determinado.

Por fim, outra medida que pode ser derivada dessa observação é a Taxa de Falhas, calculada quando subtraímos o índice máximo de Precisão (100%) pelo valor obtido. A decisão de qual aspecto reportar depende do objetivo do estudo.

### 2.4.2 Eficiência

Métricas de eficiência medem a quantidade de recursos como tempo, dinheiro ou esforço mental que devem ser despendidos para alcançar os objetivos pretendidos por aquela solução [87]. Kwang Bok Lee e Grice [71] também associam a eficiência à capacidade do sistema ser fácil de lembrar, de maneiras que, uma vez que ele é aprendido, um alto nível de produtividade se torna possível.

Devido à sua relação com a dimensão temporal, os exemplos mais comuns de eficiência se propõem a medir intervalos entre acontecimentos, como o Tempo de Conclusão da Tarefa - TCT (*Task Completion Time*). Segundo Rubin [53], essa medida se refere a quanto tempo foi necessário para cumprir uma determinada tarefa, e as estatísticas comuns que o descrevem são a média, mediana, o intervalo e o desvio-padrão.

Albert e Tullis [69] sugerem outra métrica desse tipo: a quantidade de esforço necessário para a consecução da tarefa. Ela pode ser obtida contabilizando a quantidade de ações ou passos que os usuários realizam, e quanto maior o seu número, maior o esforço. Esse esforço pode ser tanto o cognitivo (encontrar o local para cumprir a ação, decidir qual deve ser feita) quanto o físico (mover o mouse, digitar um texto ou ligar um interruptor).

Encerrando, temos a Percepção de Facilidade de Uso (*Perceived Ease of Use*). Estudada por Davis[89], refere-se ao grau em que uma pessoa acredita que usar um sistema específico seria livre de esforço, afetando a produtividade geral, como visto anteriormente. Mas além desse impacto na eficiência, esse indicador pode influenciar na aceitação do produto como um todo. Um ponto levantado por Gefen e Straub [90] sugere que essa avaliação é impactada também pelo tipo pretendido de uso para qual a solução foi feita: se a aplicação foi projetada especificamente para uma tarefa, a facilidade com que as pessoas acham que podem usar essa tecnologia afeta sua vontade de usá-la.

### 2.4.3 Satisfação

Métricas de satisfação, segundo Bevan e Macleod [87], descrevem a usabilidade percebida do sistema como um todo pelos seus usuários e a aceitabilidade do sistema por eles e para outras pessoas afetadas pelo seu uso. Os aspectos mensurados podem estar relacionados a pontos específicos do sistema, ou compreender toda a solução.

Sauro e Lewis [88] indicam que as principais ferramentas para medir esse aspecto são:

- Questionários pós-tarefa: Preenchidos imediatamente após a realização de uma tarefa específica, avaliam uma parte da solução.
- Questionários pós-teste: Preenchidos ao final de uma sessão de usabilidade, geralmente abrangem uma avaliação de todo o sistema.
- Questionários fora de um teste de usabilidade: Preenchidos em um contexto não relacionado a uma sessão de teste específica, como uma pergunta de *feedback* após o uso de alguma funcionalidade.

Eles continuam a análise afirmando que é possível fazer as próprias perguntas de avaliação, mas que o recomendado é o uso de *questionários padronizados*, que já foram desenvolvidos por outras pesquisas e são projetados para reuso. Há quatro vantagens principais na sua utilização:

1. Objetividade: medidas padronizadas promovem a objetividade, permitindo que outros pesquisadores verifiquem de forma independente as medições.
2. Replicabilidade: utilizar métodos padronizados facilita a replicação de estudos, sejam eles de outros pesquisadores ou os próprios estudos anteriores do praticante. Isso também aumenta a confiabilidade dos achados.
3. Quantificação: medidas padronizadas permitem que os praticantes relatem resultados com o uso de métodos avançados de matemática e estatística, aumentando a compreensão dos dados.
4. Economia: embora o desenvolvimento de medidas padronizadas tenha um alto custo, uma vez desenvolvidas, seu reuso se torna muito fácil.

Um exemplo clássico de um questionário padronizado que mede a satisfação é o SUS, abordado em detalhes na Seção 2.3.4. Ele é classificado como um questionário *pós-teste*, pois tem o objetivo de capturar as percepções de usabilidade ao completar um conjunto de cenários de teste. Já um caso de questionário *pós-tarefa* seria o *Single Ease Question* - SEQ, um teste ilustrado pela Figura 2.14:



Figura 2.14: O *Single Ease Question* - SEQ. (Fonte: Sauro e Lewis [88]).

Como é possível perceber, esse teste consiste em uma única pergunta, que questiona: “De uma forma geral, essa tarefa foi:”, e fornece as opções de gradação a partir de Muito Difícil até Muito Fácil. Essa pergunta foi estudada por Tedesco e Tullis [91] em uma pesquisa que comparou cinco questionários pós-tarefa e mostrou que eles poderiam identificar as ações que os usuários tiveram dificuldades. Dentre eles, a pergunta que originou o SEQ foi a que teve o resultado mais consistente em amostras pequenas, tornando-o uma escolha simples e eficiente. Sauro e Lewis [88] apenas recomendam um ajuste em relação ao estudo original: ao invés de usar cinco pontos de escala, eles sugerem utilizar sete, pois estudos verificaram um aumento na confiabilidade da medida.

## 2.5 Síntese do Capítulo

Neste capítulo abordamos os pontos teóricos principais para entendimento da pesquisa. Em relação aos aspectos de Autenticação e Autorização (Seção 2.1), necessários para o

entendimento da *Conta gov.br*, verificamos uma noção geral desses dois conceitos, assim como os modelos mais utilizados para realizar a autenticação, que podem ser baseados em algo que a pessoa sabe, que ela tem, que ela é, ou uma mistura desses fatores.

Uma análise da prevalência do uso de senhas foi feita, e constatamos que a grande quantidade de credenciais em uso atualmente pode ser prejudicial para o usuário, comprometendo sua segurança. Tal efeito se deve ao impacto negativo que a necessidade de se autenticar traz, uma vez que o usuário vê essa etapa como um obstáculo para atingir os objetivos primários que tem ao utilizar um sistema. E, com isso, vimos que uma alternativa para combater o problema foi a instituição de sistemas de Login Único (*Single Sign-On*).

O modelo teórico do SSO foi examinado, assim como as vantagens de sua adoção. Os protocolos mais utilizados para sua implementação (Kerberos, SAML, OpenID, OAuth2.0 e *OpenID Connect*) foram apresentados, detalhando características, fluxos de autenticação e questões de segurança.

De posse desses conhecimentos, foi possível verificar a solução da *Conta gov.br*. Baseada no OpenID Connect, vimos que ela possibilita o acesso a diversos serviços públicos, permitindo que a experiência do usuário seja modificada através dos conceitos autorizativos de Níveis de Autenticação e Selos de Confiabilidade. Aspectos negociais e técnicos foram avaliados e discutidos quanto à sua utilização.

Já a Seção 2.2 focou nas bases da Interação Humano-Computador, destacando a importância que a área tem ao tornar as soluções computacionais mais acessíveis e úteis para todos, através do estudo de aspectos como a Usabilidade. Analisamos como essa característica é influenciada por atributos como a facilidade de aprendizado, eficiência e eficácia de uso e satisfação do usuário. Além disso, verificamos que é possível realizar testes sistemáticos para aferir qualidades e propor melhorias no design do sistema.

Apresentamos diferentes metodologias para realizar os testes de usabilidade, incluindo Avaliação Heurística, *Cognitive Walkthrough*, *Contextual Inquiry* e Avaliação de Usuários. Também discutimos a importância de selecionar a metodologia apropriada para os objetivos dos testes e características do sistema.

Finalmente, avaliamos as métricas mais comuns utilizadas na aferição de usabilidade, associadas aos aspectos de eficácia (quão bem os usuários alcançam seus objetivos), eficiência (recursos despendidos para alcançar esses objetivos) e satisfação do usuário.

O próximo passo é descrever o processo de Revisão Sistemática de Literatura, assim como analisar seus achados, de forma que tenhamos dados suficientes para elaboração do protocolo de testes de usabilidade que será usado na presente pesquisa.

## Capítulo 3

# Revisão Sistemática de Literatura

A Revisão Sistemática de Literatura, segundo definem Kitchenham et al.[92], é uma forma de identificar, avaliar e interpretar toda a pesquisa relevante disponível para uma determinada pergunta de pesquisa, tópico ou fenômeno de interesse. O processo envolvido em sua execução busca fornecer características como imparcialidade e transparência, permitindo que seus resultados possam ser utilizados ou reproduzidos por outros pesquisadores. O método divide os passos do trabalho em três grandes fases: Planejamento, Condução e Relatório.

Na fase de Planejamento, continuam os autores, é traçado o objetivo da RSL, ou seja, o que se espera descobrir com a revisão. Para expressar de maneira clara essa meta, Questões de Pesquisa (QP) são elaboradas, e devem ser respondidas ao final da busca. Além disso, são definidos:

- Protocolo de pesquisa - As bases que serão pesquisadas são estabelecidas, assim como critérios específicos de exclusão e inclusão dos estudos. Adicionalmente, os parâmetros que comporão a pesquisa são derivados do objetivo, formando um conjunto de termos que denominamos *String* de Busca.
- *Checklist* de mensuração de qualidade dos estudos - É montado um questionário para verificar a possibilidade de um determinado estudo responder às Questões de Pesquisa. Pontos são atribuídos às respostas, e uma pontuação de limite é fixada para verificar se aquele estudo é viável ou não.
- Formulários de extração de dados - Desenha-se um formulário que busca extrair dados estruturados que servirão de base para solucionar as Questões de Pesquisa.

Cada um desses passos tem a função de reduzir o viés do pesquisador na seleção dos estudos e viabilizar a análise por pares, pois permite a replicação dos procedimentos que determinaram os estudos incluídos na RSL [92].

Kitchenham et al.[92] descrevem a fase de Condução, onde as etapas do planejamento são executadas. A *String* de Busca que foi montada é aplicada nas bases selecionadas e os artigos resultantes (também conhecidos como *estudos primários*) são analisados à luz dos critérios de exclusão e inclusão. Os que satisfizerem os requisitos, passam pelo processo de avaliação de qualidade e, se atingirem a pontuação mínima definida, têm seus dados extraídos, estruturados e sintetizados.

Os autores concluem com a etapa final do processo, que organiza o modo como os resultados serão apresentados, e por isso, se denomina como fase de Relato ou Reporte. O formato e os mecanismos de disseminação da informação são estabelecidos e, caso a equipe responsável pela RSL considere necessário, uma revisão do relatório pode ser executada.

Todas as fases descritas anteriormente são seguidas pela ferramenta Parsifal, que foi utilizada no estudo. Dessa forma, as subseções a seguir descreverão como o procedimento foi executado utilizando o sistema, possibilitando a replicação por qualquer pesquisador que deseje replicar o protocolo.

## 3.1 Planejamento

### 3.1.1 Objetivo

A presente revisão sistemática tem como objetivo **identificar as principais técnicas e métricas de usabilidade aplicadas a soluções de login único, a fim de subsidiar a avaliação da *Conta gov.br* pelo Senado Federal**. Com isso, espera-se ter os fundamentos para a proposição de um protocolo de teste de usabilidade, que será aplicado posteriormente.

### 3.1.2 Questões de Pesquisa

Considerada por Kitchenham et al. [92] uma das tarefas mais importantes do planejamento da revisão, as Questões de Pesquisa (*Research Questions* - RQ) direcionam o processo de busca, a extração e a análise de dados.

Garousi et al. [93] sugerem que as questões sejam classificadas de forma explícita pelo seu tipo, pois isso ajuda a verificar se vários aspectos do tema que está sendo investigado estão sendo abordados. Dessa forma, as Questões de Pesquisa desta dissertação foram formuladas com base nos objetivos da pesquisa apresentados e classificadas de acordo com as categorias propostas por Easterbrook et al. [94]. O resultado pode ser visto no Quadro 3.1:

Identificador	Questão de Pesquisa	Tipo de Questão de Pesquisa
QP1	Quais são os principais métodos e abordagens utilizados para testar a usabilidade de soluções de login único?	Exploratória
QP2	Quais métricas de usabilidade podem ser usadas na avaliação da <i>Conta gov.br</i> pelo Senado Federal?	Exploratória

Quadro 3.1: Questões de Pesquisa da revisão de literatura. (Fonte: O Autor.)

### 3.1.3 Definição da *String* de Busca

A forma utilizada pelo Parsifal para estruturar a *String* de Busca é o uso da técnica proposta por Petticrew e Roberts [95], que consiste em definir termos que representem os seguintes aspectos: *Population*, *Intervention*, *Comparison*, *Outcome* e *Context* - PICOC. Ele então utiliza o conector **AND** entre os termos de aspectos diferentes, e o conector **OR** nos iguais. Segundo Picalho et al. [96], esses operadores lógicos têm a função de aumentar a abrangência ou precisão da pesquisa, seja obrigando que todos os termos constem nos documentos (operador **AND**), seja verificando se pelo menos um dos termos existe nos metadados dos estudos (operador **OR**). A definição de cada aspecto varia de acordo com o objetivo do estudo. O Quadro 3.2 ilustra o direcionamento escolhido para definição desses critérios.

Aspecto	Direcionamento na definição dos termos
<i>Population</i> (População)	Estudos que tratem sobre login, segurança e autenticação
<i>Intervention</i> (Intervenção)	Utilização de testes de usabilidade aplicados à população original dos estudos
<i>Comparison</i> (Comparação)	Comparação entre as técnicas encontradas
<i>Outcome</i> (Resultado)	Resultados dos testes, métricas ou indicadores de usabilidade aplicados a soluções de login único
<i>Context</i> (Contexto)	Aspecto não utilizado no estudo, já que a ideia é recuperar dados tanto da academia, quanto da indústria

Quadro 3.2: Orientação utilizada para os aspectos do PICOC. (Fonte: O Autor.)

Para testar se os termos escolhidos para cada aspecto estavam adequados, aproveitou-se a integração do Parsifal com a base de dados da Scopus (<https://www.scopus.com>). O fluxo seguido para identificar os termos foi:

1. Definição dos termos candidatos
2. Geração automática da *String* de Busca
3. Utilização da *String* de Busca gerada para fazer a pesquisa na Scopus
4. Análise dos resultados retornados

O objetivo desse processo foi encontrar uma quantidade relevante de estudos dentro da área de Ciência da Computação mas, ao mesmo tempo, que fosse passível de análise. Foi definida, então, uma faixa de resultados entre 50 e 150 estudos dentro da Scopus. O Quadro 3.3 apresenta os termos escolhidos para a primeira execução do referido roteiro:

<b>Critério</b>	<b>Valor</b>
<b><i>Population</i></b>	Segurança, Login, Login único, Autenticação centralizada, Gerenciamento de identidade, Provedor de identidade, Integração de login
<b><i>Intervention</i></b>	Usabilidade, Modos de teste de usabilidade, Técnicas de teste de usabilidade, Métodos de teste de usabilidade, Avaliação de usabilidade, Testes de usabilidade, Testes de usuário
<b><i>Comparison</i></b>	Comparação de técnicas, Técnicas de referência
<b><i>Outcome</i></b>	Impacto na usabilidade, Indicadores de usabilidade
<b><i>Search String</i></b>	(“Autenticação centralizada” OR “Gerenciamento de identidade” OR “Integração de login” OR “Login” OR “Login único” OR “Provedor de identidade” OR “Segurança”) AND (“Usabilidade”, “Avaliação de usabilidade” OR “Modos de teste de usabilidade” OR “Métodos de teste de usabilidade” OR “Testes de usabilidade” OR “Testes de usuário” OR “Técnicas de teste de usabilidade”) AND (“Comparação de técnicas” OR “Técnicas de referência”) AND (“Impacto na usabilidade” OR “Indicadores de usabilidade”)

Quadro 3.3: PICOC inicial utilizado para o estudo. (Fonte: O Autor.)

A execução da *String* de Busca não retornou registros, sugerindo que esses termos criaram um cenário específico demais. Sendo assim, uma adequação foi realizada, retirando termos e excluindo o aspecto *Comparison* dos critérios utilizados, uma vez que uma

revisão no objetivo da Revisão Sistemática nos fez perceber que o intuito era recuperar as técnicas utilizadas, e não uma comparação entre elas. O Quadro 3.4 mostra o resultado dessa adequação:

<b>Critério</b>	<b>Valor</b>
<b><i>Population</i></b>	Segurança, Login, Login único, Gerenciamento de identidade
<b><i>Intervention</i></b>	Usabilidade, Teste
<b><i>Outcome</i></b>	Indicadores, Técnicas
<b><i>Search String</i></b>	(“Gerenciamento de identidade” OR “Login” OR “Login único” OR “Segurança”) AND (“Teste” OR “Usabilidade”) AND (“Indicadores” OR “Técnicas”)

Quadro 3.4: Primeira adequação dos critérios PICOC, para expandir os resultados da *String* de Busca. (Fonte: O Autor.)

A pesquisa na base da Scopus com essa *String* retornou 74 registros. O aumento do número validou a suposição de que a primeira estava muito específica. Porém, ao analisar o conteúdo retornado, percebeu-se que muitos estudos não eram da área da Ciência da Computação, retornando alguns testes da área médica, por exemplo. Com isso, ao invés de usar o termo “Teste” isolado em *Intervention*, especificamos mais o critério, alterando para “Teste de usabilidade”. A *String* de Busca ficou assim: (**“Gerenciamento de identidade” OR “Login” OR “Login único” OR “Segurança”**) AND (“Teste de usabilidade” OR “Usabilidade”) AND (“Indicadores” OR “Técnicas”).

Tal modificação resultou em 11 artigos, com um foco bem mais aderente à área da pesquisa. Com esse resultado, optou-se por implementar outra estratégia fornecida pelo Parsifal para aumentar a abrangência de resultados: o uso de sinônimos. Dessa forma, para cada um dos termos definidos, foram acrescentadas palavras que pudessem expressar a mesma ideia ou conceito. Além disso, palavras em inglês foram adicionadas, uma vez que a maioria das publicações utiliza esse idioma. A lista dos sinônimos utilizados é apresentada no Quadro 3.5:

<b>Critério</b>	<b>Termo</b>	<b>Sinônimos</b>
<b><i>Population</i></b>	Gerenciamento de identidade	Controle de identidade Gestão de identidade <i>Identity control</i> <i>Identity governance</i> <i>Identity management</i>
	Login	Autenticação <i>Authentication</i>

<b>Critério</b>	<b>Termo</b>	<b>Sinônimos</b>
	Login único	Autenticação única SSO Single Access Single Sign-On Single Singon Single authentication
	Segurança	<i>Security</i>
<b><i>Intervention</i></b>	Teste de usabilidade	Avaliação de usabilidade <i>UX Test</i> <i>Usability Test</i> <i>Usability Testing</i> <i>Usability evaluation</i>
	Usabilidade	UX <i>Usability</i>
<b><i>Outcome</i></b>	Indicadores	Indicador <i>Metric</i> <i>Metrics</i> Métrica Métricas <i>Indicator</i> <i>Indicators</i>
	Técnicas	Methods Métodos Techniques

Quadro 3.5: Sinônimos utilizados para aumento da abrangência dos estudos. (Fonte: O Autor.)

Essa abordagem resultou na seguinte *String* de Busca:

(“Gerenciamento de identidade” OR “Controle de identidade” OR “Gestão de identidade” OR “Identity control” OR “Identity governance” OR “Identity management” OR “Login” OR “Autenticação” OR “Authentication” OR “Login único” OR “Autenticação única” OR “SSO” OR “Single Access” OR “Single Sign-On” OR “Single Singon” OR “Single authentication” OR “Segurança” OR “Security”) AND (“Teste de usabilidade” OR “Avaliação de usabilidade” OR “UX Test” OR “Usability Test” OR “Usability Testing” OR “Usability evaluation” OR “Usabilidade” OR “UX” OR “Usability”) AND

(“Indicadores” OR “Indicador” OR “Metric” OR “Metrics” OR “Métrica” OR “Métricas” OR “indicator” OR “indicators” OR “Técnicas” OR “Methods” OR “Métodos” OR “Techniques”) .

O resultado dessa busca foi o retorno de 33.246 estudos, de várias áreas do conhecimento. Isso indicou que algum dos termos usados estava extrapolando o escopo proposto pela revisão. Analisando alguns dos resumos obtidos, identificamos a existência de vários artigos que versavam sobre segurança pública e segurança de procedimentos médicos. Como o fator *Segurança* foi o ponto comum nessa observação, esse termo, juntamente com seus sinônimos, foi excluído do conjunto utilizado.

Essa modificação trouxe 9.681 resultados. A leitura de alguns itens sugeriam um foco em usabilidade, mas não em testes de usabilidade. Decidiu-se, então, utilizar apenas o termo *Teste de usabilidade* no critério Intervenção. O resultado disso foi o retorno de 1.574 registros, com um foco mais direcionado para Testes de Usabilidade aplicados no âmbito da Ciência da Computação. Como o número ainda estava muito alto para viabilizar a revisão, o termo *Login* foi retirado, em uma tentativa de restringir o escopo apenas aos estudos que abordavam Login Único.

Essa nova busca trouxe 200 registros. Para verificar se seria possível adequar o número de resultados ao intervalo definido anteriormente, o termo *Gerenciamento de Identidade*, que era o menos aderente ao objetivo da revisão, foi retirado, restando um total de 61 registros ao fazer uma nova pesquisa. Uma análise rápida dos resultados constatou o foco nos objetivos da pesquisa. Como último esforço de trazer mais resultados relevantes, o número de sinônimos foi ampliado para os termos que restaram, conforme mostrado no Quadro 3.6:

<b>Critério</b>	<b>Termo</b>	<b>Sinônimos</b>
<b><i>Population</i></b>	Login único	Acesso único Autenticação unificada Autenticação única Login Unificado SSO <i>Single Sign On</i> <i>Single SignOn</i> <i>Single access</i> <i>Single authentication</i> <i>Single sign-on</i> <i>Unified authentication</i> <i>Unified login</i>

<b>Critério</b>	<b>Termo</b>	<b>Sinônimos</b>
<b><i>Intervention</i></b>	Teste de usabilidade	Abordagens de teste de usabilidade Análise de usabilidade Avaliação de experiência do usuário Avaliação de usabilidade Ferramentas de teste de usabilidade Medição de usabilidade Métodos de teste de usabilidade Técnicas de avaliação de usabilidade <i>UX test</i> <i>Usability analysis</i> <i>Usability evaluation</i> <i>Usability evaluation techniques</i> <i>Usability measurement</i> <i>Usability test</i> <i>Usability testing approaches</i> <i>Usability testing methods</i> <i>Usability testing techniques</i> <i>Usability testing tools</i> <i>User experience evaluation</i>
<b><i>Outcome</i></b>	Técnicas	<i>Methods</i> Métodos <i>Techniques</i>
	Indicadores	Indicador <i>Indicator</i> <i>Indicators</i> <i>Metric</i> <i>Metrics</i> Métrica Métricas

Quadro 3.6: Lista de sinônimos final. (Fonte: O Autor)

Essa modificação retornou 70 registros na busca automática, o que consideramos um número adequado para a pesquisa. Dessa forma, a *String* de Busca final foi a seguinte: (“Login único” OR “Acesso único” OR “Autenticação unificada” OR “Autenticação única” OR “Login Unificado” OR “SSO” OR “Single Sign On” OR “Single SignOn” OR “Single access” OR “Single authentication” OR “Single

sign-on” OR “Unified authentication” OR “Unified login”) AND (“Teste de usabilidade” OR “Abordagens de teste de usabilidade” OR “Análise de usabilidade” OR “Avaliação de experiência do usuário” OR “Avaliação de usabilidade” OR “Ferramentas de teste de usabilidade” OR “Medição de usabilidade” OR “Métodos de teste de usabilidade” OR “Técnicas de avaliação de usabilidade” OR “UX test” OR “Usability analysis” OR “Usability evaluation” OR “Usability evaluation techniques” OR “Usability measurement” OR “Usability test” OR “Usability testing approaches” OR “Usability testing methods” OR “Usability testing techniques” OR “Usability testing tools” OR “User experience evaluation”) AND (“Indicadores” OR “Indicador” OR “Indicator” OR “Indicators” OR “Metric”.

### 3.1.4 Critérios de Seleção

Os critérios de exclusão e inclusão referentes a essa revisão sistemática serão tratados nessa seção. Os de exclusão, assim como sua justificativa, estão apresentados no Quadro 3.7:

<b>Id</b>	<b>Descrição</b>	<b>Justificativa</b>
CE1	Ano de publicação menor que 2013	Foi estabelecido o período de dez anos de estudos, para que a pesquisa fosse abrangente. Artigos anteriores a 2013, portanto, não serão considerados.
CE2	Não foi revisado por pares	Publicações que passaram por revisão de pares tendem a ter um rigor científico maior, fornecendo maior credibilidade.
CE3	A referência é uma coletânea e não um artigo	Ao fazer pesquisas de teste, identificamos que algumas bases retornam livros ou anais de eventos. Como o foco do estudo são artigos, esses resultados foram descartados.
CE4	Não é da área da Ciência da Computação	Estudos de outras áreas tendem a não agregar dados para a revisão em curso.
CE5	O estudo trata apenas de autenticação	A <i>String</i> de Busca pode trazer resultados que tratem apenas de um dos aspectos necessários à revisão.
CE6	O estudo trata apenas de usabilidade	Esses critérios visam retirar estudos incompletos.
CE7	O foco do artigo não engloba login e usabilidade	

<b>Id</b>	<b>Descrição</b>	<b>Justificativa</b>
CE8	Publicação não acessível pelo acesso CAFe	O Acesso Comunidade Acadêmica Federada (CAFe) é um serviço que permite o acesso a artigos de um conjunto de bases de pesquisa a um determinado grupo de instituições, da qual a UnB faz parte. Esse critério elimina qualquer estudo que não seja acessível de forma livre ou por esse convênio.
CE9	Publicação não está em inglês ou português	Apenas estudos nos idiomas que o pesquisador domina serão utilizados.
CE10	Tamanho do artigo menor que 6 páginas	Visa eliminar <i>short papers</i> , para que apenas pesquisas completas sejam consideradas.

Quadro 3.7: Critérios de exclusão - RSL de Usabilidade. (Fonte: O Autor)

Já o critério de inclusão definido foi apenas um: *CI1 - O estudo aborda testes de usabilidade e login*. Isso porque essa é a premissa básica para que o estudo tenha os dados necessários para responder às Questões de Pesquisa.

### 3.1.5 Bases de Pesquisa

As bases escolhidas para realização da busca de artigos foram as seguintes:

- ACM Digital Library - <http://portal.acm.org>
- IEEE Digital Library - <http://ieeexplore.ieee.org>
- Web of Science - <http://www.isiknowledge.com>
- Scopus - <http://www.scopus.com>
- Springer Link - <http://link.springer.com>

Essas bases foram definidas por conterem um número grande de estudos na área da Ciência da Computação. Importante registrar que, inicialmente, apenas as quatro primeiras haviam sido selecionadas. Porém, ao realizar testes com a *String* de Busca, constatou-se que a base do IEEE não retornou nenhum registro. O pesquisador foi orientado a incluir, então, a base da Springer, uma vez que essa base é responsável por publicar os artigos da conferência *HCI International* [97], referência na área de usabilidade. A estratégia foi positiva, uma vez que testes com a *String* de Busca retornaram centenas de resultados.

### 3.1.6 Estratégia de Pesquisa

A estratégia de pesquisa utilizada nessa revisão consiste em um processo com três fases, desenhado para refinar os artigos que foram recuperados das bases de pesquisa. Ele está representado na Figura 3.1.

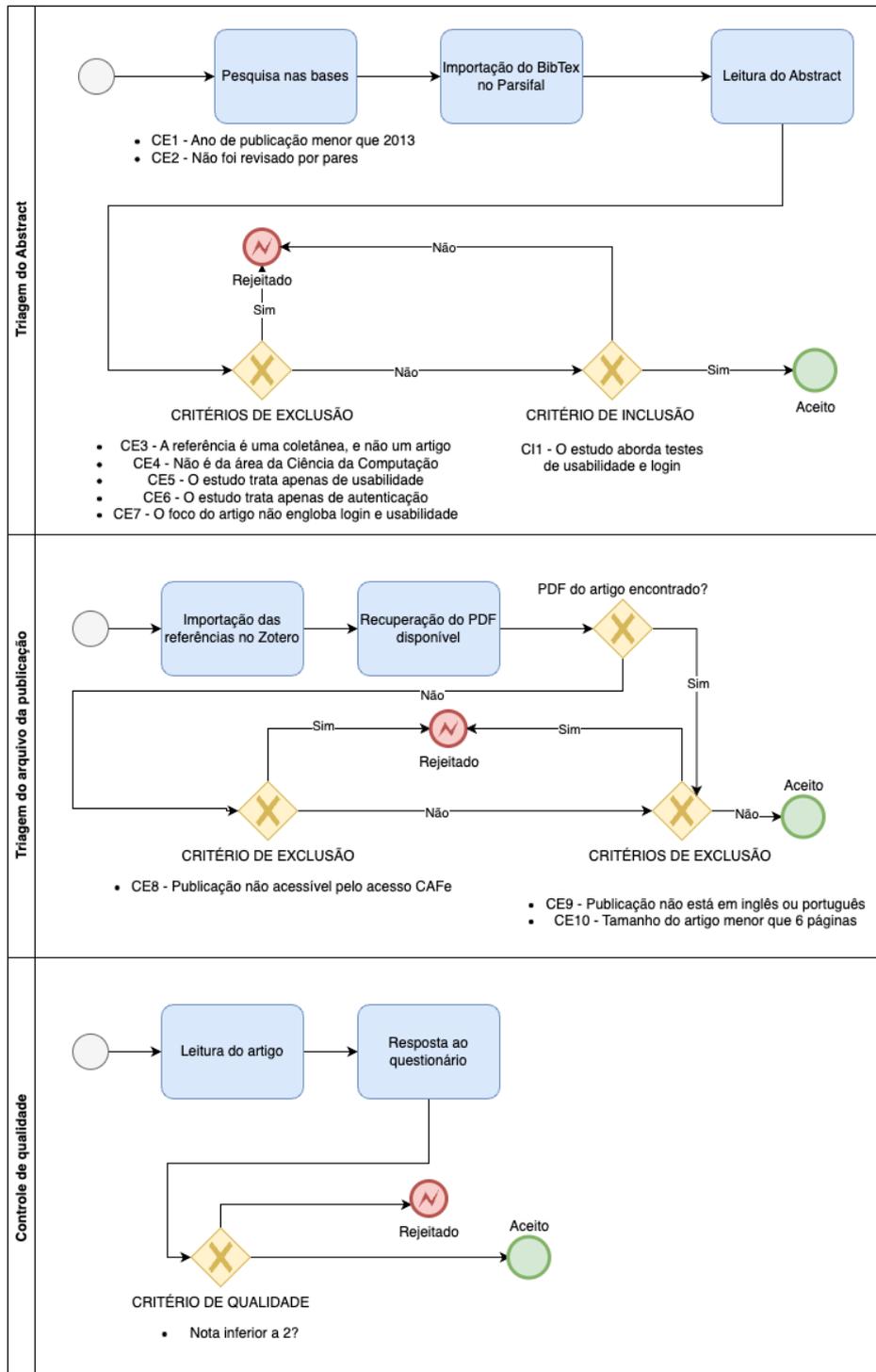


Figura 3.1: Processo de RSL - Técnicas e Métricas de Usabilidade. (Fonte: O Autor.)

Os detalhes de execução de cada uma das fases descritas, assim como o que ocorre em cada passo representado, serão abordados mais adiante, na Seção 3.2.

### 3.1.7 Mensuração da qualidade dos estudos e definição dos formulários de extração dos dados

O Parsifal utiliza a mensuração de qualidade com o objetivo de garantir a inclusão de estudos de alta qualidade, por meio de um processo estruturado e objetivo [98]. Essas diretrizes estão de acordo com o preconizado por Kitchenham et al.[92], e tornam o processo de extração de dados que responderão às Questões de Pesquisa mais fluido.

No caso do estudo em tela, foram elaboradas duas perguntas de aferição de qualidade:

1. *Como a técnica de teste de usabilidade é apresentada no artigo? (P1)* - Esse questionamento tem como objetivo verificar se o artigo possui a descrição de algum teste de usabilidade e o nível de detalhamento do mesmo, caso exista.
2. *Existe alguma métrica de usabilidade aplicada? (P2)* - O intuito dessa pergunta é aferir a utilização de métricas de usabilidade e descobrir um subconjunto que seja consolidado na literatura.

Para cada uma das perguntas, foi elaborado um conjunto de respostas e atribuída uma pontuação a cada uma delas. Essa pontuação busca medir o grau de detalhe e confiabilidade dos dados apresentados pelos estudos e está apresentada na Tabela 3.1:

Pergunta	Resposta	Pontuação
<b>P1</b>	1a - A técnica de testes é descrita e explicada, a metodologia de avaliação é clara e os resultados são bem definidos.	3
	1b - Há uma técnica de testes descrita no artigo, mas a aplicação no login não está clara. Os resultados são mensuráveis.	2
	1c - Teste de usabilidade é apresentado como um assunto secundário do artigo.	1
	1d - Não há uma técnica de teste de usabilidade no artigo.	0
<b>P2</b>	2a - Existe uma métrica conhecida e utilizada em outros estudos.	2
	2b - Há uma métrica no estudo, mas não há registros de utilização na literatura.	1
	2c - Nenhuma métrica de usabilidade é apresentada.	0

Tabela 3.1: Pontuação do *checklist* de qualidade. (Fonte: O Autor.)

Além do *score* de cada pergunta, também foi estabelecido um limite mínimo que cada estudo deveria atingir para ser utilizado na elaboração das respostas às Questões de Pesquisa. A fronteira de qualidade foi estabelecida em dois pontos, ou seja, estudos com um valor igual ou menor a esse valor não seriam considerados no estudo final. O raciocínio que levou a esse número é descrito a seguir, elencando as condições mínimas que deveriam ser alcançadas:

- A técnica de testes está muito bem descrita e pode servir de guia, mesmo que não tenha uma métrica utilizada (3 pontos em P1 + 0 pontos em P2).
- Existe uma técnica de teste de usabilidade descrita no artigo, mesmo que a aplicação não esteja clara, aliada a uma métrica qualquer (2 pontos em P1 + 1 ponto em P2).
- O estudo não tem o teste de usabilidade como foco principal, mas usa uma métrica estabelecida na literatura para medir essa propriedade (1 ponto em P1 + 2 pontos em P2).

Encerrando a fase de planejamento, um formulário simples de extração de dados foi criado contendo dois campos:

1. Técnicas de teste de usabilidade encontradas - campo de texto que permite registrar como foi o procedimento de teste executado em cada estudo.
2. Métricas de usabilidade encontradas - registro dos indicadores que foram citados no texto.

Nossa expectativa é que os dados mencionados contribuam para as respostas às Questões de Pesquisa do Quadro 3.1. A consolidação desse entendimento será a base para a definição do Protocolo de Teste de Usabilidade que planejamos aplicar em nosso estudo.

## 3.2 Condução

### 3.2.1 Triagem do *Abstract*

A primeira fase, intitulada **Triagem do *Abstract***, tem como objetivo identificar os estudos candidatos, populando o Parsifal com o resultado das buscas nas bases de dados de referências definidas na Seção 3.1.5, e aplicar os critérios de exclusão que são possíveis de avaliar com os metadados dos artigos recuperados.

O primeiro passo do fluxo é utilizar a *String* de Busca nas coletâneas selecionadas. Nesse momento, já é possível aplicar dois critérios de exclusão: o que se refere ao tempo de publicação (CE1) e o que trata da revisão por pares (CE2). O primeiro por conta

de uma característica comum da pesquisa provida por essas bases, que é a capacidade de filtrar os resultados tendo em conta a sua data de publicação, já retirando resultados que não atendam a esse critério. Nas bases da ACM e Web of Science, que permitem a inclusão de uma data específica, foi utilizado o período de 01/01/2013 a 31/07/2023. Já nas outras, que usam apenas o ano de publicação, foi inserido o intervalo entre 2013 e 2023. O segundo critério já é naturalmente atendido por conta desses repositórios só publicarem artigos que passaram por algum tipo de *peer review*.

O resultado dessas buscas foi exportado para o formato BibTex, um padrão utilizado para gerenciar referências de estudos [99], que é usado pelo Parsifal para criar sua base de dados. Esse formato tem os metadados dos artigos, assim como seu *abstract*, o que facilita a análise inicial e propicia a aplicação dos critérios de exclusão CE3 até CE7. Todos os estudos encontrados na pesquisa foram importados para o Parsifal, correspondendo ao segundo passo do fluxo do processo.

### Peculiaridades da base de dados Springer

Sobre esse passo, vale destacar algumas características da base Springer. A primeira é que o resultado de sua busca é dividida em vários tipos de conteúdo, conforme apresenta a Figura 3.2. Os itens que são do interesse da revisão sistemática são os do tipo *Conference Paper* e *Article*, pois representam o tipo de estudo que é buscado como fonte para responder às Questões de Pesquisa definidas para o presente trabalho.

#### Refine Your Search

Content Type	
Book	181
Conference Proceedings	115
Chapter	53
Conference Paper	27
Article	25
Reference Work	9

Figura 3.2: Tipos de conteúdo da base Springer Link. (Fonte: O Autor.)

O segundo ponto diz respeito ao formato como o resultado da pesquisa é exportado pela Springer. Ao selecionar a opção *Download search results*, a página monta um arquivo

do tipo *Comma-Separated Values* (CSV), um formato onde cada linha contém um registro e os valores são separados por vírgula [100]. Isso criou duas dificuldades para o processo:

1. O formato não é compatível com o Zotero e o Parsifal, inviabilizando a importação desses dados.
2. O CSV não traz consigo o *abstract*, o que tornaria o processo de análise dos *abstracts* bem penoso pois, para cada artigo do resultado, seria necessário acessar a página da Springer para verificar o conteúdo.

Entretanto, no processo de busca de uma solução para esses obstáculos, identificamos uma característica dos artigos que poderia ser útil: a Springer dispõe de uma API que recupera os dados bibliográficos de um determinado ativo através do seu *Digital Object Identifier* (DOI), um código que identifica de maneira unívoca um objeto digital [101]. Ao acessar a URL <https://citation-needed.springer.com/v2/references/<DOI>?format=refman&flavour=citation>, substituindo o parâmetro <DOI> pelo código do artigo desejado, um arquivo no formato *Research Information Systems*(RIS) [102] será disponibilizado como resposta. Esse formato é compatível com gerenciadores de referência como o Zotero e o Mendeley e inclui o resumo do artigo como um dos metadados.

Como um dos campos retornados no arquivo CSV da Springer é exatamente o DOI, a solução encontrada para o entrave foi a seguinte:

1. O arquivo CSV foi aberto utilizando o *Google Sheets*, solução fornecida pelo Google para manipulação de planilhas.
2. A coluna onde o DOI estava contido foi identificada (no nosso caso prático, era a coluna F).
3. Na linha 2, foi criada uma fórmula na última coluna disponível (coluna K), com o seguinte formato:

```
=concat(concat("https://citation-needed.springer.com/v2/
↪ references/";F2);"?format=refman&flavour=citation")
```

4. O conteúdo da célula K2 foi copiado e colado em todas as linhas, possibilitando que cada um dos registros tivesse uma célula contendo a URL para baixar o arquivo RIS.

Essa abordagem possibilitou a agregação de todas as URLs em um único documento, facilitando a recuperação dos recursos. Após esta etapa, foi possível clicar em cada um dos links para baixar o arquivo e adicioná-lo ao Zotero. Para otimizar o processo, utilizamos uma extensão do Google Chrome chamada *TabSave*, que permite fazer o *download*

de várias URLs ao mesmo tempo. Os arquivos foram salvos na máquina e importados para uma coleção do Zotero. Finalmente, essa coleção foi exportada no formato BibTex, viabilizando a importação no Parsifal.

Para concluir as observações sobre a base da Springer, é importante ressaltar que a integração do repositório com o acesso CAFE é bem instável. Por várias vezes, o sistema apresentou erro ao tentar recuperar artigos da base usando as credenciais da UnB. Dessa forma, caso essa pesquisa seja replicada em algum momento, é preciso atentar para esta dificuldade.

### Resultado da busca

Ao final da pesquisa nas bases, um total de 141 estudos foram recuperados, distribuídos de acordo com o gráfico da Figura 3.3:

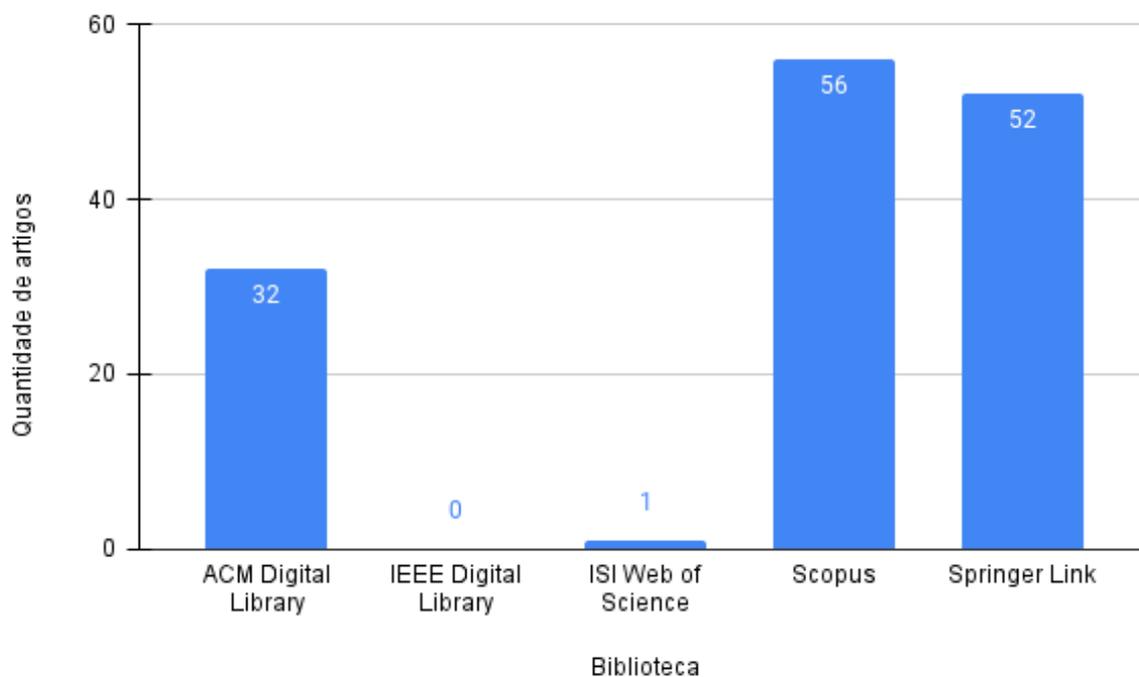


Figura 3.3: Distribuição de resultados por base de pesquisa. (Fonte: O Autor.)

### Leitura do *abstract* e aplicação dos critérios de exclusão e inclusão

Após a importação dos metadados no Parsifal, ele fornece uma interface onde é possível visualizar os detalhes de cada artigo e selecionar, para cada registro, o critério de exclusão ou inclusão definido com base na leitura do *abstract*.

Antes, porém, foi feita a pesquisa por artigos duplicados. O Parsifal tem uma funcionalidade que compara os resultados, indicando quais poderiam aparecer em mais de uma base de pesquisa. Do total de 141, nove possuíam essa característica.

Todos os resumos foram lidos e analisados pelo pesquisador, que procurou elementos que indicassem se, naquele estudo, havia sido aplicado um teste de usabilidade em alguma solução de login. A estatística final dessa inspeção está apresentada na Figura 3.4:

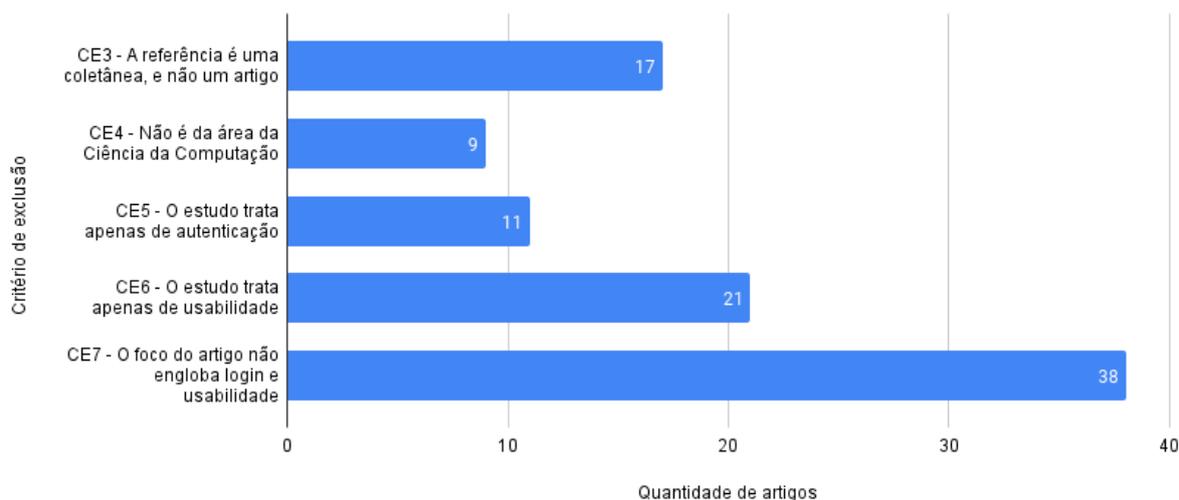


Figura 3.4: Estatística dos artigos excluídos X critério de exclusão. (Fonte: O Autor.)

Sobre o resultado, cabem alguns apontamentos. A quantidade de artigos que retornou na pesquisa cujo conteúdo principal não versava sobre usabilidade e login foi considerada alta (39,58% do total). Isso pode indicar que tópicos de segurança e usabilidade afetam os mais variados sistemas, sendo citados mesmo quando o objetivo do estudo não está nessas áreas.

Além disso, o número de coletâneas (*Conference Proceedings*) que foi apresentado pode indicar que estudos de usabilidade e login têm despertado o interesse da comunidade acadêmica. Essa percepção fica mais forte ao verificar que mais de 70% das conferências aconteceu nos anos de 2022 e 2023, sugerindo esse aumento de importância na discussão. A Figura 3.5 mostra essa estatística com mais clareza.

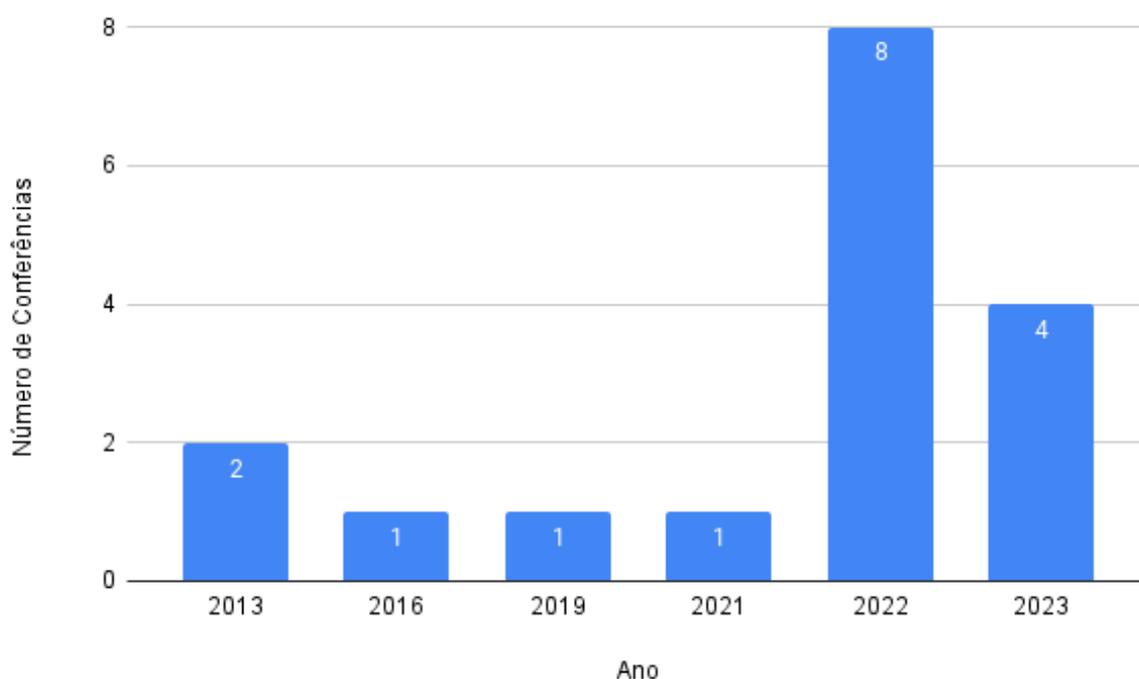


Figura 3.5: Conferências com estudos de usabilidade e login por ano. (Fonte: O Autor.)

Ao final dessa fase, 36 estudos atenderam ao critério de inclusão *CII - O estudo aborda testes de usabilidade e login*, e se tornaram elegíveis para a próxima fase, que será apresentada na seção seguinte.

### 3.2.2 Triagem do arquivo da publicação

Os 36 artigos que restaram na primeira fase foram importados para o Zotero, utilizando como entrada os arquivos gerados pelas bases de pesquisa e que haviam sido importados no Parsifal anteriormente. Com isso, a fase de **Triagem do arquivo da publicação** se iniciou.

O Zotero dispõe de uma funcionalidade que recupera o PDF de um registro, pesquisando se há algum documento de acesso livre que corresponda àquele estudo. Ao solicitarmos a pesquisa para a ferramenta, foram encontrados nove registros.

Essa abordagem, porém, não teve a economia de tempo desejada quando o processo foi definido. Ao verificar o conteúdo dos estudos, percebeu-se que quatro artigos estavam com a marcação “Versão aceita” ou “Versão submetida”. Alguns continham marcas d’água ou avisos de que aquela não era a versão publicada, e que poderia não conter os ajustes solicitados para que a publicação fosse efetivada.

Diante da incerteza sobre a atualização dos arquivos, optamos por verificar todos os estudos juntamente com os outros, fazendo o *download* diretamente das bases. Recomen-

damos, portanto, que essa funcionalidade do Zotero só seja utilizada após a verificação se o artigo não está disponível na biblioteca digital correspondente.

Do total de estudos qualificados, 27 puderam ter seu conteúdo recuperado pelo acesso das bases e nove estavam com acesso restrito, mesmo utilizando as credenciais de acesso da CAFe. Uma pesquisa na internet com cada um dos títulos que estavam faltando indicou que três deles estavam disponíveis em acesso livre em outro local (USENIX [103] e DiVA [104]). Os outros seis foram excluídos pelo critério de exclusão *CE8 - Publicação não acessível pelo acesso CAFe*, totalizando, portanto, 30 artigos para a próxima verificação.

Essa validação consistia em verificar os critérios de exclusão restantes: *CE9 - Publicação não está em inglês ou português* e *CE10 - Tamanho do artigo menor que 6 páginas*. Nenhum dos artigos foi eliminado pelo critério CE9 e, apenas dois, não tinham a quantidade mínima de páginas definida pelo critério CE10. Com isso, 28 artigos foram selecionados para a última fase do processo, em que a qualidade dos estudos era mensurada e os dados relevantes extraídos.

### 3.2.3 Controle de qualidade

Os estudos foram lidos e o *checklist* de qualidade definido na Seção 3.1.7 foi respondido para cada uma das pesquisas. Dos 28 artigos que restaram da fase anterior, 18 obtiveram a nota mínima estipulada no protocolo. O resultado compilado desses registros está apresentado no Quadro 3.8:

ID	Título	P1	P2	Total
E1 [25]	<i>Investigating Users' perspectives of web single sign-on: Conceptual gaps and acceptance model - Sun et al.</i>	3	2	5
E2 [105]	<i>Toward a secure and usable cloud-based password manager for web browsers - Zhao e Yue</i>	3	1	4
E3 [106]	<i>Faces in the Distorting Mirror: Revisiting Photo-Based Social Authentication - Polakis et al.</i>	3	1	4
E4 [107]	<i>On user authentication by means of video events recognition - Catuogno e Galdi</i>	3	1	4
E5 [78]	<i>Authentication Melee: A Usability Analysis of Seven Web Authentication Systems - Ruoti et al.</i>	3	2	5
E6 [108]	<i>On the Security and Usability of Segment-Based Visual Cryptographic Authentication Protocols - Wang et al.</i>	3	1	4

<b>ID</b>	<b>Título</b>	<b>P1</b>	<b>P2</b>	<b>Total</b>
E7 [109]	<i>Assessments of a cloud-based data wallet for personal identity management - Karegar et al.</i>	3	2	5
E8 [110]	<i>N-Auth: Mobile authentication done right - Peeters et al.</i>	3	2	5
E9 [111]	<i>I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication - Weidman e Grossklags</i>	3	2	5
E10 [23]	<i>SafeKeeper: Protecting Web Passwords Using Trusted Execution Environments - Krawiecka et al.</i>	3	2	5
E11 [112]	<i>Helping John to Make Informed Decisions on Using Social Login - Karegar et al.</i>	3	2	5
E12 [113]	<i>A Qualitative Study on Usability and Acceptability of Yubico Security Key - Das et al.</i>	2	1	3
E13 [114]	<i>An Empirical Usability Analysis of the Google Authentication API - Wijayarathna e Arachchilage</i>	3	0	3
E14 [115]	<i>Deploying authentication in the wild: Towards greater ecological validity in security usability studies - Aebischer et al.</i>	3	0	3
E15 [116]	<i>User perceptions of the usability and security of smartphones as FIDO2 roaming authenticators - Owens et al.</i>	3	2	5
E16 [117]	<i>An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control - Korir et al.</i>	3	2	5
E17 [118]	<i>WristAcoustic: Through-Wrist Acoustic Response Based Authentication for Smartwatches - Huh et al.</i>	3	2	5
E18 [79]	<i>Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations - Constantinides et al.</i>	3	2	5

Quadro 3.8: Pontuação dos estudos no controle de qualidade. (Fonte: O Autor.)

A Figura 3.6 traz um resumo visual de como cada critério influenciou na exclusão dos artigos buscados inicialmente:

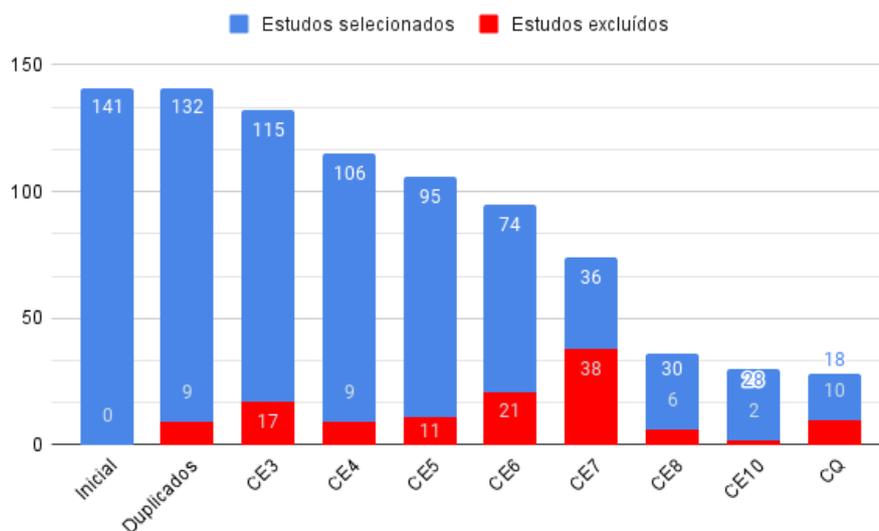


Figura 3.6: Evolução da triagem dos estudos da RSL. (Fonte: O Autor.)

O conteúdo dos artigos e a relação com as Questões de Pesquisa serão analisados na próxima seção.

### 3.2.4 Análise dos dados

Cada uma das pesquisas foi estudada para extrair dados que ajudassem a responder às duas Questões de Pesquisa elencadas no Quadro 3.1. A forma de apresentação desses resultados será feita conforme a Tabela 3.8, que está ordenada da pesquisa mais antiga para a mais recente. Aqui será exposto um breve sumário de como o artigo se conecta ao presente estudo e quais técnicas foram utilizadas, juntamente com as métricas oriundas da aplicação das mesmas. Essas informações servirão de base para a confecção do protocolo de testes que será utilizado no decorrer deste trabalho.

Iniciamos, então, por Sun et al. [25], Id E1. O estudo investiga os entraves na adoção de soluções de *Single Sign-On*, verificando que há uma relação entre o modelo mental que os usuários têm da arquitetura do SSO e as preocupações com exposição de dados e equívocos na utilização das soluções. Para aferir a usabilidade das opções de *Single Sign-On*, os pesquisadores fizeram um estudo exploratório, com questionários (demográficos e de escala Likert) e entrevistas semiestruturadas, além de observação dos participantes enquanto seguiam um roteiro de tarefas pré-definidas. Os participantes foram pagos para realizar a pesquisa, que foi revisada pelo Comitê de Ética da instituição, e cuja métrica resultante foi a Facilidade Percebida de Uso (*Perceived Ease of Use*).

O texto feito por Zhao e Yue [105], Id E2, se propõe a estudar os aspectos de segurança de gerenciadores de senha dos navegadores da Internet e informa que, apesar de ajudar

os usuários nas tarefas de utilizar senhas nas mais diversas páginas de internet, essas ferramentas possuem brechas de segurança. Para atacar alguns desses aspectos, eles propõem um modelo de armazenamento em nuvem, e realizam um teste de usabilidade no protótipo, a fim de verificar se essa abordagem traria ganhos na utilização pelos usuários.

Neste teste, um roteiro de tarefas foi enviado a cada um dos participantes, que tinham que comparar um navegador com o protótipo criado pelos pesquisadores com um navegador original. A interação com os sistemas era observada pelos pesquisadores, que coletavam os dados comparativos em um questionário com escala Likert que aferia qual das soluções era melhor, na opinião dos usuários, e qual era mais fácil de utilizar. A métrica veio da conversão direta da média das respostas a esse questionário, uma prática aceita e comumente usada, conforme mostrado por Chiasson et al. [119]. Nenhum participante foi pago para fazer a pesquisa, que foi revisada pelo Comitê de Ética da Universidade.

O artigo de Polakis et al. [106], Id E3, propõe um modelo de autenticação que visa resolver uma brecha na autenticação social feita pelo Facebook, que requeria que os usuários reconhecessem seus amigos em fotos propostas como desafio pela plataforma, mas que estava sendo burlada através de softwares de reconhecimento facial. A estratégia dos pesquisadores foi modificar as fotos utilizadas para confirmação a um ponto de inviabilizar o reconhecimento por máquina, ao mesmo tempo que permitia a identificação por parte de seres humanos. Um dos aspectos que foram medidos foi a usabilidade do sistema, aferida pelo percentual de acerto dos desafios, e pelo tempo médio de conclusão da tarefa. Essas informações foram coletadas pelo próprio uso do aplicativo, através de telemetria. Participantes foram recrutados e pagos, e a pesquisa foi revisada pelo Comitê de Ética.

A proposta de Catuogno e Galdi [107], Id E4, consistiu na criação de um protótipo para gerar desafios de duplo fator de autenticação por meio de vídeos curtos, em contraste com soluções que empregam imagens para essa finalidade. Isso se deve ao fato de que a abordagem com vídeos é menos suscetível a reconhecimento computacional do que a utilização de imagens. Para validar se o protótipo seria uma alternativa plausível, um pequeno estudo de usabilidade foi realizado. Os usuários foram convidados a utilizar o sistema de autenticação no máximo três vezes em um período que variou de uma a duas semanas, e preencheram um questionário de escala Likert que aferia as impressões de facilidade, tempo de acesso e aprovação geral da solução. O artigo não descreveu se houve submissão a um Comitê de Ética, e nem se houve incentivo para os participantes.

A pesquisa conduzida por Ruoti et al. [78], Id E5, comparou a usabilidade de três formas de autenticação, uma vez que considera que essa característica é importante na utilização de credenciais, mas ao mesmo tempo, identifica que há poucos estudos formais sobre o assunto. As formas pesquisadas foram: autenticação federada, *QR Code* e soluções

baseadas em e-mail. Após essa primeira parte, um quarto estudo foi realizado utilizando as três soluções para os participantes do estudo. O experimento consistia em acessar dois sites criados pelos pesquisadores: um fórum de perguntas e um bancário. A escolha dos dois assuntos foi feita por conta do diferente nível de atenção que as pessoas dão às credenciais em cada uma das situações. Após seguir um roteiro para a utilização das formas de autenticação, os participantes preencheram um questionário da *System Usability Scale* (SUS), métrica escolhida para permitir a comparação entre os resultados. Os voluntários receberam um voucher de 10 dólares como incentivo para a participação, e os estudos foram aprovados pelo *Internal Revision Board* (IRB) da faculdade.

Já Wang et al. [108], Id E6, analisaram a segurança de um tipo específico de autenticação, a criptografia visual, onde o servidor e o usuário compartilham uma chave na forma de uma imagem, que ao ser vista através de um cartão transparente específico, revela uma outra, que deve ser informada ao servidor a fim de completar o desafio e finalizar o processo de autenticação. A forma mais amigável desse processo utiliza dígitos representados por 7 segmentos, que fornecem um número resultante ao desafio proposto pelo servidor. Os pesquisadores fizeram um teste de usabilidade na solução, para verificar o impacto da segurança nesse quesito. Ele consistiu em recuperar, através de telemetria, dados que permitissem ver duas métricas: Precisão do Usuário (*User Accuracy*) e o Tempo Médio de Conclusão (*Average Completion Time*). Os participantes foram recrutados pelo serviço do *Amazon Mechanical Turk* [120], um serviço pago que permite a terceirização de tarefas, como a realização de uma pesquisa, para uma força de trabalho virtual. A pesquisa foi submetida para aprovação de um Comitê de Ética.

O trabalho de Karegar et al. [109], Id E7, consistiu na realização de testes de usuário em uma carteira digital provida pelo projeto CREDENTIAL [121], uma solução de armazenamento de identidade em nuvem que foi financiado pela União Europeia. Esses testes abrangeram funcionalidades como autorização e autenticação, revelando preferências, dúvidas e dificuldades de compreensão na aplicação da ferramenta, aspectos que aproximam o estudo da nossa revisão sistemática. Um roteiro foi disponibilizado para os participantes, que após isso preenchiam um formulário de escala Likert que gerava uma pontuação da *System Usability Scale* (SUS). Além dessa métrica, também foram aferidos o Tempo de Conclusão da Tarefa e a Duração total. Não foram encontrados detalhes sobre a revisão por algum comitê de ética ou pagamento dos participantes.

Peeters et al. [110], Id E8, especificaram uma solução de autenticação mobile, a n-Auth, que se propôs a sanar os problemas oriundos da utilização de senhas como credenciais, uma vez que usa a habilidade dos celulares em ler um *QR Code* para fazer a autenticação. Um estudo de usabilidade foi realizado para verificar se a utilização seria amigável, uma vez que princípios de *Human-Computer Interaction* (HCI) foram utilizados

no desenvolvimento do seu projeto. Os participantes logaram em um site disponibilizado pelos pesquisadores ao longo de duas semanas, e ao terminar a interação, um conjunto de perguntas em escala Likert era disponibilizado. A intenção foi mensurar a Facilidade de Adoção, a Facilidade Percebida e o Tempo de Conclusão, comparando a solução do n-Auth com o uso de senhas. Os participantes foram pagos para realizar os testes de usuários, e não foi mencionado se a pesquisa teve uma revisão por parte de um Comitê.

A análise feita por Weidman e Grossklags [111], Id E9, procurou entender as consequências da troca de um sistema de autenticação baseado em *token*, implementado em uma instituição acadêmica, para uma autenticação de duplo fator que utiliza os próprios celulares dos empregados para verificar o acesso aos ativos digitais da organização. Para isso, uma pesquisa de benefícios e usabilidade foi realizada no processo de login do novo modelo de segurança, buscando identificar o que era melhor aceito e o que encontrava resistência entre os servidores. A estratégia foi fazer um questionário usando escala Likert para saber se o novo sistema de autenticação era mais seguro para a organização, se o novo mecanismo era facilmente entendido, ou se era inconveniente. A confiabilidade das respostas foi aferida com o Alfa de Cronbach. O pagamento de incentivos para os participantes foi vetado, e um comitê de revisão aprovou as práticas executadas.

No estudo realizado por Krawiecka et al. [23], Id E10, os autores propõem uma solução de armazenamento de senhas chamada *SafeKeeper*, que tenta endereçar problemas como ataques de *phishing* e acessos de servidores corrompidos, conservando a facilidade de implantação e integração com plataformas existentes, como o WordPress. Ao mesmo tempo que protege as informações armazenadas no servidor, um complemento de *browser* informa ao usuário final se o servidor que está sendo acessado é confiável. Como parte do estudo, uma pesquisa de usabilidade foi feita para atestar a facilidade dos usuários em usar a solução para identificar se é seguro informar as senhas em um determinado site.

O procedimento de teste foi complexo. Um grupo de pessoas foi recrutado para acessar um conjunto de sites que estava hospedado em um servidor dedicado da universidade. Para elas foi apresentada a forma de atuação do *SafeKeeper*, e para cada site, os participantes tinham que responder se o site era protegido, indicando o grau de certeza da resposta. Dois meses após esse procedimento, 20 participantes desse grupo foram convocados a refazer o teste, mas sem nenhuma instrução. Tal processo foi feito para averiguar se eles se lembravam de como usar a ferramenta. Um terceiro grupo, que nunca teve nenhuma instrução sobre o funcionamento do *SafeKeeper*, foi recrutado e fez o roteiro de testes, de forma que fosse possível fazer uma comparação entre os usuários treinados e os que nunca tinham usado a solução. Um questionário que media o grau de facilidade em quatro níveis foi preenchido, permitindo que se aferisse a Facilidade Percebida de Uso. Outra métrica que foi extraída foi a Efetividade, com base nas respostas sobre a proteção fornecida para

um determinado site. Não houve informação de pagamento de participantes, e nem se houve revisão formal do procedimento por um Comitê.

O autor Farzaneh Karegar, que já foi citado nessa lista anteriormente, se juntou a outro grupo de pesquisadores em 2018 [112], Id E11, para abordar o paradoxo existente entre a privacidade e a facilidade fornecida por soluções de *Single Sign-On* providas por redes sociais como Facebook e Google, uma vez que para manter a primeira o ideal é não utilizar esse artifício, porém isso resulta em um sacrifício na usabilidade e funcionalidade. Por conta desse cenário, os autores se propuseram a verificar como apresentar informações mais apuradas do modo como os dados pessoais são utilizados, de maneiras que fosse possível ao usuário fazer uma escolha mais consciente do quanto sua privacidade será comprometida ao utilizar um Provedor de Identidade. Um estudo de usabilidade foi feito para identificar o impacto dessa mudança.

O experimento consistiu em identificar problemas de usabilidade existentes na plataforma de *Single Sign-On* do Facebook, utilizando uma revisão da literatura que listou os pontos de maior atrito, além da técnica do Percurso Cognitivo (*Cognitive Walkthrough*). Esses problemas se tornaram requisitos para a solução proposta, que foi avaliada em um teste de usuários cujos participantes preencheram questionários de perguntas abertas e de múltipla escolha, além de perguntas sobre as preocupações com a privacidade, usando o *Internet Users' Information Privacy Concerns* (IUIPC) [122]. As métricas de usabilidade aferidas foram o SUS e o Tempo de Conclusão da Tarefa. Os participantes foram pagos para realizar a pesquisa, que seguiu os procedimentos éticos do Conselho de Pesquisa Sueca.

O artigo de Das et al. [113], Id E12, se propôs a analisar a usabilidade de um mecanismo de autenticação de dois fatores, catalogando os pontos que pudessem atrapalhar a utilização do dispositivo e fornecendo esse *feedback* ao fabricante. Após a implementação das sugestões, foram percebidas mudanças significativas em termos de usabilidade, que foi testada através de questionários, entrevistas e seções de *Think Aloud Protocol*. Essas ferramentas permitiram aos pesquisadores definir quatro métricas: *Stop points*, pontos onde os usuários não sabiam o que fazer ou pensavam que tinham completado a tarefa; *Halt points*, onde eles paravam e não continuavam; *Confusion points*, onde houve parada, mas não foi necessária ajuda para prosseguir; e *Value points*, comentários onde os participantes expressaram sua própria visão e opinião a respeito do produto, e o que poderia ser feito para melhorá-lo. O procedimento foi validado com protocolos de um Comitê de Revisão, e não ficou claro se os participantes receberam algum tipo de incentivo para participar da pesquisa.

O texto de Wijayarathna e Arachchilage [114], Id E13, investigou questões de usabilidade no uso da API do Google para autenticação, buscando definir a razão dos de-

envolvedores cometerem erros em seu uso. Ainda que o cenário seja diferente de um usuário tentando fazer login, o estudo trouxe valor por reforçar a percepção de como o *Think Aloud Protocol* pode ser usado para diagnosticar problemas de usabilidade. Aliado ao Questionário de Dimensões Cognitivas [75], conseguiu identificar os eventos em que os usuários mostraram surpresa ou tiveram que fazer uma escolha difícil, as mudanças de contexto, dificuldades e problemas de entendimento. Os recrutados ganharam um voucher de 15 dólares para participar da pesquisa, e o estudo passou por uma avaliação do Comitê de Ética de Pesquisa Humana da universidade.

No trabalho desenvolvido por Aebischer et al. [115], Id E14, os pesquisadores apresentaram uma alternativa ao uso de senhas para autenticação em sistemas web, através da ferramenta Pico, que realiza o login através de *QR Codes*. Um dos pontos abordados foi a usabilidade desse sistema em aspectos como o esforço cognitivo para usar a solução e a facilidade percebida de uso. Para levantar essas métricas, os participantes usaram a solução por duas semanas, e responderam questionários com escala Likert que avaliavam o grau de dificuldade do uso da ferramenta, e entrevistas semiestruturadas que coletavam dados sobre a cognição. Os participantes receberam um voucher de 10 GBP para cooperarem com a pesquisa, e os procedimentos passaram por avaliação de um Comitê de Ética.

Um ano depois, em 2021, Owens et al. [116], Id E15, analisaram o padrão FIDO2, uma especificação feita pela *FIDO Alliance (Fast IDentity Online Alliance)* [123]. Essa organização sem fins lucrativos visa reduzir a dependência global de senhas para autenticação online fomentando soluções de protocolos mais seguros, e no caso do FIDO2, é utilizado um método de autenticação sem senha, através de um dispositivo autenticador que gera um par de chaves para efetuar o login. Os pesquisadores realizaram um estudo sobre a usabilidade de um sistema que utilizou um *smartphone* como um autenticador itinerante (*roaming authenticator*) do padrão FIDO2, comparando esses dados com a usabilidade de uso das senhas.

A dinâmica do experimento foi a seguinte: foram montados dois grupos de usuários, divididos em quem usava senhas e quem utilizava a solução FIDO. Eles receberam um roteiro de tarefas para serem feitas em dez dias, e preencheram um questionário SUS no início e no final da experiência. Com esse processo foi possível aferir a pontuação SUS, a Facilidade Percebida e o Tempo Médio de Conclusão de cada uma das soluções. Os participantes foram recrutados pelo Amazon MTurk, ou seja, foram pagos para fazer parte do estudo, e mesmo sem ter um conselho de ética formal, o estudo passou por uma revisão interna dos seus procedimentos a fim de assegurar a privacidade dos voluntários.

A publicação de Korir et al. [117], Id E16, narra a criação do protótipo de um aplicativo de carteira digital que concentrava informações de identidade descentralizada (*decentralized*

id) dos usuários. O objetivo era estudar as percepções dos usuários sobre essa abordagem, verificando aspectos de segurança, privacidade e usabilidade. Os participantes recebiam um roteiro para usar com a solução, e os aspectos de usabilidade eram testados através de entrevistas semiestruturadas, *Think Aloud Protocol*, Investigação Contextual (*Contextual Inquiry*) e o questionário SUS. As métricas recuperadas através do procedimento foram os incidentes de usabilidade elencados por Nielsen e a pontuação no *System Usability Scale*. Houve incentivo financeiro para a participação na pesquisa, e apesar de não haver referência de um Comitê de Ética formal, o artigo menciona que regras éticas de pesquisa foram aplicadas, já que eles seguiram os preceitos do Relatório Menlo [124], um trabalho que propôs um quadro de diretrizes éticas para pesquisa em segurança da informação e computação.

A pesquisa de Huh et al. [118], Id E17, descreve um novo sistema de desbloqueio para *smartwatches* que usa o som e a pose da mão para identificar o usuário, uma vez que a utilização de PINs e padrões de desenho não são muito eficientes em telas pequenas de relógio. Como solicitar que usuários façam de forma consistente múltiplas poses de mão durante a autenticação pode criar desafios de usabilidade, testes de usuário foram realizados para verificar essa característica. Testes de esforço cognitivo e físico foram aplicados, e questionários da SUS respondidos a fim de definir a pontuação na escala. Os participantes foram pagos, e não houve menção se houve alguma consulta a um Comitê de Ética.

Finalizando o conjunto de artigos estudados, Constantinides et al. [79], Id E18, apresentaram uma nova solução de autenticação, o *Duo Pass*. Ele é um sistema que combina elementos visuais e textuais para criar senhas únicas e significativas, baseadas nas experiências pessoais dos usuários no ambiente hospitalar. O intuito é tornar as senhas mais fáceis de lembrar para os usuários, ao mesmo tempo em que mantém um alto nível de segurança. Para validar a proposta, testes de segurança percebida, confiabilidade e usabilidade foram executados na solução. Foi criado um roteiro para que os participantes utilizassem o login em diversos contextos, e, em termos de usabilidade, foram aplicados questionários SUS para obter a pontuação da proposta. Um grupo, o experimental, utilizou a nova proposta, enquanto um outro, de controle, continuou usando o modo atual de login. Todos os participantes foram voluntários, e não houve, no texto, algo que indicasse que um Comitê de Ética tivesse sido consultado para revisar a pesquisa.

O Quadro 3.9 contém uma compilação de todos os resultados encontrados, para sintetizar as respostas às Questões de Pesquisa formuladas:

<b>ID</b>	<b>Técnicas de Teste de usabilidade (QP1)</b>	<b>Métricas de usabilidade (QP2)</b>
E1	Questionário de Escala Likert Entrevista semiestruturada Observação pelos pesquisadores Roteiro Participação paga Diretrizes éticas por Regulamento ou Comitê	Facilidade Percebida no Uso
E2	Questionário de Escala Likert Roteiro Comparação entre duas soluções Participação voluntária Diretrizes éticas por Regulamento ou Comitê	Conversão direta da pontuação da Escala Likert
E3	Telemetria Roteiro Participação paga Diretrizes éticas por Regulamento ou Comitê de Ética	Percentual de Acertos Tempo de Conclusão da Tarefa
E4	Questionário de Escala Likert Uso da solução após treinamento	Facilidade Percebida no Uso Tempo de Acesso Aprovação da solução
E5	Questionário SUS Roteiro Participação paga Diretrizes éticas por Regulamento ou Comitê	Pontuação SUS
E6	Telemetria Uso da solução após treinamento	Precisão do Usuário Tempo de Conclusão da Tarefa
E7	Questionário SUS Roteiro	Pontuação SUS Tempo de Conclusão da Tarefa Duração Total
E8	Questionário de Escala Likert Roteiro Participação paga Diretrizes éticas por Regulamento ou Comitê	Facilidade de Adoção Facilidade Percebida no Uso Tempo de Conclusão da Tarefa

*Continua na próxima página*

Quadro 3.9 – Continuação da página anterior

ID	Técnicas de Teste de usabilidade (QP1)	Métricas de usabilidade (QP2)
E9	Questionário de Escala Likert Comparação entre dois sistemas Validação com o Alfa de Cronbach Participação voluntária Diretrizes éticas por Regulamento ou Comitê	Percepção de qual era o mais seguro Facilidade Percebida no Uso Solução mais conveniente
E10	Questionário com quatro graus de dificuldade para escolha Perguntas sobre a efetividade da solução Grupo instruído para fazer a atividade Grupo de controle sem instrução para fazer a atividade	Facilidade Percebida no Uso Efetividade
E11	<i>Cognitive Walkthrough</i> Questionários de perguntas abertas e de múltipla escolha Questionário SUS <i>Internet Users' Information Privacy Concerns (IUIPC)</i> Roteiro Participação paga Diretrizes éticas por Regulamento ou Comitê	Pontuação SUS Tempo de Conclusão da Tarefa
E12	<i>Think Aloud Protocol</i> Questionários Entrevistas Diretrizes éticas por Regulamento ou Comitê	<i>Stop points</i> <i>Halt points</i> <i>Confusion points</i>
E13	<i>Think Aloud Protocol</i> Questionário de Dimensões Cognitivas Participação paga Diretrizes éticas por Regulamento ou Comitê	Pontos de escolha difícil Mudanças de contexto Dificuldades e mudanças de contexto
E14	Questionário de Escala Likert Entrevista semiestruturada Participação paga Diretrizes éticas por Regulamento ou Comitê	Esforço cognitivo Facilidade Percebida no Uso

*Continua na próxima página*

Quadro 3.9 – Continuação da página anterior

ID	Técnicas de Teste de usabilidade (QP1)	Métricas de usabilidade (QP2)
E15	Questionário de Escala Likert Questionário SUS Roteiro Comparação entre dois sistemas Participação paga Diretrizes éticas por Regulamento ou Comitê	Facilidade Percebida no Uso Pontuação SUS Tempo de Conclusão da Tarefa
E16	<i>Think Aloud Protocol</i> Entrevista semiestruturada Roteiro <i>Contextual Inquiry</i> Questionário SUS Participação paga Diretrizes éticas por Regulamento ou Comitê	Incidentes de usabilidade de Nielsen Pontuação SUS
E17	Testes de esforço cognitivo Questionário SUS Participação paga	Pontuação SUS
E18	Roteiro Questionário SUS Comparação entre dois sistemas Participação voluntária	Pontuação SUS Confiabilidade

Quadro 3.9: Resumo de Técnicas e Métricas encontradas nos estudos. (Fonte: O Autor.)

É possível agrupar as técnicas que foram utilizadas e contar a frequência de uso de cada uma delas. A Figura 3.7 mostra uma representação desse total:

Frequência de uso das técnicas

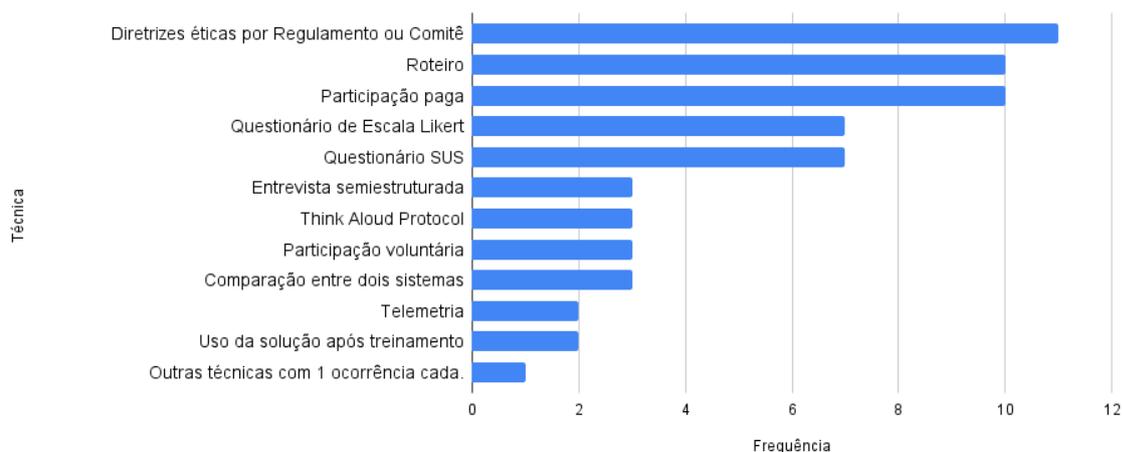


Figura 3.7: Frequência de uso das técnicas de teste de usabilidade. (Fonte: O Autor.)

Uma análise semelhante é feita com as métricas obtidas nos estudos, conforme mostra a Figura 3.8:

Frequência de métricas obtidas

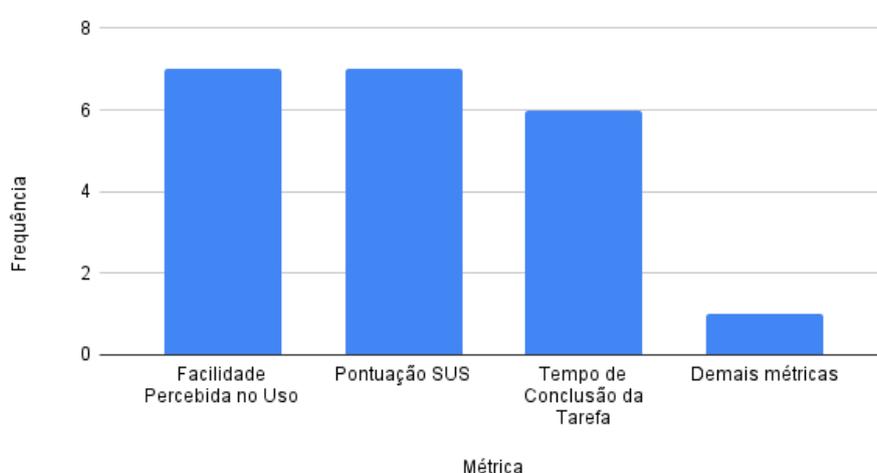


Figura 3.8: Frequência de métricas obtidas pela Revisão Sistemática de Literatura. (Fonte: O Autor.)

Com base nesses dados, é possível inferir que:

- Nortear o estudo com diretrizes éticas pode ser uma boa prática, uma vez que 61% dos estudos realizados se valeu desse artifício.
- O uso de um roteiro para execução dos testes pelos participantes é indicado.

- Incentivar os participantes através de pagamentos é uma opção legítima, caso se tenha dificuldades em conseguir um número significativo de voluntários.
- O meio mais utilizado para executar testes de usabilidade na nossa amostra é a Escala Likert, uma vez que o Questionário SUS também é baseado na mesma escala.
- As características mais procuradas pelos pesquisadores no que diz respeito à usabilidade de uma solução de login único são a Facilidade Percebida no Uso e o Tempo de Conclusão.
- O uso da Pontuação SUS é uma métrica comum em estudos desse tipo.

Por fim, há uma característica que permeou a totalidade dos estudos: a aplicação de um questionário demográfico. As informações coletadas variaram entre eles, mas questões comuns entre os mesmos foram relacionadas à idade, grau de instrução e nível de entendimento de tecnologia.

### 3.3 Síntese do Capítulo

Detalhamos, neste capítulo, uma Revisão Sistemática de Literatura (RSL) com foco em testes de usabilidade para soluções de login único. Apresentamos os princípios teóricos que norteiam as fases principais que compõem um trabalho desse tipo: Planejamento, Condução e Relato.

Descrevemos as características e resultados esperados de cada uma delas, e então a execução do procedimento foi iniciada. Especificamos os dados do Planejamento referentes à RSL de usabilidade em soluções de login único, com a definição das Questões de Pesquisa, do protocolo que seria seguido, dos critérios de exclusão e inclusão e dos parâmetros de qualidade dos estudos.

A fase de Condução foi marcada por situações inusitadas que não estavam previstas no Planejamento, como a dificuldade de lidar com metadados da base Springer e o fracasso na utilização da descoberta automática de arquivos dos estudos pela ferramenta Zotero. Felizmente isso não comprometeu o estudo, que ao final, conseguiu uma massa de 18 pesquisas, de um total inicial de 141, que passaram em todos os critérios.

Todos os estudos analisados mostraram ter uma descrição rica da metodologia utilizada, o que permitiu a captura das informações mais relevantes para responder às Questões de Pesquisa formuladas. Descobrimos que os métodos mais utilizados para estudos desse tipo envolvem a criação de um roteiro de atividades para os participantes, o balizamento por diretrizes éticas formais, utilização de questionários de Escala Likert para aferir a experiência dos usuários e o pagamento de honorários quando necessário.

Em relação às métricas aferidas, as mais frequentes foram a Facilidade Percebida no Uso, o Tempo de Conclusão da tarefa e a pontuação do *System Usability Scale*. Esperamos que a utilização desse conjunto permita capturar os aspectos mais importantes para os usuários quando utilizam uma solução de *Single Sign-On*.

Essas informações servirão de base para a montagem do protocolo de teste da próxima seção. Nela, usaremos essas diretrizes, juntamente com a realidade de implantação da solução da **Conta gov.br** no e-Cidadania, para propor um protocolo de testes que será conduzido a fim de nos fornecer os dados necessários para a consecução dos objetivos dessa pesquisa.

# Capítulo 4

## Metodologia proposta

Nesta seção, reuniremos as informações coletadas através do embasamento teórico e dos estudos da Revisão Sistemática da Literatura para delinear o Protocolo de Testes de Usabilidade da *Conta gov.br*. Além disso, também descreveremos como um teste-piloto será realizado com base nesse protocolo, de forma que a aplicação do teste de usuário possa ser ampliada posteriormente.

### 4.1 Protocolo de Teste de Usabilidade

Tomando por base os princípios enumerados por Bastien[65], que foram apresentados na Seção 2.3.4, vamos apresentar os direcionamentos que nortearão cada um dos itens elencados por ele.

#### Definição dos objetivos do teste

O teste de usabilidade da integração da *Conta gov.br* no sistema e-Cidadania do Senado Federal tem como objetivos principais:

- Identificar a usabilidade geral e a facilidade percebida do uso do login padrão (com e-mail e senha) do sistema e-Cidadania.
- Identificar a usabilidade geral e a facilidade percebida do uso da *Conta gov.br*.
- Comparar os dois resultados para verificar os ganhos e as perdas da integração com a *Conta gov.br*.

#### Qualificação e recrutamento dos participantes

Seguindo os preceitos de Tullis e Albert [66], a meta de um bom recrutamento seria formular critérios de participação que refletissem o público-alvo do e-Cidadania. Como é

um sistema que já está em produção há 12 anos, o intuito seria levantar as estatísticas dos usuários cadastrados para embasar o teste. Infelizmente, o e-Cidadania não tem dados de gênero, instrução e nem faixa etária, uma vez que o cadastro só exige o nome, e-mail, unidade federativa de residência e idade mínima de 12 anos de idade[125].

Sendo assim, para ter o mínimo de balizamento, utilizaremos os seguintes critérios:

- Proporção por gênero: acompanharemos os dados do Censo Demográfico de 2022 [126] para a definição desse número. Como o Censo faz a estratificação por faixas etárias e a idade de 12 anos está dentro da faixa de 10 a 14 anos, utilizaremos a próxima faixa (15 anos) como idade de corte para fins de cálculo.
- Proporção por idade: utilizaremos a mesma fonte de dados, dividindo em quatro faixas - 15 a 29 anos, 30 a 44 anos, 45 a 59 anos, acima de 60 anos.
- Uso anterior da **Conta gov.br**: buscaremos amostras que tenham tanto pessoas que já tenham usado a **Conta gov.br** anteriormente, quanto usuários que nunca tenham usado a solução.

Sendo assim, deverá ser feita uma pesquisa prévia, com o objetivo de recrutar os participantes, onde seja possível identificar os dados acima para montagem da amostra, além do nível de instrução e do grau de familiaridade com tecnologia. Essas duas últimas informações são oriundas dos achados da Revisão Sistemática e consideramos prudente incluí-las também.

Outro fruto da RSL é a validação da importância de seguir diretrizes éticas em estudos de usabilidade com usuários. Para satisfazer esse requisito, seguiremos a instrução de Hass [67]: explicitar os itens que afetam os participantes em um Formulário de Consentimento.

Finalmente, para resguardar a privacidade dos respondentes, adotaremos uma prática executada por Karegar et al. [112] em sua avaliação de usabilidade: a utilização de uma *persona*. Isso quer dizer que proveremos para os participantes as credenciais que devem ser usadas no momento dos testes, de maneira que não será necessário utilizar suas próprias credenciais. Essa decisão foi tomada porque a **Conta gov.br** usa o CPF como login, e isso já expõe um dado pessoal sensível dos participantes.

O meio de recrutamento que será usado é a distribuição da pesquisa pelas redes sociais, como o Whatsapp. O envio de e-mails para as pessoas que já integram a base de dados do e-Cidadania está sendo estudado, e caso seja feito, deve ser realizado pelo DataSenado[127], órgão de pesquisas institucional do Senado Federal.

O número pretendido de participantes será definido com base nos critérios elencados por Albert e Tullis [69], que foram vistos na Seção 2.3.4. No caso da avaliação de usabilidade desta pesquisa, temos características dos dois cenários descritos: ao mesmo tempo

que o escopo do design a ser testado é limitado e não existe a necessidade de capturar todos os problemas de usabilidade (aspectos de um cenário de menor risco - 5 a 10 participantes), desejamos fazer uma comparação estatística, e supomos que os usuários sejam particularmente diversos (aspectos de cenários críticos - 10 a 25 participantes).

Diante dessa realidade, definiremos o número mínimo de participantes como **10**, por ser o número comum entre os dois intervalos apresentados. Já a meta de participantes pretendida será **18**, calculado como o número central do intervalo do cenário crítico. Importante frisar que essa quantia é um ponto de partida, e pode ser ampliada caso não se consiga validar a integridade das respostas por meios estatísticos.

Concluindo, não está previsto o pagamento de honorários aos participantes, uma vez que não há nenhum patrocínio para essa pesquisa. Contudo, caso não se consiga uma amostra significativa, essa possibilidade passa a ser uma opção, com o intuito de viabilizar a pesquisa.

### **Seleção das tarefas e descrição dos cenários**

Fundamentados nos objetivos do teste que mencionamos na Seção 4.1, definimos que as seguintes tarefas devem ser executadas na avaliação:

- Testar o login com a *Conta gov.br*:
  - Clicar no botão **Entrar com gov.br**.
  - Informar o CPF da *persona* fornecida.
  - Informar a senha da *persona*.
  - Avaliar a usabilidade e facilidade de uso desse modo de autenticação.
- Testar o login com usuário e senha:
  - Informar o e-mail da *persona* fornecida.
  - Informar a senha da *persona*.
  - Avaliar a usabilidade e facilidade de uso desse modo de autenticação.

Uma proposta de cenário será apresentada na Seção 4.2, no contexto do estudo-piloto.

### **Escolha do que será medido e registro dos dados**

Com base nos achados da Revisão Sistemática de Literatura realizada e, em consonância com os objetivos do teste determinados anteriormente, foi definido um conjunto de métricas. Elas estão discriminadas abaixo, juntamente com a forma como serão captadas:

- Tempo de Conclusão: será calculado com base na duração aferida durante a execução do teste, que será gravado. Corresponde ao tempo que os participantes levaram para completar cada um dos tipos de login.
- Facilidade Percebida no Uso: aferida por uma pergunta utilizando o *Single Ease Question*, abordada na Seção 2.4.3. Porém, ao invés de utilizar cinco níveis para a resposta, como mostrado na proposta original de Tedesco e Tullis [91], utilizaremos a escala contínua de sete pontos, seguindo orientação dada por Sauro e Lewis [88].
- Usabilidade geral: através da pontuação *System Usability Scale*, medida por um questionário SUS (Seção 2.3.4) adaptado para a **Conta gov.br** e para o uso de e-mail e senha.

As métricas que são aferidas por questionários (SEQ e SUS) serão coletadas por um formulário eletrônico que será disponibilizado para os participantes.

### Preparação dos materiais e do ambiente de teste

Como foi adotada a premissa de utilizar o conceito de *persona* no teste com o intuito de proteger os dados pessoais dos participantes, não será possível fazer um teste de usabilidade no ambiente de produção do e-Cidadania, já que isso envolveria o uso das credenciais reais dos usuários. Por conta dessa decisão, o teste será feito no ambiente de homologação do sistema. Esse ambiente possui um servidor e um banco de dados separados e está integrado ao ambiente de testes da **Conta gov.br**. Com isso, é possível criar as credenciais necessárias para o teste utilizando a *persona*.

Como o ambiente de homologação do e-Cidadania só é acessível originalmente através da rede interna do Senado, será preciso modificar as regras de acesso para permitir, no período de testes, que usuários externos possam utilizar o sistema para que a avaliação de usabilidade seja possível. Essa alteração será temporária e controlada, a fim de evitar a exposição desse ativo na Internet por mais tempo do que o necessário.

### Escolha do testador e design do protocolo de teste

Rubin [53] orienta que utilizar um roteiro padronizado para conduzir o teste é importante para que todos recebam a mesma informação, reduzindo as chances que discrepâncias de condições entre um e outro participante. Ele sugere um *script* de introdução ao estudo, que será adaptado mais adiante, na Seção 4.2, para a realidade da pesquisa com a **Conta gov.br**.

## Design/seleção de questionários de satisfação e procedimentos de análise de dados

O questionário de satisfação padrão que será utilizado é o do *System Usability Scale*, conforme definido na Seção 4.1. Nos testes-piloto, apresentaremos um questionário adicional com o objetivo de avaliar o procedimento de teste. Esse questionário terá um *Single Ease Question* de sete níveis para responder aos seguintes questionamentos:

- “De uma forma geral, fazer as tarefas do teste foi algo:” - de Muito Difícil até Muito Fácil.
- “Qual o nível de clareza das instruções fornecidas para a reunião?”- de Muito Confusas até Muito Simples.
- “As atividades de permitir a utilização do microfone e câmera e o Compartilhamento de Tela foram atividades:”- de Muito Difíceis até Muito Fáceis

Além deles, haverá um campo de texto aberto para que o participante responda: “Há alguma sugestão que queira dar para facilitar o teste?”. Esse *feedback* será utilizado para melhorar a execução do teste.

A consistência dos dados será validada através do cálculo do Alfa de Cronbach nas respostas dos questionários, tal qual foi feito por Weidman e Grossklags [111]. A comparação entre as duas avaliações (login único e e-mail/senha) verificará se há significância estatística entre elas.

### Apresentação e comunicação dos resultados

Os dados resultantes do teste de usabilidade comporão o guia prático de utilização da *Conta gov.br*. Espera-se, com isso, que a decisão de incorporar a solução aos serviços fornecidos seja embasada em dados que afetam os usuários.

## 4.2 Configuração do Estudo-Piloto

Esta seção se destina a apresentar os materiais preparados para execução do teste-piloto. Aqui, serão definidos detalhes sobre a quantidade de pessoas, qualificação dos participantes, questionários e tecnologia que será usada nas sessões de avaliação de usabilidade.

### Distribuição dos participantes

Verificando os dados do Censo de 2022 [126], que foram definidos como a referência para o cálculo da proporção dos participantes, temos que a proporção por gênero de pessoas

acima de 15 anos é de 52% de mulheres e 48% de homens. Além disso, observamos a seguinte distribuição por idade na Tabela 4.1:

<b>Faixa etária</b>	<b>Mulheres</b>	<b>Homens</b>
<b>Acima de 60 anos</b>	21,07%	18,22%
<b>45 a 59 anos</b>	23,35%	23,04%
<b>30 a 44 anos</b>	28,95%	29,65%
<b>15 a 29 anos</b>	26,62%	29,09%

Tabela 4.1: Percentual da população por gênero X Faixas de idade. (Fonte: O Autor.)

Fundamentados nesses dados, estipularemos como meta a distribuição ilustrada pela Tabela 4.2, uma vez que ela tem percentuais próximos aos verificados na estatística da Tabela 4.1, definida como base. Ela também tenta distribuir, de forma uniforme, o conhecimento prévio da *Conta gov.br*.

<b>Faixa etária</b>	<b>Feminino</b>		<b>Masculino</b>	
	<b>Quant.</b>	<b>%</b>	<b>Quant.</b>	<b>%</b>
<b>Acima de 60 anos</b>	1	25%	1	25%
<b>45 a 59 anos</b>	1	25%	1	25%
<b>30 a 44 anos</b>	1	25%	1	25%
<b>15 a 29 anos</b>	1	25%	1	25%
<b>% total (sexo)</b>	50%		50%	

Tabela 4.2: Distribuição sugerida para execução do teste-piloto. (Fonte: O Autor.)

Além dessa alocação de participantes, também tentaremos equilibrar a quantidade de pessoas que já usaram a *Conta gov.br* com aquelas que nunca usaram, buscando ter quatro representantes de cada uma dessas situações.

## Mensagem e Formulário de Recrutamento

A mensagem que será enviada por e-mail e pela rede social WhatsApp, divulgando a pesquisa prévia para recrutamento do teste de usabilidade do e-Cidadania integrado à *Conta gov.br* é a seguinte:

Você tem 5 minutos para contribuir em uma pesquisa?

Queremos mensurar o grau de conhecimento que as pessoas têm da *Conta gov.br* e

do sistema e-Cidadania do Senado Federal. Além disso, procuramos pessoas que possam participar de um estudo de usabilidade envolvendo esses dois sistemas. Agradecemos muito se puder ajudar! Obrigado!

<LINK DO FORMULÁRIO DA PESQUISA>

Na sequência, apresentamos as mensagens de agradecimento por aceitar fazer parte da pesquisa, incluindo as respostas para os participantes elegíveis e para aqueles que não atendem às condições de participação.

Saudações, <Nome>!

Agradecemos seu interesse em participar de nossa pesquisa de usabilidade dos sistemas e-Cidadania e da **Conta gov.br**! Atitudes como essa fortalecem a ciência!

#### CASO A PESSOA NÃO POSSA PARTICIPAR

Nosso estudo envolve a seleção de usuários que atendam a certas características específicas e em quantidade limitada. Atualmente, alcançamos o número necessário de participantes com perfil semelhante ao seu. Portanto, infelizmente, não poderemos incluí-lo(a) nesta fase do estudo.

Agradecemos sua disponibilidade.

#### CASO A PESSOA QUEIRA PARTICIPAR

O processo de pesquisa de usabilidade do e-Cidadania e da **Conta gov.br** consiste em analisar a forma como você trabalha com tais soluções. Para isso, é necessário realizar uma videochamada com você, onde sua tela seria compartilhada e o procedimento de uso gravado. Um roteiro de tarefas será disponibilizado para você, considerando para sua realização, aproximadamente, 30 minutos.

Caso tenha interesse em participar, por favor, responda a esse e-mail informando uma sugestão de data e hora de realização do teste.

Agradecemos sua disponibilidade.

A mensagem que será enviada para os participantes com os detalhes da reunião on-line onde a avaliação de usabilidade ocorrerá contém o texto logo a seguir:

Olá, <Nome>!

Nossa reunião para execução do teste de usabilidade do e-Cidadania está agendada para o dia <Inserir a data>, às <Inserir as horas>.

Para que a sessão ocorra sem intercorrências, recomendamos que você mantenha somente a janela do navegador aberta, fechando os demais aplicativos em uso.

O link para nossa reunião, que ocorrerá com a ferramenta Google Meet, é: <Inserir o link da reunião>. Ao entrar, é possível que ele pergunte se você deseja habilitar o microfone e a câmera. Por favor, autorize esse acesso para que o estudo seja possível.

Quando o Google Meet apresentar sua câmera e microfone, solicite a participação na reunião. Quando for autorizado, a reunião se iniciará automaticamente.

Sua tela terá que ser compartilhada durante a sessão de testes. O pesquisador dará o auxílio necessário para que isso aconteça, caso encontre alguma dificuldade.

Muito obrigado por fazer parte da nossa pesquisa! Até lá!

Já o formulário de recrutamento que será enviado seguirá o que foi definido na Seção 4.1, e terá a estrutura apresentada no Apêndice A.1.

## **Executando o teste de usabilidade**

Ao marcar os detalhes do teste com o participante, será enviado um link do Google Meet. Quando a ligação estiver estabelecida, seguiremos o roteiro de introdução da sessão de teste que está no texto a seguir, baseado no modelo proposto por Rubin [53]:

*Os participantes que forem realizar o teste já preencheram o questionário de background, que contém também o acordo de não divulgação. Então, darei a eles uma visão geral das atividades que serão realizadas.*

*Anotar a hora de início:*

Obrigado por concordar em participar do nosso estudo de usabilidade hoje. Meu nome é Demétrius Jubé e conduzirei essa sessão de teste. Durante a mesma, estarei usando este roteiro para tentar garantir que as minhas instruções para todos os participantes sejam idênticas.

Para a realização do teste, como explicado no contato prévio, o procedimento deverá ser gravado. Você concorda com a gravação?

*Esperar a resposta da pessoa. Caso aceite, dizer o seguinte:*

Obrigado por aceitar. Vou então pedir para fazermos o seguinte: vou iniciar a gravação, introduzir a pesquisa e perguntar novamente se você concorda com a gravação da sessão. Peço que responda: “Sim, concordo com a gravação da sessão”. Pode ser assim?

Também peço que você feche qualquer sistema ou aplicação que estiver usando no momento, deixando apenas a janela com a nossa reunião, para evitar que dados sensíveis sejam expostos.

*Caso a pessoa autorize, iniciar a gravação da videochamada e dizer o seguinte:*

Bom dia/tarde/noite, <NOME DO PARTICIPANTE>. Obrigado por fazer parte do nosso estudo de usabilidade. Para sua realização, será necessário gravar o procedimento de teste. Você concorda com a gravação da sessão?

Obrigado por aceitar. Nosso objetivo hoje é observar você usando o sistema e-Cidadania. Durante a sessão, você trabalhará sozinho(a) enquanto eu o(a) acompanho pela videochamada. O tempo estimado do estudo é de 30 minutos.

Nesta sessão, vou pedir que você realize tarefas comuns, para entender como este sistema funciona com usuários do seu perfil. Por favor, considere que não estamos testando você - é você quem está nos ajudando a avaliar o sistema.

Vamos ajustar agora sua tela para que ela seja compartilhada comigo. Para fazê-lo, procure a opção de “Compartilhar Tela”. É o quinto botão, da esquerda para a direita, que fica na parte inferior da tela, entre o botão de “Reações” (uma carinha sorrindo) e o botão de “Levantar a Mão” (uma mão aberta). Uma tela vai aparecer perguntando o que você deseja compartilhar. Clique em “Janela”, e selecione a janela que a reunião está acontecendo.

Aqui está como a sessão funcionará:

- Vou enviar o link de um formulário eletrônico que conterà as instruções do teste que será realizado
- Ao abri-lo, o formulário apresentará a primeira instrução. Peço que leia em voz alta a instrução. Você pode ficar à vontade para tirar dúvidas sobre o que está escrito a qualquer momento
- Quando a página do e-Cidadania estiver sendo apresentada na sua tela e você estiver pronto(a) para começar, diga “Estou pronto(a) para começar”.
- Comece a trabalhar na tarefa apenas depois que eu disser “Por favor, comece.” Começarei a contar o tempo assim que você tocar no teclado ou no mouse, então não toque em nenhum dos dois até estar pronto(a) para iniciar a tarefa.
- Quando tiver completado a tarefa, diga em voz alta “Terminei.” Levante as mãos para a câmera para sinalizar que você terminou e está esperando pela próxima tarefa.
- Após cada tarefa, você responderá algumas perguntas sobre sua experiência ao realizar a tarefa no sistema.
- No final da sessão, você responderá mais um questionário sobre sua experiência geral.

Os cenários descritos no Quadro 4.1 serão apresentados no formulário eletrônico que colherá as respostas dos participantes. Ele engloba todas as tarefas elencadas na Seção 4.1:

<b>Item</b>	<b>Valor</b>
Cenário de Teste	Avaliação de usabilidade - e-Cidadania

Continua na próxima página

Quadro 4.1 – Continuação da página anterior

Item	Valor
Contexto	<p>Essa pesquisa tem como objetivo avaliar a usabilidade do sistema e-Cidadania e faz parte da Dissertação de Mestrado do aluno Demétrius de Almeida Jubé (demetrius.jube@aluno.unb.br).</p> <p>Nesta sessão, será solicitado que você realize tarefas comuns, para entender como este sistema funciona com usuários do seu perfil. Por favor, considere que não estamos testando você - é você quem está nos ajudando a avaliar o sistema.</p> <p>Assuma o seguinte contexto:</p> <p>Cida Gouveia, uma cidadã engajada nas questões sociais do país, deseja participar ativamente da democracia votando em uma Consulta Pública de seu interesse no sistema e-Cidadania do Senado Federal. Ela está em sua casa, utilizando seu computador pessoal, e precisa realizar a votação de forma rápida e segura para contribuir com sua opinião sobre o Estatuto do Idoso. Atuando como Cida, acesse o sistema e-Cidadania para encontrar a Consulta Pública que altera a lei mencionada.</p> <p>Quando estiver pronto(a) para começar, clique no botão “Próxima” para ir para a seção seguinte.</p>
Cenário 1	<ol style="list-style-type: none"> <li>1. Acesse o endereço &lt;Inserir o endereço de acesso ao e-Cidadania&gt;</li> <li>2. Quando a tela de login aparecer e você estiver pronto(a) para começar, diga: “Estou pronto(a) para começar”</li> <li>3. Quando receber a autorização para iniciar, utilize a opção de logar com e-mail e senha, usando as seguintes credenciais: <ul style="list-style-type: none"> <li>• E-mail: teste.usabilidade.gov.br@gmail.com</li> <li>• Senha: Cidadania123</li> </ul> </li> <li>4. Quando a tela de boas-vindas aparecer, informando que você está autenticado no Portal e-Cidadania, levante as mãos para a câmera e diga em voz alta: “Terminei”</li> <li>5. Aguarde a autorização do pesquisador para fazer a próxima tarefa.</li> <li>6. Procure a Consulta Pública que fala sobre o Estatuto do Idoso. Quanto achar que a encontrou, levante as mãos para a câmera e diga em voz alta: “Terminei”</li> <li>7. Responda às perguntas abaixo:</li> </ol>

Continua na próxima página

Quadro 4.1 – Continuação da página anterior

Item	Valor
Logout	<p>Os passos a seguir servem para preparar o ambiente para a outra tarefa. Faça o que se pede:</p> <ol style="list-style-type: none"> <li>1. Clique na opção Sobre do menu do e-Cidadania Identifique, no canto superior direito, onde estão escritas as palavras “Meu nome”</li> <li>2. Clique no link “Sair”, que está abaixo dessas palavras</li> <li>3. Verifique se a tela apresenta a mensagem “Você não está autenticado”, juntamente com a página de login</li> <li>4. O ambiente está pronto para a próxima tarefa</li> </ol>
Cenário 2	<ol style="list-style-type: none"> <li>1. Na tela de login, quando você estiver pronto(a) para começar, diga: “Estou pronto(a) para começar”</li> <li>2. Quando receber a autorização para iniciar, utilize a opção de logar com a <b>Conta gov.br</b>, usando as seguintes credenciais: <ul style="list-style-type: none"> <li>• CPF: 431.657.160-56</li> <li>• Senha: CidaGouveia@123</li> </ul> </li> <li>3. Quando a tela de boas-vindas aparecer, informando que Cida está autenticada no Portal e-Cidadania, levante as mãos para a câmera e diga em voz alta: “Terminei”</li> <li>4. Aguarde a autorização do pesquisador para fazer a próxima tarefa.</li> <li>5. Procure a Consulta Pública que fala sobre o Estatuto do Idoso. Quanto achar que a encontrou, levante as mãos para a câmera e diga em voz alta: “Terminei”</li> <li>6. Responda às perguntas a seguir:</li> </ol>

Quadro 4.1: Descrição do Cenário de Teste de usabilidade - E-mail e senha e **Conta gov.br**. (Fonte: O Autor.)

As perguntas que serão respondidas após a execução dos cenários propostos são uma junção do questionário SUS com o *Single Ease Question*, conforme descrito no Quadro 4.2:

Número	Pergunta
1	Eu acho que gostaria de usar esse sistema frequentemente.
2	Eu achei esse sistema desnecessariamente complexo.
3	Eu achei esse sistema fácil de usar.

Continua na próxima página

Quadro 4.2 – Continuação da página anterior

Número	Pergunta
4	Eu achei que precisaria de ajuda de uma pessoa técnica para ser capaz de usar esse sistema.
5	Eu achei que as várias funções desse sistema foram bem integradas.
6	Eu acho que o sistema apresenta muita inconsistência.
7	Eu imagino que a maioria das pessoas pode aprender a usar esse sistema rapidamente.
8	Eu achei esse sistema muito pesado para usar.
9	Eu me senti muito seguro usando o sistema.
10	Eu precisei aprender muitas coisas antes que pudesse utilizar esse sistema.
11 (SEQ)	De uma forma geral, essa tarefa foi:

Quadro 4.2: Perguntas do questionário SUS e SEQ utilizadas no teste de usabilidade. (Fonte: O Autor.)

Na execução do estudo-piloto, uma seção de perguntas adicional será apresentada para identificar o *feedback* dos participantes sobre os procedimentos executados na avaliação. As perguntas dessa seção são apresentadas no Apêndice A.2.

As sugestões que forem dadas pelos integrantes do estudo-piloto, assim como as dificuldades observadas durante a realização das sessões, servirão de base para tornar o processo de coleta de informações final mais simples e preciso. Elas também darão o insumo para a criação das rotinas de análise das respostas, que permitirão extrair as métricas definidas no protocolo de pesquisa.

### 4.3 Síntese do Capítulo

Neste capítulo apresentamos a metodologia proposta para execução dos testes de usabilidade do e-Cidadania juntamente com a **Conta gov.br**, sendo que dois aspectos foram analisados: o protocolo de teste que seria seguido, e a estruturação de um estudo-piloto para validar o que foi projetado.

No protocolo estabelecemos os objetivos do teste, o modo de qualificação e recrutamento dos participantes, o conjunto de tarefas que deveriam ser realizadas para avaliar o processo de login, tanto do mecanismo próprio do e-Cidadania, quanto da **Conta gov.br**. Além disso, definimos as métricas que seriam coletadas (Tempo de Conclusão, Facilidade Percebida e Pontuação SUS), e também traçamos um panorama de como seria o ambiente de teste.

Já no estudo-piloto instanciamos o protocolo, estipulando valores concretos para aquilo que estava abstrato. Como exemplo, temos:

- Definição da distribuição sugerida dos participantes, utilizando os dados do Censo de 2022, já que não foi possível extrair o público-alvo do próprio e-Cidadania, por conta de restrições de dados
- Especificação das mensagens e formulários de recrutamento, além do formulário de pesquisa
- Estabelecimento dos *scripts* de condução e dos cenários dos testes
- Questionários de *feedback* para a dinâmica dos testes

Em suma, o capítulo propiciou a confecção de materiais que serão utilizados na prática, seguindo tanto o arcabouço teórico visto no capítulo do Embasamento, quanto utilizando as informações oriundas da Revisão Sistemática da Literatura. Tais ações foram imprescindíveis para que os procedimentos fossem executados e os dados, coletados, conforme explicitado no Capítulo 5.

# Capítulo 5

## Análise dos Resultados

O processo de teste de usabilidade desenvolvido nesta pesquisa foi influenciado por dois fatores importantes que impactaram o planejamento e a execução da coleta de dados. O primeiro foi a constatação de que o estudo deveria ser submetido ao Comitê de Ética da Universidade de Brasília, pois utilizamos na pesquisa técnicas qualitativas de levantamento de dados, como a utilização de um questionário aplicado em seres humanos para medir a usabilidade [128]. Esse requisito adicionou etapas burocráticas e ajustes no cronograma do estudo. O segundo fator foi a disponibilização dos resultados da enquete que o Instituto DataSenado realizou com os usuários do e-Cidadania, fato que mudou a dinâmica de recrutamento. Os dois fatos relevantes serão tratados nas seções 5.1 e 5.2.

### 5.1 Submissão ao Comitê de Ética

O Comitê de Ética em Pesquisa em Ciências Humanas e Sociais (CEP/CHS) da Universidade de Brasília, registrado em 2007, foi o primeiro comitê especializado na pesquisa social criado no Brasil. O objetivo primário do colegiado, que é composto por uma equipe multidisciplinar e multiprofissional, é revisar e monitorar eticamente as pesquisas que envolvem seres humanos, visando garantir a integridade e segurança dos participantes nas pesquisas [129].

Tal verificação é feita analisando um conjunto de documentos que são entregues para exame, conforme a lista abaixo:

- Carta de encaminhamento: documento que contém as informações básicas da pesquisa, como o título e os pesquisadores, além de uma breve descrição dos objetivos e métodos. Serve para formalizar o pedido de análise junto ao Comitê.

- Folha de rosto: documento que é gerado no cadastro dos documentos na Plataforma Brasil [130], sistema utilizado para concentrar os pedidos de análise em todo o território brasileiro.
- Instrumento de coleta de dados: questionário ao qual os participantes serão submetidos no teste, visando garantir que não haja pergunta que possa deixar o respondente desconfortável.
- Carta de Aceite Institucional: documento que deve conter o aval da instituição que receberá a pesquisa. No caso da pesquisa em tela, alguma autoridade do Senado Federal, já que o e-Cidadania, sistema avaliado na pesquisa, é de responsabilidade do órgão.
- Currículo Lattes de todos os pesquisadores envolvidos.
- Carta de revisão ética: registro que apresenta os riscos aos quais os participantes da pesquisa estarão expostos, bem como quais são as tratativas para minimizá-los.
- Termo de Consentimento Livre e Esclarecido (TCLE): termo que apresenta as informações da pesquisa para os participantes, garantindo que eles estejam plenamente informados sobre o estudo e consentam voluntariamente em participar. Ele descreve os riscos e benefícios da pesquisa, além de ressaltar a confidencialidade dos dados pessoais que forem coletados.
- Termo de Autorização para Utilização de Imagem e Som de Voz: utilizado quando há gravação do participante. Ele detalha como a imagem e a voz serão utilizados na pesquisa, ao mesmo tempo que garante a privacidade do respondente ao afirmar que os dados não serão divulgados em nenhum tipo de meio de comunicação.

Ao receber o projeto, o CEP/CHS realiza uma avaliação documental para verificar a completude e conformidade dos documentos submetidos [131]. Se aprovado nessa etapa, o projeto é designado a um parecerista para análise ética e documental. O parecer elaborado é então discutido em reunião do colegiado, onde podem ser feitas inclusões ou alterações. O parecer final do colegiado é posteriormente enviado ao pesquisador, concluindo o processo de avaliação ética.

Os documentos citados anteriormente foram elaborados entre 1 e 15 de maio de 2024, quando a Carta de Aceite Institucional foi submetida ao Senado Federal para análise e parecer da Diretoria-Geral, unidade considerada mais apropriada para se manifestar sobre o assunto. Entretanto, como o e-Cidadania é de responsabilidade da Secretaria-Geral da Mesa, o documento foi enviado para lá e sua análise se estendeu até o dia 14/6/2024. Esse prazo dilatado impactou o cronograma e a execução do planejamento da pesquisa, pois há uma característica adicional quando um estudo é submetido ao Comitê de Ética: não

é possível submeter o questionário a ninguém, pois o CEP/CHS só analisa projetos que não tiveram sua etapa de coleta de dados iniciada. E, como o processo de análise ética tem um prazo indefinido, uma vez que é minucioso, o Comitê orienta que a data prevista para a coleta seja projetada com uma margem de tempo adicional de um mês após a data da reunião do colegiado do mês da submissão, o que deixaria a pesquisa liberada para aquisição de dados a partir do final de julho de 2024.

Diante desse cenário de incerteza, a submissão dos questionários prevista no estudo-piloto foi abortada, já que esperar todo esse tempo para validar o processo de coleta traria um risco muito grande à conclusão bem-sucedida do estudo. Como alternativa, o roteiro original foi apresentado a um grupo de pessoas de confiança do pesquisador, que deram sugestões de melhoria no procedimento e que serão apresentadas posteriormente.

Por fim, o parecer consubstanciado do CEP/CHS foi liberado em 23 de junho de 2024, sob o número 6.903.626. No documento, o colegiado afirma que todas as questões formuladas para os respondentes estão de acordo com as orientações do Comitê, e valida o Termo de Consentimento Livre e Esclarecido para uso com os participantes. Essa chancela mostrou-se importante posteriormente, quando alguns candidatos questionaram a autenticidade da pesquisa, temendo que se tratasse de um golpe. Ao orientar que os interessados consultassem o parecer na Plataforma Brasil, eles puderam confirmar a veracidade das informações e decidir participar do estudo.

As alterações metodológicas vistas nessa seção não foram as únicas. Veremos na seção 5.2 quais foram as mudanças feitas após o resultado da enquete conduzida pelo DataSenado.

## 5.2 Enquete do DataSenado

O Instituto DataSenado é um órgão do Senado Federal que realiza estudos e pesquisas sobre temas de interesse público e legislativo, fornecendo informações para subsidiar o trabalho dos senadores e oferecer dados ao público. A unidade conduz enquetes, pesquisas de opinião e análises, abrangendo áreas como política, economia e direitos do cidadão [127]. O Instituto também pode ser acionado por unidades internas para prover os gestores com dados para embasar decisões sobre a condução de ações ao público interno ou externo.

Foi com esse último intuito que a Coordenação do Programa e-Cidadania, unidade responsável por gerir o sistema, solicitou que fosse feita uma enquete para avaliar a opinião dos usuários sobre a integração do e-Cidadania com a *Conta gov.br*. O objetivo era medir o impacto dessa mudança, além de verificar qual a possibilidade de tornar este modo de autenticação obrigatório para quem quisesse votar nas proposições apresentadas na plataforma.

As perguntas da enquete foram desenvolvidas pelos analistas do DataSenado com o auxílio do pesquisador, que sugeriu incluir questões sobre a utilização da **Conta gov.br** para acessar outros serviços, a percepção de segurança e privacidade no uso dessa autenticação, e o interesse em participar de uma videoconferência para avaliar a solução. Aqueles que respondessem à última pergunta afirmativamente compartilhariam seu e-mail pessoal com o pesquisador, de forma que pudessem ser contatados posteriormente para a execução do teste de usabilidade.

O objetivo dessa abordagem foi ampliar o alcance do recrutamento dos candidatos do teste, uma vez que a base de usuários existente para envio da enquete contava com 639.493 registros, distribuídos por todo o Brasil. Com isso, esperava-se alcançar uma amostra mais diversa de candidatos e promover maior aleatoriedade no processo de captação de respondentes. O efeito colateral dessa decisão foi a impossibilidade de ter, no estudo de usabilidade, alguém que não conhecesse o sistema e-Cidadania. Esse fato gera uma perda da perspectiva de pessoas que nunca tinham usado o sistema e poderiam fornecer impressões únicas desse público, mas foi considerada aceitável diante dos benefícios citados anteriormente e, pelo fato de que a usabilidade a ser medida é do processo de login utilizado, e não do sistema em si.

A coleta de dados ocorreu de 20 de maio a 2 de junho de 2024, através de um questionário on-line, que alcançou uma taxa de resposta de 3,02% do total de convites enviados por e-mail, com 19.309 respostas válidas. Os dados demográficos dos respondentes podem ser verificados na Figura 5.1 e os resultados principais que interessam à pesquisa foram os seguintes:

- Uso da **Conta gov.br** pelos usuários do e-Cidadania: 96% dos que não utilizaram a **Conta gov.br** como meio de autenticação indicaram que possuem credencial no serviço, com 79% relatando satisfação com o componente.
- Privacidade: 72% sentem-se seguros ou muito seguros ao usar a **Conta gov.br** para se autenticar.
- Disponibilidade para participar de uma videoconferência sobre o tema: 31% dos respondentes mostraram interesse em participar de uma videochamada sobre o uso da **Conta gov.br** no e-Cidadania.
- Continuidade do uso com obrigatoriedade da **Conta gov.br**: 72% afirmaram que continuariam usando o e-Cidadania caso o uso da **Conta gov.br** fosse obrigatório.

Esses dados são relevantes por sugerirem que o uso da **Conta gov.br** está bem difundido entre os respondentes e, portanto, a integração do meio de autenticação com serviços disponibilizados pelo Senado pode encontrar pouca resistência por parte dos cidadãos que,

em sua maioria, sentem-se seguros ao utilizar a ferramenta. Mas, é bom destacar que isso é uma inferência, uma vez que o levantamento foi feito por meio de uma enquete, que não permite generalizações, ao contrário das pesquisas realizadas pelo órgão, que aplicam técnicas estatísticas para garantir representatividade e precisão nas estimativas [132].

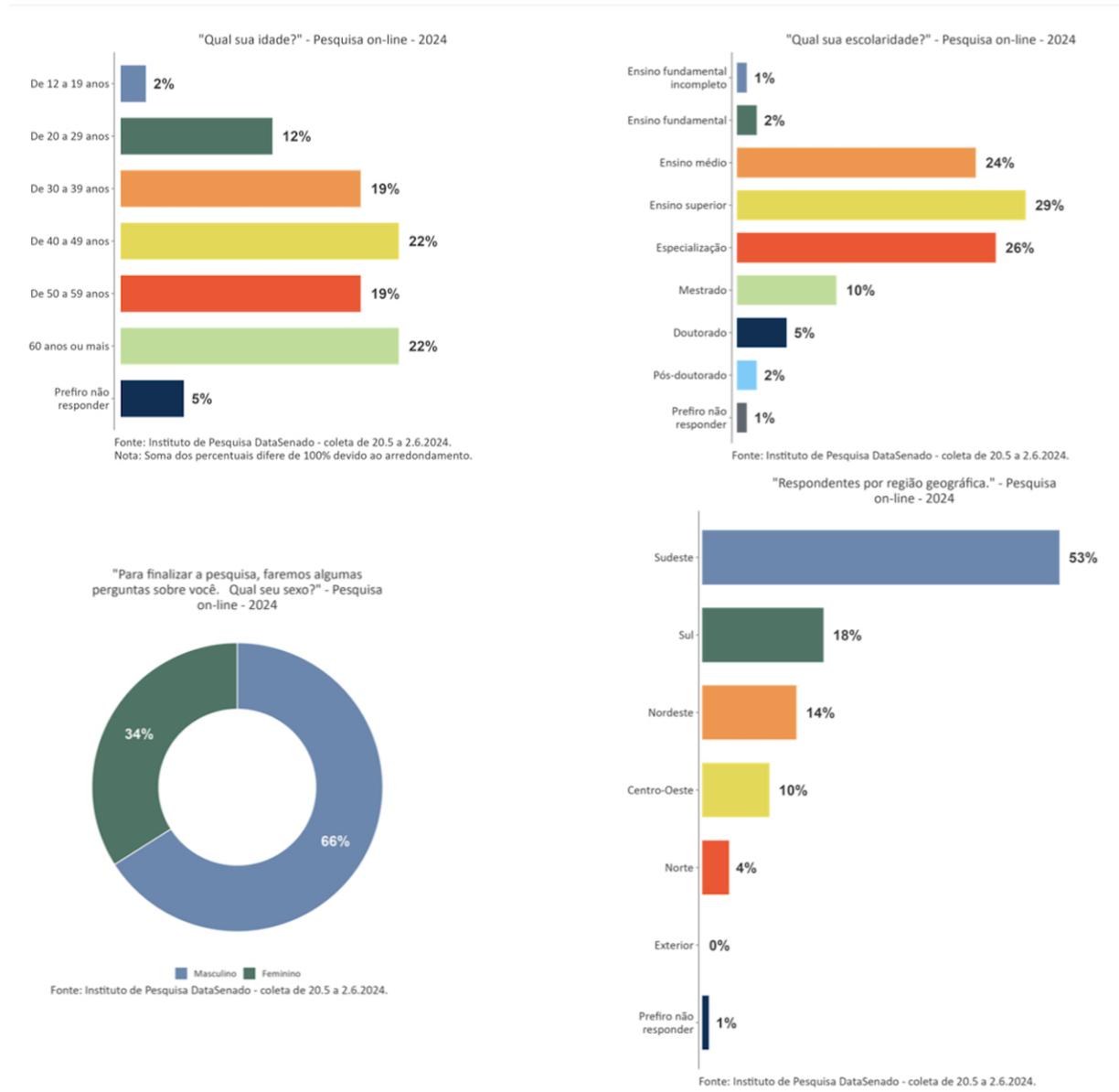


Figura 5.1: Dados demográficos da enquete DataSenado. (Fonte: Instituto DataSenado [133]).

Por fim, como as informações dos respondentes mostraram uma cobertura por todo o território nacional e uma ampla diversidade de faixa etária e escolaridade, optamos por utilizar essa fonte de dados como base para o recrutamento dos participantes do teste de usabilidade, visando tornar a seleção mais aleatória e abrangente. Para fins de compara-

ção, uma enquete de recrutamento feita pelo pesquisador e enviada por redes sociais no período de março a abril de 2024 conseguiu um total de 102 pessoas dispostas a participar do processo de teste, enquanto pelo DataSenado tivemos 5.900 pessoas disponíveis.

Essa decisão exigiu que o processo de recrutamento fosse redesenhado, uma vez que, para proteger a privacidade dos participantes da enquete, o Instituto DataSenado forneceu apenas os e-mails daqueles que se prontificaram a participar do teste, sem nenhum cruzamento com as respostas dadas na enquete. Os detalhes do novo protocolo de teste, contendo as diretrizes de recrutamento e as modificações sugeridas no roteiro inicial, serão apresentados na seção subsequente.

## 5.3 Protocolo Final do Teste de Usabilidade

Como citado nas seções 5.1 e 5.2, a submissão ao Comitê de Ética e os resultados apresentados pela enquete do Instituto DataSenado levaram a alterações no protocolo de teste de usabilidade que foi proposto no Capítulo 4, no que diz respeito ao recrutamento dos participantes e ao roteiro de aplicação.

### 5.3.1 Recrutamento

A base do recrutamento foi a lista de e-mails fornecida pelo DataSenado dentre aqueles que se prontificaram a participar da videochamada do teste de usabilidade. Embora 5.900 pessoas tenham respondido afirmativamente à questão sobre a disponibilidade de participar da pesquisa, a lista de endereços eletrônicos que foi entregue continha 5.016 registros. Essa discrepância ocorreu porque o item que perguntava o e-mail do respondente não era de preenchimento obrigatório.

O e-mail de recrutamento foi ajustado para conter as informações da aprovação no Comitê de Ética, como o número do parecer, as instruções de como validá-lo e os contatos do pesquisador. Além disso, foi acrescentada uma contextualização da pesquisa DataSenado para que o destinatário lembrasse da resposta à enquete, que foi realizada anteriormente. Finalmente, anexado ao corpo do e-mail, foi enviado o Termo de Consentimento Livre e Esclarecido definido no processo de aprovação da pesquisa junto ao CEP/CHS, assinado digitalmente. O TCLE encontra-se no Apêndice B e o modelo do texto de recrutamento está apresentado a seguir:

Olá!

No período de 20 de maio a 02 de junho de 2024, o Instituto DataSenado realizou uma enquete para conhecer a opinião dos usuários do e-Cidadania sobre a integração com a Conta GOV.BR. Constatamos nos nossos registros que você respondeu de forma afirmativa à pergunta: “Você teria interesse em participar de uma atividade por

videochamada sobre os temas levantados nessa pesquisa? Ela seria feita em um outro momento, combinado com você”.

Essa atividade faz parte da pesquisa “Análise da usabilidade da *Conta gov.br* para adoção pelo Senado Federal”, sob a responsabilidade de Demétrius de Almeida Jubé, estudante de mestrado do Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília. O objetivo desta pesquisa é avaliar os benefícios em relação à usabilidade que a incorporação da *Conta gov.br* trouxe para o sistema e-Cidadania do Senado Federal.

Vale frisar que essa pesquisa obteve aprovação do Comitê de Ética em Pesquisa em Ciências Humanas e Sociais da UnB (CEP CHS), através do Parecer 6.903.626, que pode ser validado através da Plataforma Brasil (<https://plataformabrasil.saude.gov.br/>), item “Confirmar Aprovação pelo CAAE ou Parecer”. Essa aprovação garante ao participante aspectos como segurança dos dados pessoais e anonimato no resultado do estudo.

O processo de pesquisa de usabilidade do e-Cidadania e da *Conta gov.br* consiste em analisar a forma como você trabalha com tais soluções. Para isso, é necessário que você tenha acesso a um computador com microfone para que seja realizada uma videochamada com você (a câmera é opcional). Nesse encontro sua tela seria compartilhada e o procedimento de uso, gravado. Um roteiro de tarefas será disponibilizado, e o tempo estimado para sua realização é de aproximadamente 30 minutos.

Dessa forma, caso ainda tenha interesse em participar, por favor, responda a esse e-mail informando uma sugestão de data e hora de realização do teste. Se preferir que essa combinação seja feita pelo WhatsApp, basta informar o número na resposta também.

Se não quiser receber outros e-mails relativos a essa pesquisa, por favor, nos avise também.

Agradecemos sua disponibilidade.

Demétrius Jubé

<Telefone do pesquisador>

Abordaremos, na seção 5.3.2, quais foram as modificações realizadas no roteiro de aplicação originalmente proposto na seção 4.2.

### 5.3.2 Roteiro de aplicação

O roteiro original foi alterado por conta de sugestões que foram dadas quando o texto foi apresentado a familiares, colegas pesquisadores e do Senado Federal, em busca de críticas e recomendações, conforme mencionado na seção 5.1, e estão elencadas a seguir:

1. Reescrever o ponto do roteiro que avisava sobre a gravação, aproximando-o do momento em que ela efetivamente seria realizada.

2. Separar as tarefas de pesquisa da Consulta Pública do processo de autenticação, deixando claro que são situações distintas. Além disso, a complexidade da pesquisa exigiu essa segregação para evitar influência na avaliação do login.
3. Explicitar na instrução do cenário de login com a **Conta gov.br** que a autenticação deve ser feita utilizando esse mecanismo.
4. Solicitar que o próprio participante leia em voz alta as instruções, em vez do pesquisador, para reduzir a dependência de explicações e aumentar a atenção na execução do teste. A leitura deve se restringir aos pontos em que o participante precisa realizar uma ação, evitando impaciência.
5. Destacar, nas perguntas de avaliação do SUS, que o termo “sistema” se refere especificamente aos mecanismos de login utilizados.
6. Solicitar o fechamento das abas do navegador que estiverem abertas com o e-Cidadania entre um cenário e outro, prevenindo confusão sobre onde o participante deve continuar o roteiro.
7. Simplificar as instruções, eliminando a necessidade de gestos como levantar as mãos. Como o processo é gravado, o monitoramento da execução do teste pode ser feito sem esse recurso.

Além dessas sugestões, outra mudança que foi executada por conta de uma orientação apresentada em Sauro e Lewis [88] relativa ao formato do teste utilizado, que é a comparação intra-sujeitos (*within-subjects comparison*). Nesse tipo de avaliação, os mesmos usuários avaliam condições diferentes no mesmo teste, como ocorre na presente pesquisa, onde os participantes examinam o login utilizando a **Conta gov.br** e a conta usando e-mail e senha. Os autores sugerem que testes com essa característica alternem a apresentação dos produtos aos participantes para evitar o efeito *carryover*.

Este fenômeno, também conhecido como efeito de transferência, ocorre quando a experiência de um participante em uma etapa do experimento influencia seu desempenho em uma etapa seguinte. Bordens e Abbott [134] explicam que esse efeito pode comprometer a validade dos resultados em experimentos de desenho intra-sujeitos, pois pressupõe que as características dos participantes permaneçam constantes em todas as condições. No entanto, quando um tratamento ou tarefa anterior altera a forma como o participante executa a seguinte, a comparação entre os cenários testados pode ser prejudicada.

Dessa forma, apresentar os métodos de autenticação em uma ordem fixa poderia criar um viés na análise. Supondo que a autenticação com a **Conta gov.br** fosse sempre experimentada primeiro, os participantes poderiam criar um viés positivo simplesmente

por ser a primeira experiência, ou negativo, caso sejam mais críticos por não terem a habilidade necessária para a execução do roteiro.

Sendo assim, a estratégia do contrabalanceamento (*counterbalancing*), que consiste em variar a ordem de apresentação das experiências, foi aplicada criando dois formulários que alternavam entre os dois cenários de teste (**Conta gov.br** e e-mail e senha), e que seriam apresentados de forma intercalada entre os participantes.

Finalmente, a submissão ao Comitê de Ética nos instigou a apresentar no formulário eletrônico um texto com o termo de autorização para utilização de imagem e voz para fins de pesquisa. Dessa forma, ficaria mais claro para o participante a forma como a gravação realizada seria usada, conferindo mais segurança e, também, dando a oportunidade dele declinar do estudo, caso não concordasse com algo. O roteiro final está apresentado a seguir:

Obrigado por concordar em participar do nosso estudo de usabilidade hoje. Meu nome é Demétrius Jubé e conduzirei essa sessão de teste. Durante a mesma, estarei usando este roteiro para tentar garantir que as minhas instruções para todos os participantes sejam idênticas.

Faremos algumas configurações para a reunião. Peço que você feche qualquer sistema ou aplicação que estiver usando no momento, deixando apenas a janela com a nossa reunião, para evitar que dados sensíveis sejam expostos.

Vamos ajustar agora sua tela para que ela seja compartilhada comigo. Para fazê-lo, procure a opção de “Compartilhar Tela”. É o quinto botão, da esquerda para a direita, que fica na parte inferior da tela, entre o botão de “Reações” (uma carinha sorrindo) e o botão de “Levantar a Mão” (uma mão aberta). Uma tela vai aparecer perguntando o que você deseja compartilhar. Clique em “Janela”, selecione a janela que a reunião está acontecendo, e clique no botão “Compartilhar”. Eu vou desligar a minha câmera para podermos visualizar apenas a sua tela.

Vou enviar o link de um formulário eletrônico que conterá as instruções do teste que será realizado pelo chat da reunião. É o segundo botão, da direita para a esquerda, da parte inferior da tela, que tem o nome “Chat com todos”.

*Nesse momento, é enviado o link do formulário referente ao teste, baseado na resposta do teste anterior. Caso tenha sido feito o teste com o cenário da **Conta gov.br** primeiro, enviaremos o formulário em que o login com e-mail e senha é a primeira tarefa.*

Para a realização do teste, como explicado no contato prévio, o procedimento deverá ser gravado. Você concorda com a gravação?

*Esperar a resposta da pessoa. Caso aceite, dizer o seguinte:*

Obrigado por aceitar. Vou então pedir para fazermos o seguinte: vou iniciar a gravação, introduzir a pesquisa e perguntar novamente se você concorda com a gra-

vação da sessão. Peço que responda: “Sim, concordo com a gravação da sessão”. Pode ser assim?

*Caso a pessoa autorize, iniciar a gravação da videochamada e dizer o seguinte:*

A gravação foi iniciada. Bom dia/tarde/noite, <NOME DO PARTICIPANTE>. Obrigado por fazer parte do nosso estudo de usabilidade. Para sua realização, será necessário gravar o procedimento de teste. Você concorda com a gravação da sessão?

Obrigado por aceitar. Nosso objetivo hoje é observar você usando o sistema e-Cidadania. Durante a sessão, você trabalhará sozinho(a) enquanto eu o(a) acompanho pela videochamada. O tempo estimado do estudo é de 30 minutos.

Neste teste, vou pedir que você realize tarefas comuns, para entender como este sistema funciona com usuários do seu perfil. Por favor, considere que não estamos testando você - é você quem está nos ajudando a avaliar o sistema.

Aqui está como o teste funcionará:

- O formulário contém Seções. Peço que aguarde minhas instruções antes de ir de uma seção para outra.
- Em cada seção, haverá um texto explicando o que deve ser feito. Pedirei que leia o texto de algumas instruções em voz alta. Você pode ficar à vontade para tirar dúvidas sobre o que está escrito a qualquer momento.
- Algumas seções contêm perguntas sobre sua experiência ao realizar a tarefa no sistema. As perguntas tem como objetivo captar a sensação, por isso, é interessante que responda na primeira impressão que tiver, sem precisar pensar muito, pois elas podem parecer não ter uma lógica clara.

Alguma dúvida?

*Texto para ser lido na primeira seção do formulário - Termo de autorização e dados demográficos.*

Essa seção contém a autorização de uso de imagem e som da voz. Fique à vontade para ler, **não precisa ser em voz alta**, e caso concorde, preencher os dados do formulário e passar para a próxima seção.

*Texto para ser lido na segunda seção do formulário - Contexto do teste.*

Essa seção contém o contexto em que as tarefas serão realizadas. Peço que leia, **não precisa ser em voz alta**, e quando terminar, avance para a próxima seção.

*Texto para ser lido na terceira seção do formulário - Primeiro mecanismo de login e questionário SUS/SEQ.*

Essa seção contém o cenário de teste que será executado. Peço que você leia o roteiro todo **em voz alta**, e caso não tenha nenhuma dúvida, nós executamos o roteiro. Depois disso, voltamos pra essa tela pra responder às perguntas. Pode ser assim?

*Texto para ser lido na quarta seção do formulário - Consultas públicas.*

Nessa seção, peço que execute a instrução apresentada.

*Texto para ser lido na quinta seção do formulário - Logout.*

Nessa seção vou pedir que você leia o roteiro todo **em voz alta**, e caso não tenha nenhuma dúvida, nós executamos, ok?

*Texto para ser lido na sexta seção do formulário - Segundo mecanismo de login e questionário SUS/SEQ.*

Essa seção contém outro cenário de teste que será executado. Peço que você leia o roteiro todo **em voz alta**, e caso não tenha nenhuma dúvida, nós executamos o roteiro. Depois disso, voltamos pra essa tela pra responder às perguntas. Pode ser assim?

*Texto para ser lido na sétima seção do formulário - Ideias legislativas.*

Nessa seção, peço que execute a instrução apresentada, e depois finalize a pesquisa.

Vou encerrar a gravação...

*Terminar a gravação e agradecer à pessoa pela participação no estudo.*

O Quadro 5.1 apresenta como ficou o formulário final utilizado na pesquisa:

Seção	Texto
1	<p>Essa pesquisa tem como objetivo avaliar a usabilidade do sistema e-Cidadania e faz parte da Dissertação de Mestrado do aluno Demétrius de Almeida Jubé (demetrius.jube@aluno.unb.br).</p> <p><b>Termo de autorização para utilização de imagem e som de voz para fins de pesquisa</b></p> <p>Eu autorizo a utilização da minha imagem e som de voz, na qualidade de participante no projeto de pesquisa intitulado Análise de benefícios da adoção da <b>Conta gov.br</b> para o Senado Federal, sob responsabilidade de Demétrius de Almeida Jubé, vinculado ao Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília.</p> <p>Minha imagem e som de voz podem ser utilizadas apenas para análise por parte da equipe de pesquisa.</p>

Continua na próxima página

Quadro 5.1 – Continuação da página anterior

Seção	Texto
	<p>Tenho ciência de que não haverá divulgação da minha imagem nem som de voz por qualquer meio de comunicação, sejam eles televisão, rádio ou internet, exceto nas atividades vinculadas ao ensino e à pesquisa explicitadas acima. Tenho ciência também de que a guarda e demais procedimentos de segurança com relação às imagens e som de voz são de responsabilidade do pesquisador responsável.</p> <p>Deste modo, ao clicar no botão abaixo, declaro que autorizo, livre e espontaneamente, o uso para fins de pesquisa, nos termos acima descritos, da minha imagem e som de voz.</p>
2	<p>Nesta sessão de teste, será solicitado que você faça tarefas típicas de uso do sistema, para aprender como este sistema funciona para você. Por favor, tenha em mente que não estamos testando você - é você quem está nos ajudando a avaliar o sistema.</p> <p>Assuma o seguinte contexto:</p> <p>Cida Gouveia, uma cidadã engajada nas questões sociais do país, deseja participar ativamente da democracia votando em uma Consulta Pública de seu interesse no sistema e-Cidadania do Senado Federal. Ela está em sua casa, utilizando seu computador pessoal, e precisa entender algumas funções do e-Cidadania. Atuando como Cida, acesse o sistema e-Cidadania para encontrar as Consultas Públicas e as Ideias Legislativas.</p> <p>Quando estiver pronto(a) para começar, clique no botão “Próxima” para ir para a Seção seguinte.</p>
3	<p><b>Cenário 1 - Utilização do E-mail e Senha</b></p> <p>Siga o roteiro abaixo:</p> <ol style="list-style-type: none"> <li>1. Acesse o endereço &lt;Inserir o endereço de acesso ao e-Cidadania&gt;</li> <li>2. Quando receber a autorização para iniciar, utilize a opção de logar com e-mail e senha, usando as seguintes credenciais: <ul style="list-style-type: none"> <li>• E-mail: teste.usabilidade.gov.br@gmail.com</li> <li>• Senha: Cidadania123</li> </ul> </li> <li>3. Espere a confirmação da sua autenticação, com o aparecimento da mensagem “Você está autenticado”</li> </ol>

Continua na próxima página

Quadro 5.1 – Continuação da página anterior

Seção	Texto
	4. Responda às perguntas a seguir, assumindo que o “sistema” se refere ao processo de autenticação usando e-mail e senha:
4	Consultas Públicas Faça o que se pede: 1. Procure no e-Cidadania uma forma de ver as Consultas Públicas. Quando achar que encontrou, diga: “Terminei”.
5	Logout Os passos abaixo servem para preparar o ambiente para a outra tarefa. Faça o que se pede: 1. Feche a aba do e-Cidadania que está aberta 2. Acesse o endereço <Inserir o endereço de acesso ao e-Cidadania> 3. Identifique, no lado direito da tela, onde estão escritas as palavras “Meu nome” 4. Clique no link “Sair”, que está abaixo dessas palavras 5. Verifique se a tela apresenta a mensagem “Você não está autenticado”, juntamente com a página de login 6. O ambiente está pronto para a próxima tarefa
6	<b>Cenário 2 - Login com a <i>Conta gov.br</i></b> Siga o roteiro abaixo: 1. Acesse o endereço <Inserir o endereço de acesso ao e-Cidadania> 2. Quando receber a autorização para iniciar, utilize a opção de logar com <b>gov.br</b> , usando as seguintes credenciais: <ul style="list-style-type: none"> <li>• CPF: 431.657.160-56</li> <li>• Senha: CidaGouveia@123</li> </ul> 3. Espere a confirmação da sua autenticação, com o aparecimento da mensagem “Bem-vindo, MEU NOME! teste.usabilidade.gov.br@gmail.com Você está autenticado no Portal e-Cidadania” 4. Responda às perguntas a seguir, assumindo que o “sistema” se refere ao processo de autenticação usando a <b>Conta gov.br</b> :
7	Ideias Legislativas Faça o que se pede:

Continua na próxima página

Quadro 5.1 – Continuação da página anterior

Seção	Texto
	1. Procure no e-Cidadania uma forma de ver as Ideias Legislativas. Quando achar que encontrou, diga: “Terminei”.

Quadro 5.1: Descrição do Teste de usabilidade - E-mail e senha e *Conta gov.br*. (Fonte: O Autor.)

Verificaremos os detalhes de como o teste de usabilidade foi aplicado na seção seguinte.

## 5.4 Execução do teste de usabilidade

A aplicação dos testes de usabilidade envolveu procedimentos padronizados e a captação das respostas que viabilizariam a análise a que o estudo se propôs. As seções 5.4.1 e 5.4.2 mostrarão os detalhes do processo de recrutamento e os dados demográficos dos participantes.

### 5.4.1 Recrutamento dos participantes

Para envio das mensagens de recrutamento, foi analisado o uso de serviços de envio de e-mail em massa, como o *SendPulse* [135]. Porém, isso implicaria em enviar os endereços eletrônicos dos respondentes para a plataforma, o que compartilharia a conta de e-mail dessas pessoas com a empresa, conforme explicado na Política de Privacidade [136]. Uma vez que as diretrizes éticas estabelecidas pelo CEP/CHS destacam que o pesquisador é o responsável pela guarda dos dados pessoais dos participantes, avaliamos que essa solução não seria adequada, dado o risco de vazamento dos dados caso o sistema de envio de e-mails sofresse algum ataque digital.

Diante desse contexto, optamos por utilizar a ferramenta de Mala Direta do Microsoft Word [137], uma vez que concentrava o processamento de envio na máquina do pesquisador, sem a necessidade de difundir os endereços eletrônicos para terceiros. Foi criado um arquivo CSV [100] com os e-mails fornecidos pelo Instituto DataSenado para servir de fonte de dados do documento, utilizando a conta de e-mail do pesquisador atrelada à Universidade de Brasília.

A fim de evitar que o envio massivo de mensagens fosse caracterizado como *spam*, limitamos os envios a 500 e-mails por dia. Esse número foi baseado no número de contatos máximo que plataformas de envio de e-mail em massa como *SendPulse* e *MailChimp* utilizam em seus planos gratuitos.

Foram executados dois envios em massa, nos dias 26 e 27 de agosto de 2024, totalizando 1.000 e-mails enviados conforme a ordem que estava originalmente no arquivo. Destes, oito se revelaram inválidos e 111 destinatários responderam ao e-mail, sendo que 13 disseram não ter interesse em participar da pesquisa. A Figura 5.2 ilustra o resultado da ação.



Figura 5.2: Resultado do envio do e-mail de recrutamento de participantes (Fonte: O Autor.)

As 98 pessoas restantes foram contatadas por e-mail ou WhatsApp, de forma a tentar identificar uma disponibilidade comum entre o pesquisador e o participante. Ao final desse processo, a meta de 30 entrevistas foi atingida nas datas e horários constantes no Quadro 5.2, que também separa os participantes de acordo com o cenário do teste a que foram submetidos:

E-mail e Senha/Conta gov.br		Conta gov.br/E-mail e Senha	
Participante	Data/Hora	Participante	Data/Hora
P1	30/08/2024 14:47	P2	30/08/2024 15:13
P3	30/08/2024 16:25	P4	03/09/2024 09:45
P5	03/09/2024 10:13	P6	03/09/2024 11:23
P8	03/09/2024 14:34	P7	03/09/2024 13:20
P10	03/09/2024 19:27	P9	03/09/2024 14:55
P12	04/09/2024 18:05	P11	04/09/2024 15:51
P14	06/09/2024 09:17	P13	05/09/2024 15:45
P16	10/09/2024 15:08	P15	09/09/2024 18:48
P18	15/09/2024 09:28	P17	11/09/2024 15:04
P20	01/11/2024 16:53	P19	01/11/2024 14:57

Continua na próxima página

E-mail e Senha/Conta gov.br		Conta gov.br/E-mail e Senha	
Participante	Data/Hora	Participante	Data/Hora
P22	02/11/2024 11:18	P21	02/11/2024 09:19
P24	02/11/2024 14:16	P23	02/11/2024 12:14
P26	04/11/2024 17:19	P25	02/11/2024 15:14
P28	29/11/2024 09:40	P27	05/11/2024 10:14
P30	13/12/2024 17:56	P29	29/11/2024 10:24

Quadro 5.2: Entrevistas organizadas por cenário, apresentando participantes e respectivas datas e horas de realização. (Fonte: O Autor.)

O Quadro 5.3 apresenta os dados demográficos de cada um dos participantes, sendo que as colunas foram renomeadas para melhorar a legibilidade, conforme as definições a seguir:

- **QD1:** Qual a sua faixa de idade?
- **QD2:** Qual seu gênero?
- **QD3:** Qual o seu grau de instrução?
- **QD4:** Em qual Estado do Brasil você nasceu?
- **QD5:** Em qual Estado do Brasil você reside?
- **QD6:** Você já usou a **Conta gov.br**, utilizada como login para acessar serviços do SUS, inscrever-se no ENEM, consultar sua CNH ou Carteira de Trabalho Digital, simular aposentadoria no Meu INSS, entre outros serviços?
- **QD7:** Como você classifica sua habilidade com uso de soluções de tecnologia da informação (Ex: Uso de redes sociais, aplicativos, editores de texto, planilhas, navegação por sites)?

ID	QD1	QD2	QD3	QD4	QD5	QD6	QD7
P1	30 a 44 anos	F	Pós-Graduação	AM	AM	Sim	6
P2	30 a 44 anos	F	Pós-Graduação	SC	SC	Sim	7
P3	Acima de 60 anos	M	Graduação	RJ	RJ	Sim	7
P4	Acima de 60 anos	F	Pós-Graduação	SP	SP	Sim	7
P5	30 a 44 anos	M	Pós-Graduação	SP	SP	Sim	7
P6	30 a 44 anos	M	Pós-Graduação	RO	RO	Sim	7

Continua na próxima página

Quadro 5.3 – Continuação da página anterior

ID	QD1	QD2	QD3	QD4	QD5	QD6	QD7
P7	30 a 44 anos	M	Pós-Graduação	SP	SP	Sim	6
P8	45 a 59 anos	F	Graduação	DF	DF	Sim	6
P9	30 a 44 anos	M	Pós-Graduação	BA	PB	Sim	6
P10	30 a 44 anos	M	Pós-Graduação	PE	PE	Sim	6
P11	45 a 59 anos	F	Pós-Graduação	RJ	RJ	Sim	7
P12	30 a 44 anos	M	Graduação	MG	SP	Sim	7
P13	45 a 59 anos	M	Pós-Graduação	ES	RJ	Sim	7
P14	45 a 59 anos	F	Pós-Graduação	MG	MG	Sim	7
P15	15 a 29 anos	F	Ensino Médio	BA	BA	Sim	7
P16	15 a 29 anos	F	Ensino Médio	TO	TO	Sim	7
P17	30 a 44 anos	M	Graduação	RS	RS	Sim	6
P18	45 a 59 anos	F	Pós-Graduação	PR	PR	Sim	4
P19	45 a 59 anos	M	Pós-Graduação	MG	DF	Sim	6
P20	Acima de 60 anos	M	Graduação	RJ	RJ	Sim	7
P21	45 a 59 anos	M	Pós-Graduação	CE	AL	Sim	5
P22	15 a 29 anos	F	Graduação	RJ	RJ	Sim	6
P23	30 a 44 anos	M	Graduação	SP	SP	Sim	6
P24	30 a 44 anos	M	Pós-Graduação	MG	SC	Sim	7
P25	45 a 59 anos	F	Pós-Graduação	MA	MA	Sim	6
P26	Acima de 60 anos	M	Graduação	SP	SP	Sim	6
P27	30 a 44 anos	M	Graduação	RS	RS	Sim	6
P28	45 a 59 anos	M	Pós-Graduação	MG	ES	Sim	7
P29	45 a 59 anos	F	Pós-Graduação	AM	AM	Sim	5
P30	30 a 44 anos	M	Graduação	RJ	RJ	Sim	7

Quadro 5.3: Dados demográficos dos participantes da pesquisa. (Fonte: o Autor).

Na seção 5.4.2 será apresentada a análise demográfica dos participantes desta pesquisa.

### 5.4.2 Análise Demográfica

O perfil dos participantes da pesquisa foi diversificado. Em relação à distribuição por gênero, observa-se que 60% dos respondentes são do gênero masculino, enquanto 40% pertencem ao gênero feminino, acompanhando a distribuição vista na enquete que originou o recrutamento. No que se refere à faixa etária, a maior concentração está entre os indivíduos de 30 a 44 anos, que representam 43,3% do total, seguidos pela faixa de 45 a

59 anos, com 33,3%. Grupos menores incluem jovens de 15 a 29 anos, que somam 10%, e idosos acima de 60 anos, correspondendo a 13,3%. A Figura 5.3 apresenta esses dados.

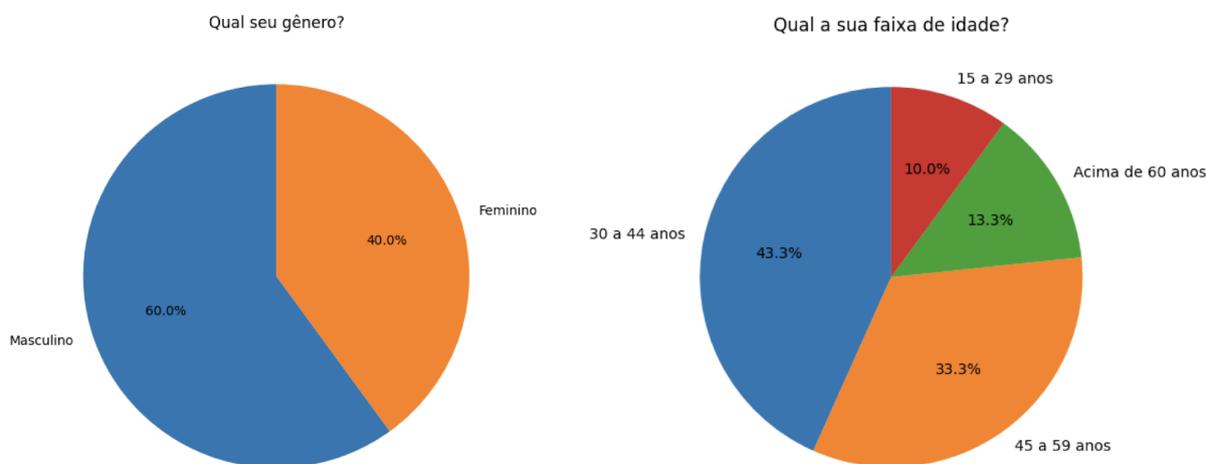


Figura 5.3: Dados de gênero e idade dos participantes (Fonte: O Autor.)

No aspecto educacional, os dados revelam um público predominantemente qualificado. A maioria dos participantes possui pós-graduação, representando 60% do total, enquanto 33,3% são graduados. Apenas uma parcela menor, de 6,7%, declarou ter como grau máximo de instrução o ensino médio. Esse cenário, aliado à predominância de pessoas com menos de 60 anos na pesquisa, pode ter tido influência nos dados relativos à habilidade de uso de soluções de tecnologia. Avaliada na escala SEQ de 1 a 7, a maior concentração dos participantes está nos níveis 6 e 7, indicando que a maioria acha fácil ou muito fácil interagir com essas soluções. A Figura 5.4 apresenta esses cenários de forma consolidada.

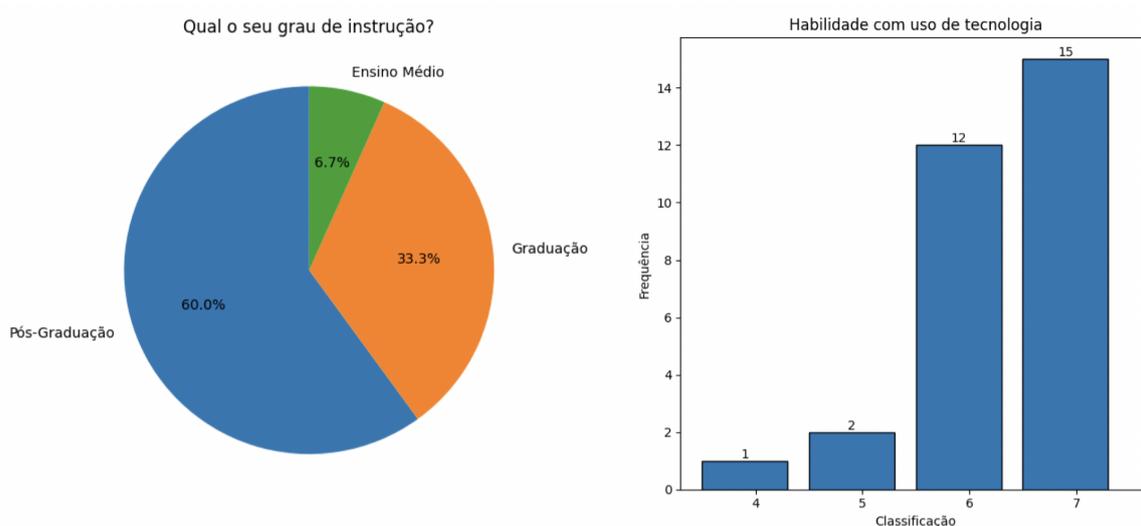


Figura 5.4: Grau de instrução e habilidade com uso de tecnologia dos participantes (Fonte: O Autor.)

Em termos regionais, observa-se que a maior parte dos respondentes nasceu e reside na região Sudeste, correspondendo a 53,3% e 46,7%, respectivamente, evidenciando uma concentração populacional e de residência nessa área. Outras regiões, como Nordeste, Sul, Norte e Centro-Oeste, apresentam distribuições menos expressivas, com destaque para o Nordeste e Sul, que somam 16,7% cada como locais de residência. Essas informações estão alinhadas com a fonte de recrutamento utilizada e confirmaram a hipótese de que usar os dados do Instituto DataSenado conferiria um alcance maior de participantes e daria uma abrangência nacional ao estudo. Os dados completos estão apresentados na Figura 5.5.

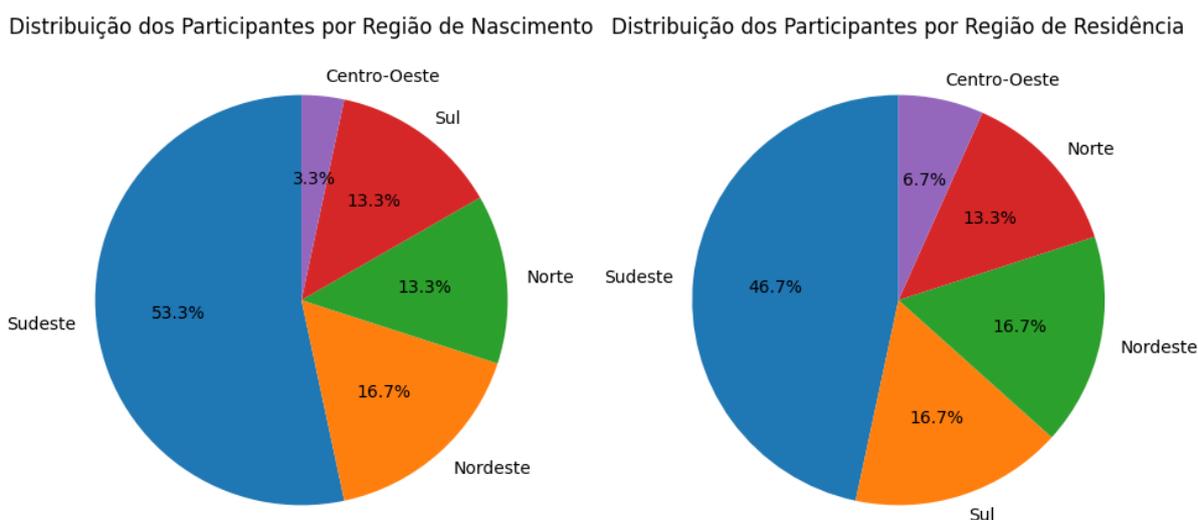


Figura 5.5: Região de nascimento e residência dos participantes (Fonte: O Autor.)

Finalmente, todos os 30 entrevistados já tinham utilizado a *Conta gov.br* para se autenticar em algum serviço fornecido pelo Poder Público. Essa característica gera um ponto de atenção, pois deixa de fora da análise o ponto de vista das pessoas que não conhecem o mecanismo, e que poderiam influenciar nos quesitos de usabilidade medidos.

Os dados coletados no questionário preenchido pelos participantes, assim como as análises iniciais dos mesmos, serão apresentados na seção 5.5.

## 5.5 Resultados

Procederemos com a análise das métricas de usabilidade definidas no modelo proposto no Capítulo 4, passando pelo indicador de Usabilidade geral, medida pelo SUS, pela Facilidade Percebida, mensurada pelo SEQ, e finalizando com o Tempo de Conclusão da Tarefa.

### 5.5.1 Usabilidade geral (SUS)

Os registros dos dois formulários de teste foram mesclados em um conjunto de dados unificado para permitir a análise. As Tabelas 5.1 e 5.2 ilustram qual foi a pontuação de cada uma das perguntas do questionário SUS para o cenário de login usando o E-mail e Senha e a *Conta gov.br* respectivamente. Além das respostas de cada questão, nomeadas de Q1 até Q10, há também o resultado do cálculo do SUS de cada participante.

Para analisar as múltiplas facetas que esses números trazem, vamos utilizar como base a pesquisa conduzida por Blattgerste et al. [138]. Nesse estudo, os autores avaliam diversas soluções de cálculo e interpretação do SUS e propõem uma ferramenta de código aberto que permite contextualizar e visualizar os resultados das medições que usam o método com foco na comunidade acadêmica e científica.

A ferramenta, denominada *SUS Analysis Toolkit* e disponível no endereço <https://sus.mixality.de/>, também permite a comparação multivariável, ou seja, agregar medições da *System Usability Scale* de diferentes soluções ou cenários e agregar os dados de forma que seja possível confrontar os resultados. E, pra concluir, ela também facilita o cálculo de estatísticas inferenciais, de forma que seja possível determinar, por exemplo, se a diferença média entre duas medições é estatisticamente significativa.

Ao consolidar as informações e enviar para análise, os dados estatísticos constantes na Tabela 5.3 foram calculados. Importante frisar que já foi feita a classificação por adjetivos, proposta por Bangor et al. [81] e apresentada na seção 2.3.4, e que permite uma interpretação mais simples dos números obtidos.

Uma das opções de ilustração desses dados é o gráfico de caixa (*boxplot*), uma vez que apresenta a distribuição de um conjunto de dados numéricos destacando informações como dispersão, mediana e possíveis valores muito fora do padrão (*outliers*). Ao apresentar cenários distintos de forma agrupada, é possível fazer a comparação visual das circunstâncias representadas. No caso em tela, o resultado da Tabela 5.3 deu origem ao gráfico da Figura 5.6.

Participante	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS
P1	5	1	5	1	5	1	5	1	4	1	97,5
P2	4	1	5	1	5	1	5	3	5	1	92,5
P3	5	1	5	1	1	1	1	1	5	1	80,0
P4	5	3	5	1	4	1	4	1	5	1	90,0
P5	2	1	5	5	5	1	3	1	5	5	67,5
P6	5	2	4	4	5	1	4	1	5	1	85,0
P7	4	1	5	1	5	1	5	1	4	1	95,0
P8	5	1	5	1	5	1	5	1	5	5	90,0
P9	5	1	5	1	5	1	5	1	5	1	100,0
P10	5	1	5	3	5	1	5	1	5	5	85,0
P11	1	3	4	1	5	1	5	3	3	1	72,5
P12	4	2	5	1	3	1	5	1	4	1	87,5
P13	5	3	4	2	5	1	4	1	5	1	87,5
P14	5	1	5	1	5	1	5	1	5	1	100,0
P15	3	1	5	1	5	1	3	1	3	1	85,0
P16	4	1	5	3	5	1	5	1	5	1	92,5
P17	5	1	5	1	5	1	5	1	4	1	97,5
P18	5	1	5	1	5	1	5	1	3	1	95,0
P19	5	1	5	1	5	1	5	1	4	1	97,5
P20	5	1	5	1	5	2	3	2	5	4	82,5
P21	5	4	4	2	4	4	4	3	4	4	60,0
P22	4	1	5	1	4	1	5	1	2	1	87,5
P23	5	1	5	1	5	1	4	1	4	1	95,0
P24	5	2	5	1	5	1	5	1	5	1	97,5
P25	3	2	3	1	3	2	2	2	4	2	65,0
P26	4	1	5	2	5	2	4	2	5	1	87,5
P27	5	1	5	1	5	1	5	1	5	1	100,0
P28	5	1	5	1	2	1	1	1	5	1	82,5
P29	2	1	5	1	5	1	5	1	5	1	92,5
P30	5	1	5	1	5	1	5	1	5	1	100,0

Tabela 5.1: Respostas SUS - Cenário E-mail e Senha. (Fonte: o Autor).

Participante	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS
P1	5	1	5	1	5	1	5	1	4	1	97,5
P2	5	1	5	1	5	1	5	1	5	2	97,5
P3	5	1	5	1	5	1	5	1	5	1	100,0
P4	3	2	4	1	3	3	2	1	2	1	65,0
P5	5	4	4	4	5	1	5	1	5	4	75,0
P6	5	3	4	4	5	2	4	1	5	2	77,5
P7	5	2	4	1	4	1	4	1	3	1	85,0
P8	5	1	5	2	5	1	5	1	1	5	77,5
P9	5	1	5	1	5	1	5	1	5	1	100,0
P10	5	1	5	3	5	1	5	1	5	5	85,0
P11	5	1	5	1	5	1	5	1	5	1	100,0
P12	3	4	2	1	2	3	4	1	4	1	62,5
P13	5	1	5	1	5	1	5	1	5	1	100,0
P14	5	1	5	1	5	1	4	5	5	3	82,5
P15	5	1	5	1	5	1	3	1	5	1	95,0
P16	5	1	5	3	5	1	1	1	5	3	80,0
P17	5	1	5	1	5	1	5	1	4	1	97,5
P18	5	1	5	1	5	1	5	1	3	1	95,0
P19	5	1	5	1	5	1	4	1	4	1	95,0
P20	5	1	5	1	5	4	3	2	5	4	77,5
P21	5	1	4	1	4	4	3	3	4	2	72,5
P22	4	1	5	1	4	1	5	1	5	1	95,0
P23	5	2	4	1	4	1	5	1	4	1	90,0
P24	5	1	5	1	5	1	5	1	5	1	100,0
P25	3	4	3	2	4	2	3	2	3	2	60,0
P26	5	2	4	2	5	4	4	2	5	1	80,0
P27	5	5	5	1	5	1	4	1	5	1	87,5
P28	5	1	5	1	5	2	5	1	4	1	95,0
P29	5	2	5	3	5	2	5	2	5	3	82,5
P30	5	1	5	1	5	2	5	1	5	1	97,5

Tabela 5.2: Respostas SUS - Cenário *Conta gov.br*. (Fonte: o Autor).

Estatística	Conta gov.br	E-mail
Média do SUS	86,83	88,25
Desvio Padrão	12,03	10,63
Min	60,0	60,0
Max	100,0	100,0
1º Quartil	77,5	84,375
Mediana	88,75	90,0
3º Quartil	97,5	97,5
Escala Adjetivo	<i>Best Imaginable</i>	<i>Best Imaginable</i>

Tabela 5.3: Estatísticas descritivas do SUS por cenário. (Fonte: O Autor.)

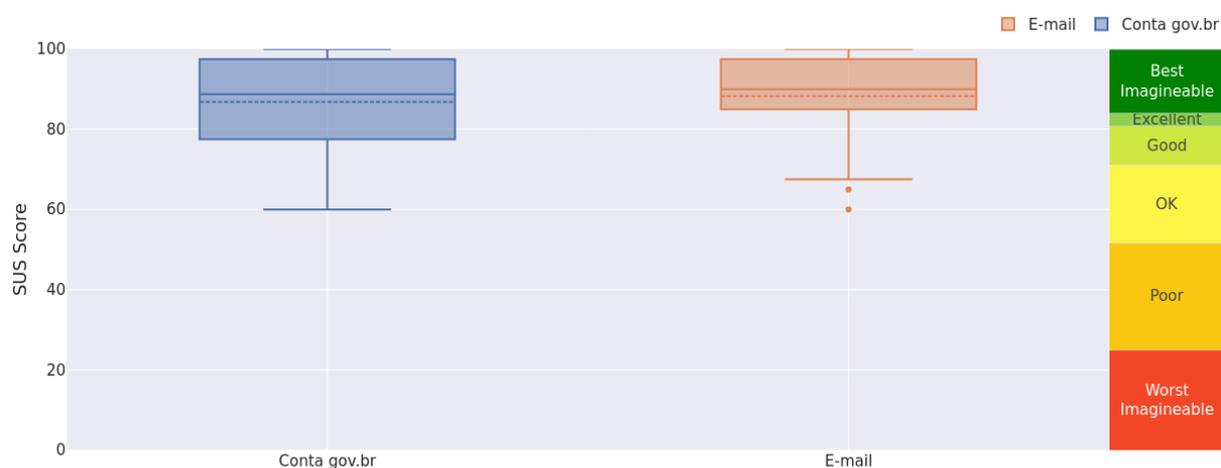


Figura 5.6: Dados estatísticos da medição do SUS. (Fonte: O Autor.)

Analisando as informações, é possível perceber que a mediana do cenário com E-mail e Senha é levemente superior a da **Conta gov.br**, sugerindo uma percepção ligeiramente melhor para o primeiro cenário. O gráfico também mostra que o intervalo interquartil da **Conta gov.br** é maior, indicando maior variabilidade na percepção de usabilidade desse mecanismo. Apesar dessa variedade, os dois contextos apresentaram a mesma escala de adjetivo, sugerindo que não houve, em termos de usabilidade, diferença para os participantes do estudo nesse quesito.

Outra forma de visualizar os dados é através do valor do percentil, uma maneira proposta por Sauro e Lewis [88] para comparação do SUS obtido com outros sistemas. Para isso, foi utilizada uma base de 446 estudos, que continham mais de 5.000 respostas individuais do SUS, as quais foram mapeadas para uma tabela de referência de percentis. Ao utilizar o escore bruto do SUS de algum estudo, é possível encontrar o percentil

correspondente àquele valor e verificar como aquele resultado se posiciona em relação aos outros. O *SUS Toolkit* fez a análise que está ilustrada na Figura 5.7.

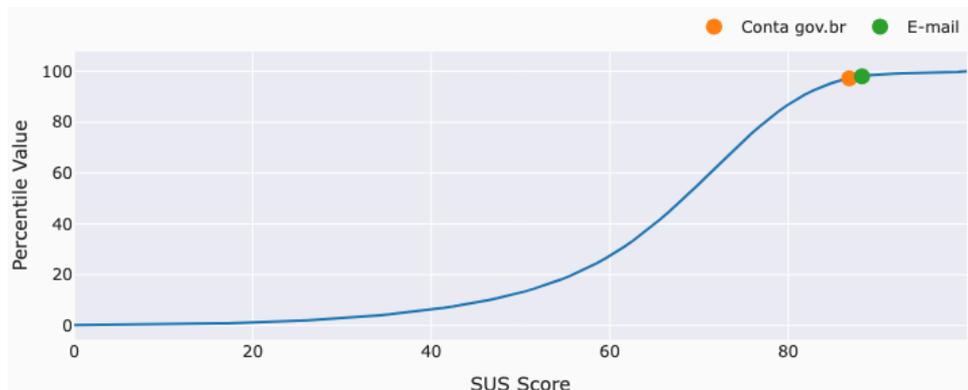


Figura 5.7: Comparação de percentis entre a *Conta gov.br* e o Email e Senha. (Fonte: O Autor.)

O gráfico sugere que, em termos de usabilidade, a distinção entre os dois mecanismos é muito pequena. Para verificar se essa diferença é ou não estatisticamente significativa, é possível utilizar o *SUS Statistics Calculator*, ferramenta integrante da solução desenvolvida por Blattgerste et al. [138] e disponível no endereço <https://statistics.sus.tools/>. De forma similar ao processo de análise do SUS, os dados do estudo são enviados para o site, que valida algumas condições para determinar como fazer o teste, a saber:

1. Se o estudo tem amostras dependentes ou independentes.
2. O tamanho das amostras, para determinação do tipo de teste (paramétrico ou não-paramétrico).
3. Normalidade da diferença entre as medições pareadas (resíduos).
4. Existência de *outliers* nos resíduos.

No caso em tela, temos amostras dependentes, pois a comparação intra-sujeitos implica que os participantes opinaram em todos os cenários analisados. O tamanho da amostra (30) sugere o uso de um teste paramétrico, uma vez que esse número é o limiar para uma distribuição normal, condição necessária para o uso desse teste. Essa suspeita é confirmada através do teste de Shapiro-Wilk [139], que não indicou variação significativa da normalidade dos resíduos ( $W(30) = 0,98$ ,  $p = 0,86$ ). Finalmente, não houve *outliers* significativos na amostra.

Diante dos resultados, a solução utilizou o Teste T Pareado para testar a hipótese da existência de diferença significativa entre os dois cenários apresentados. Essa linha de ação está consoante com a proposta por Sauro e Lewis [88] para comparação de escores do

SUS, e determinou que não há uma divergência relevante ( $t(29) = -0,64$ ,  $p = 0,5258$ ). O Intervalo de Confiança para a diferença média vai de  $-5,93$  a  $3,09$ , indicando que o intervalo observado pode variar dentro dessa faixa. Concluindo, o Índice do Tamanho do Efeito ( $d$  de Cohen [140]), medida que permite avaliar de forma relativa o tamanho da diferença entre as médias, foi  $d = 0,12$ , o que o classifica como um Tamanho de Efeito Muito Pequeno, indicando que a diferença é irrelevante.

Adicionalmente, o *SUS Analysis Toolkit* permite verificar como cada questão do SUS impactou na usabilidade geral. Para isso, as respostas são normalizadas em uma escala de 0 a 10, incluindo os itens com viés negativo, de forma que a comparação e a interpretação sejam facilitadas, uma vez que valores altos sempre representam melhor usabilidade. Os dados resultantes estão na Tabela 5.4 e podem ser visualizados no gráfico da Figura 5.8.

Questão	Conta gov.br		E-mail	
	Valor	Desvio Padrão	Valor	Desvio Padrão
Q1	9,42	1,54	8,33	2,69
Q2	8,33	2,84	8,92	2,01
Q3	9,00	1,78	9,50	1,19
Q4	8,75	2,30	8,83	2,48
Q5	9,17	1,75	8,83	2,48
Q6	8,50	2,47	9,50	1,50
Q7	8,17	2,58	8,08	2,94
Q8	9,17	2,07	9,25	1,60
Q9	8,33	2,53	8,58	2,01
Q10	8,00	3,12	8,42	3,38

Tabela 5.4: Contribuições por questão respondida para a *Conta gov.br* e E-mail. (Fonte: o Autor).

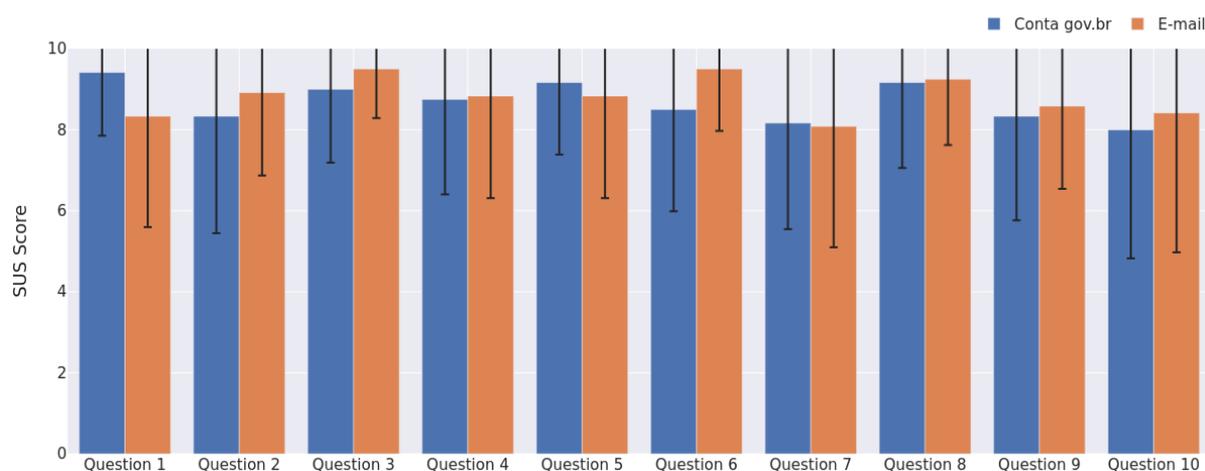


Figura 5.8: Impacto de cada pergunta para a avaliação de usabilidade da *Conta gov.br* e do Email e Senha. (Fonte: O Autor.)

O gráfico nos permite averiguar, de forma visual, que realmente existiu um equilíbrio nas avaliações dos dois mecanismos de login. Há, entretanto, uma ligeira vantagem para o uso do E-mail e Senha nas questões de número 2 (“Eu achei esse sistema desnecessariamente complexo.”), 3 (“Eu achei esse sistema fácil de usar.”), 6 (“Eu acho que o sistema apresenta muita inconsistência.”) e 10 (“Eu precisei aprender muitas coisas antes que pudesse utilizar esse sistema.”), sugerindo que é mais simples e fácil usar uma credencial de e-mail e senha do que passar pelo processo de autenticação da *Conta gov.br*, diminuindo a chance de inconsistências afetarem o processo. Há também a indicação de que os participantes já estão bastante habituados com o processo de usar um nome de usuário e senha para acessar serviços na Internet.

Em contrapartida, a *Conta gov.br* foi melhor avaliada nas questões de número 1 (“Eu acho que gostaria de usar esse sistema frequentemente.”) e 5 (“Eu achei que as várias funções desse sistema foram bem integradas.”), apontando que, mesmo que o processo de e-mail e senha seja mais simples, a aceitação da *Conta gov.br* é boa, e o fluxo que é apresentado para realizar a autenticação se encaixa bem ao e-Cidadania.

Discutiremos, na seção 5.5.1, a confiabilidade e consistência dos dados coletados no questionário SUS.

### Análise de confiabilidade usando o Alfa de Cronbach

Dentro do modelo proposto na seção 4.1, está prevista a verificação da confiabilidade das respostas utilizando o Alfa de Cronbach ( $\alpha$ ), índice que foi abordado no Capítulo 2 e que mede a consistência interna dos dados que foram coletados nos questionários, definindo como 0,7 o limiar para um conjunto consistente de dados.

Importante frisar que a análise de questionários que possuem perguntas com viés diferentes, como é o caso do SUS, precisam ter suas escalas invertidas, de forma que os valores sejam orientados na mesma direção, como afirma Solis Salazar [141]. Desta forma, as perguntas pares, que possuem essa característica, devem ser normalizadas. Isso é feito subtraindo o valor da resposta do número 6, de forma que uma resposta com valor 1 (discordo totalmente) se torne 5 (concordo totalmente). Os valores resultantes da normalização estão apresentados nas Tabelas 5.5 e 5.6.

Para realizar o cálculo do índice, foi utilizada a biblioteca `pinguin` [142], um pacote de código aberto escrito em Python que disponibiliza várias funções estatísticas, sendo que a análise de consistência usando o Alfa de Cronbach é uma delas. Ao alimentar a ferramenta com os dados normalizados, encontramos resultados abaixo do índice aceitável, conforme mostrado a seguir:

$$\alpha_{\text{E-mail e Senha}} = 0,5631 \quad (\text{IC } 95\%: [0,287; 0,763])$$

$$\alpha_{\text{Conta gov.br}} = 0,6735 \quad (\text{IC } 95\%: [0,467; 0,823])$$

Como podemos verificar, nenhum dos cenários apresentou uma confiabilidade satisfatória ( $\alpha \geq 0,7$ ), o que nos levou a buscar as razões para o desfecho observado. Dentre algumas das opções existentes, temos:

1. Inconsistência do questionário: caso as perguntas que compõem o questionário não meçam um único conceito, como a usabilidade, não haverá uma alta correlação entre os itens.
2. Resposta inconsistente em relação ao padrão geral: participantes anteriores deram respostas semelhantes e a nova resposta inclui valores muito diferentes.
3. Variância total aumentada: se a nova resposta tem uma combinação de valores extremos que altera significativamente a soma total.
4. Erros de preenchimento ou viés: respostas preenchidas de forma aleatória, por engano ou com viés diminuem a consistência interna.

De início, podemos descartar o item 1, uma vez que a tradução do questionário SUS utilizada teve sua consistência interna validada, obtendo um valor de 0,76 [80]. Já as alternativas restantes são plausíveis e podem conter a explicação do resultado aferido. A fim de investigar essas possibilidades, decidimos verificar como o valor do índice variava à medida que as respostas eram computadas. Os dados do cenário de E-mail e Senha estão apresentados na Figura 5.9, enquanto a evolução do indicador no cenário da **Conta gov.br** pode ser visualizada na Figura 5.10.

<b>Participante</b>	<b>Q1</b>	<b>Q2</b>	<b>Q3</b>	<b>Q4</b>	<b>Q5</b>	<b>Q6</b>	<b>Q7</b>	<b>Q8</b>	<b>Q9</b>	<b>Q10</b>
P1	5	5	5	5	5	5	5	5	4	5
P2	4	5	5	5	5	5	5	3	5	5
P3	5	5	5	5	1	5	1	5	5	5
P4	5	3	5	5	4	5	4	5	5	5
P5	2	5	5	1	5	5	3	5	5	1
P6	5	4	4	2	5	5	4	5	5	5
P7	4	5	5	5	5	5	5	5	4	5
P8	5	5	5	5	5	5	5	5	5	1
P9	5	5	5	5	5	5	5	5	5	5
P10	5	5	5	3	5	5	5	5	5	1
P11	1	3	4	5	5	5	5	3	3	5
P12	4	4	5	5	3	5	5	5	4	5
P13	5	3	4	4	5	5	4	5	5	5
P14	5	5	5	5	5	5	5	5	5	5
P15	3	5	5	5	5	5	3	5	3	5
P16	4	5	5	3	5	5	5	5	5	5
P17	5	5	5	5	5	5	5	5	4	5
P18	5	5	5	5	5	5	5	5	3	5
P19	5	5	5	5	5	5	5	5	4	5
P20	5	5	5	5	5	4	3	4	5	2
P21	5	2	4	4	4	2	4	3	4	2
P22	4	5	5	5	4	5	5	5	2	5
P23	5	5	5	5	5	5	4	5	4	5
P24	5	4	5	5	5	5	5	5	5	5
P25	3	4	3	5	3	4	2	4	4	4
P26	4	5	5	4	5	4	4	4	5	5
P27	5	5	5	5	5	5	5	5	5	5
P28	5	5	5	5	2	5	1	5	5	5
P29	2	5	5	5	5	5	5	5	5	5
P30	5	5	5	5	5	5	5	5	5	5

Tabela 5.5: Respostas SUS com perguntas de viés negativo normalizadas - Cenário E-mail e Senha.

Participante	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
P1	5	5	5	5	5	5	5	5	4	5
P2	5	5	5	5	5	5	5	5	5	4
P3	5	5	5	5	5	5	5	5	5	5
P4	3	4	4	5	3	3	2	5	2	5
P5	5	2	4	2	5	5	5	5	5	2
P6	5	3	4	2	5	4	4	5	5	4
P7	5	4	4	5	4	5	4	5	3	5
P8	5	5	5	4	5	5	5	5	1	1
P9	5	5	5	5	5	5	5	5	5	5
P10	5	5	5	3	5	5	5	5	5	1
P11	5	5	5	5	5	5	5	5	5	5
P12	3	2	2	5	2	3	4	5	4	5
P13	5	5	5	5	5	5	5	5	5	5
P14	5	5	5	5	5	5	4	1	5	3
P15	5	5	5	5	5	5	3	5	5	5
P16	5	5	5	3	5	5	1	5	5	3
P17	5	5	5	5	5	5	5	5	4	5
P18	5	5	5	5	5	5	5	5	3	5
P19	5	5	5	5	5	5	4	5	4	5
P20	5	5	5	5	5	2	3	4	5	2
P21	5	5	4	5	4	2	3	3	4	4
P22	4	5	5	5	4	5	5	5	5	5
P23	5	4	4	5	4	5	5	5	4	5
P24	5	5	5	5	5	5	5	5	5	5
P25	3	2	3	4	4	4	3	4	3	4
P26	5	4	4	4	5	2	4	4	5	5
P27	5	1	5	5	5	5	4	5	5	5
P28	5	5	5	5	5	4	5	5	4	5
P29	5	4	5	3	5	4	5	4	5	3
P30	5	5	5	5	5	4	5	5	5	5

Tabela 5.6: Respostas SUS com perguntas de viés negativo normalizadas - Cenário *Conta gov.br*.

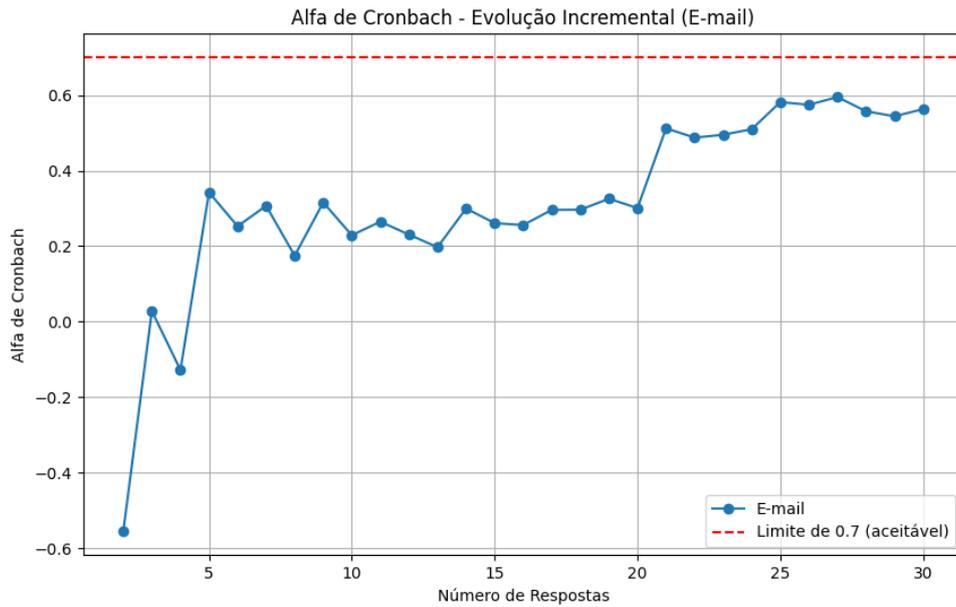


Figura 5.9: Análise incremental do Alfa de Cronbach - E-mail e Senha. (Fonte: O Autor.)

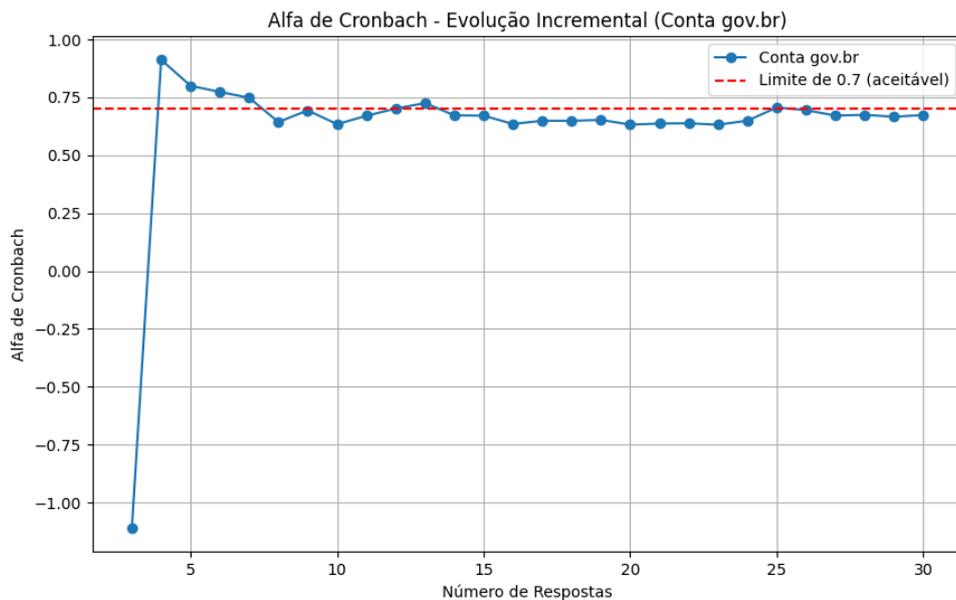


Figura 5.10: Análise incremental do Alfa de Cronbach - *Conta gov.br*. (Fonte: O Autor.)

Ao comparar as duas imagens, observa-se que as respostas dos participantes na autenticação via E-mail e Senha apresentaram maior variação do que na autenticação pela *Conta gov.br*. Essa diferença resultou em um valor global mais alto para este último cenário (0,6735) em comparação ao primeiro (0,5631).

É possível, também, analisar a influência de respostas discrepantes no cálculo do Alfa de Cronbach. Ao utilizar os dados do cenário E-mail e Senha após a resposta 25 (ponto

escolhido por indicar uma estabilização do índice), observamos uma queda abrupta entre as respostas 27 e 28. Olhando os dados brutos, percebemos que há uma diferença significativa entre as respostas das Questões 5 (P27: 5; P28: 2) e 7 (P27: 5; P28: 1). A queda continua entre as questões 28 e 29, com a discrepância ocorrendo entre as Questões 1 (P28: 5; P29: 2), 5 (P28: 2; P29: 5) e 7 (P28: 1; P29: 5). Esse comportamento sugere que essas diferenças realmente afetam o indicador.

Isso nos leva a ponderar sobre a motivação dessa diferença. Uma visão rasa nos levaria a concluir que poderia ter havido algum erro no preenchimento das respostas, conforme aventado na lista de possibilidades que foi vista anteriormente. Porém, uma especificidade no nosso estudo exige um olhar mais apurado, pois o uso do Alfa de Cronbach na mensuração de usabilidade pode ser problemático, segundo Schrepp [143].

Em seu estudo, o autor pondera que as respostas dadas em questionários que medem a usabilidade são subjetivas, baseadas na experiência única do usuário que executou o teste. Desta forma, não há como classificar uma resposta como “errada” ou “certa”, mas sim, que ela se desvia do padrão das respostas dadas pelos outros participantes. Esse pensamento é corroborado por Streiner [144], que afirma que nem todas as formas de teste de confiabilidade podem ser usadas para todos os tipos de medidas.

Com base nessas evidências, assumimos que, mesmo que o Alfa de Cronbach não tenha atingido o limiar aceitável, não há razão para classificá-los como uma inconsistência, mas sim, como uma característica do estudo. O próprio Schrepp [143] demonstrou que a quantidade de amostras influencia o valor computado para o índice, sugerindo que um número maior de respostas poderia levar o Alfa a um patamar posterior a 0,7.

Daremos continuidade à apresentação das outras métricas de usabilidade definidas, analisando na seção 5.5.2 os dados da Facilidade Percebida de Uso.

### 5.5.2 Facilidade Percebida de Uso (SEQ)

Conforme explicado na seção 4, a forma de medição da facilidade de uso dos dois cenários foi a pergunta *Single Ease Question*, onde uma escala Likert de 7 pontos, variando de **Muito Difícil** a **Muito Fácil**, era apresentada aos participantes para que eles definissem a sensação de usar as duas soluções de autenticação. As informações captadas na entrevista estão apresentadas na Tabela 5.7, e as estatísticas descritivas na Tabela 5.8.

ID	Conta gov.br	E-mail e senha	ID	Conta gov.br	E-mail e senha	ID	Conta gov.br	E-mail e senha
P1	7	7	P2	7	7	P3	7	7
P4	7	7	P5	6	5	P6	6	6
P7	6	7	P8	6	7	P9	7	7
P10	7	7	P11	7	7	P12	6	7
P13	7	6	P14	7	7	P15	7	7
P16	7	7	P17	7	7	P18	7	7
P19	7	7	P20	7	7	P21	6	6
P22	7	7	P23	7	7	P24	7	7
P25	5	6	P26	7	6	P27	7	7
P28	6	7	P29	6	7	P30	7	7

Tabela 5.7: Respostas à pergunta SEQ para aferição da Facilidade Percebida. (Fonte: o Autor).

Estatística	Conta gov.br	E-mail e senha
Média do SEQ	6,67	6,77
Desvio Padrão	0,55	0,50
Min	5,00	5,00
Max	7,00	7,00
1º Quartil	6,00	7,00
Mediana	7,00	7,00
3º Quartil	7,00	7,00

Tabela 5.8: Estatísticas descritivas do SEQ para *Conta gov.br* e E-mail e senha. (Fonte: o Autor).

Para a ilustração dessas informações, quando valores contínuos de categorias discretas são comparados, Albert e Tullis [69] sugerem o uso de um gráfico de barras contendo o intervalo de confiança, ou seja, a faixa de valores onde a média dos dados provavelmente está. Usando como critério um intervalo de 95%, obtemos a ilustração da Figura 5.11.

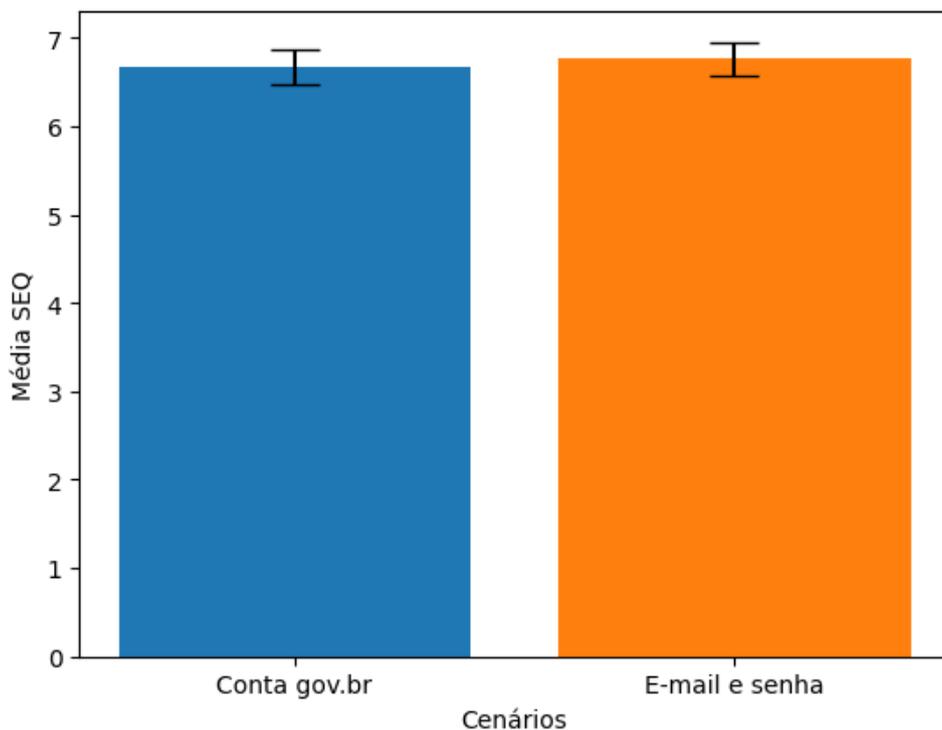


Figura 5.11: Média do SEQ para os cenários testados. (Fonte: O Autor.)

Os dados sugerem que não houve uma diferença na percepção de facilidade de uso das duas maneiras de autenticação. Para confirmar essa hipótese, convém validar se a diferença é estatisticamente significativa. De forma análoga ao que foi feito com a pontuação do SUS, vamos verificar se é possível fazer um Teste T Pareado.

A primeira checagem a ser feita, como vimos na seção 5.5.1, é da normalidade dos resíduos entre as duas amostras. Aplicando o teste de Shapiro-Wilk na diferença das medições entre a *Conta gov.br* e o cenário de E-mail e senha, temos como resultado  $W(30) = 0,7210$ ,  $p = 0,000032$ . Como  $p \leq 0,05$ , rejeitamos a hipótese nula de que os resíduos seguem uma distribuição normal. Essa característica pode decorrer do fato de que as respostas têm baixa variação, uma vez que estão concentradas nos valores 6 e 7.

Nas condições apresentadas, em que as amostras são pareadas e que não há distribuição normal, Bordens e Abbott [134] indicam o uso de testes não-paramétricos, em particular o Teste de Wilcoxon de Postos Sinalizados. Aplicando o teste com as informações coletadas, encontramos a estatística  $Z = 15,0$ ,  $p = 0,3173$ , indicando que a diferença observada não é estatisticamente significativa ( $p > 0,05$ ) e, concluindo que, para os participantes do estudo, não houve diferença prática na Facilidade Percebida para o uso dos dois mecanismos de autenticação.

Os dados relativos ao Tempo de Conclusão da tarefa, último indicador de usabilidade definido para nosso estudo, serão apresentados na seção 5.5.3.

### 5.5.3 Tempo de Conclusão da Tarefa (TCT)

O Tempo de Conclusão da Tarefa, como visto na seção 2.4.2, fornece uma dimensão relativa à eficiência que uma determinada solução possui. A diferença entre os cenários do uso de E-mail e Senha e da **Conta gov.br** nos permitirá comparar as duas situações. A fronteira definida para isso será a apresentação da tela de login e da correspondente tela de sucesso de autenticação.

É importante ressaltar que houve uma pequena atualização no layout do sistema no mês de outubro de 2024, de forma que a tela de login usando E-mail e Senha, assim como as telas de sucesso de autenticação dos dois cenários analisados, sofreram alterações. O resultado disso é que temos conjuntos diferentes de telas para os participantes que realizaram o teste até setembro (P1 a P18) e os que fizeram a entrevista nos meses finais de 2024 (P19 a P30). As telas consideradas são apresentadas nas Figuras 5.12 a 5.18.

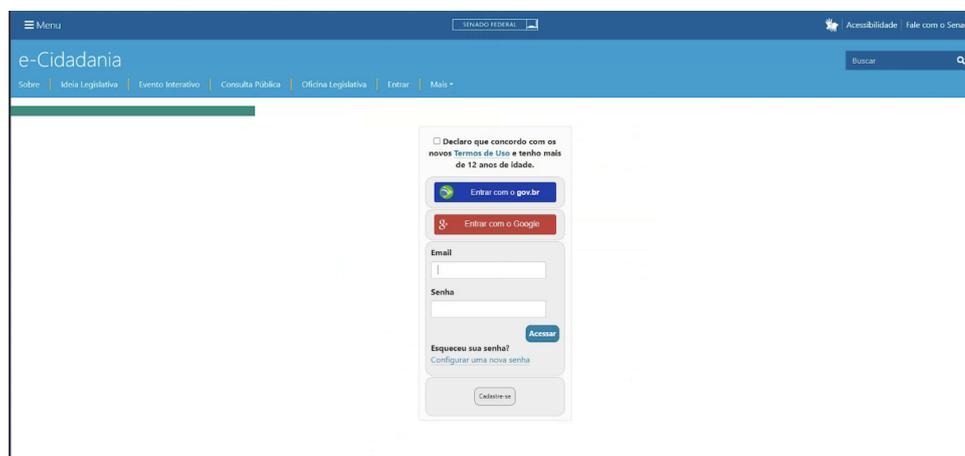


Figura 5.12: Tela de login - E-mail e Senha - Anterior. (Fonte: O Autor.)



Figura 5.13: Tela de login - E-mail e Senha - Atual. (Fonte: O Autor.)



Figura 5.14: Tela de login - *Conta gov.br*. (Fonte: O Autor.)

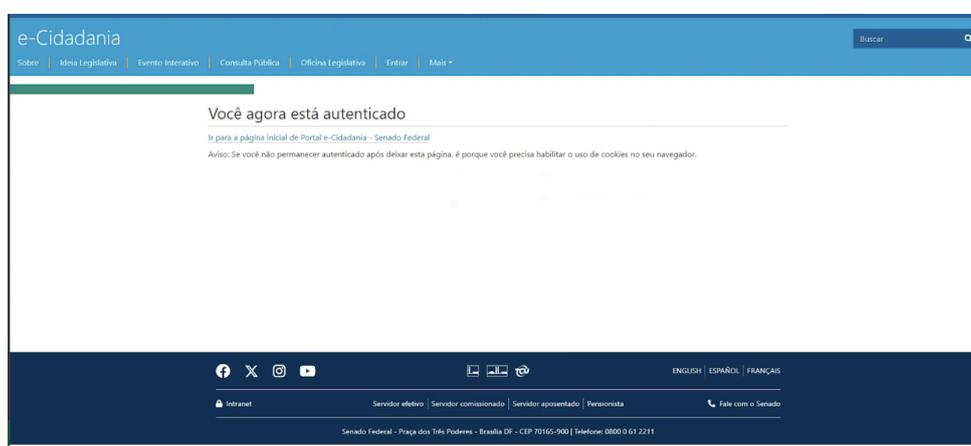


Figura 5.15: Tela de sucesso - E-mail e Senha - Anterior. (Fonte: O Autor.)

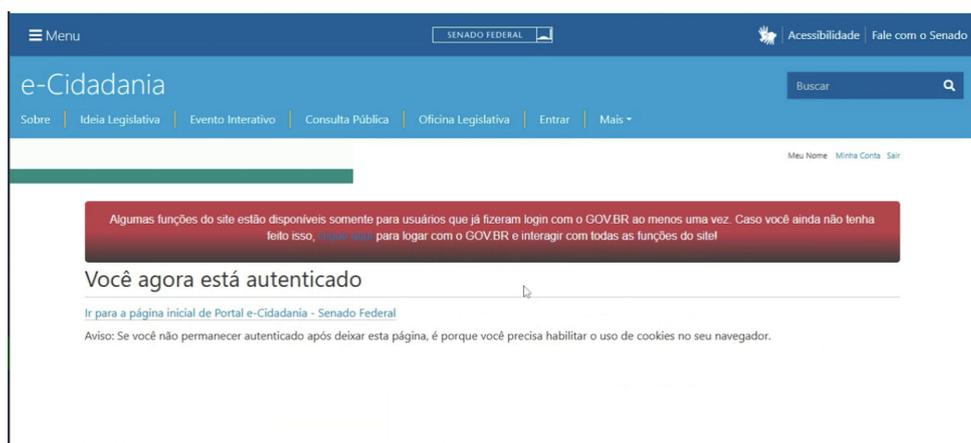


Figura 5.16: Tela de sucesso - E-mail e Senha - Atual. (Fonte: O Autor.)

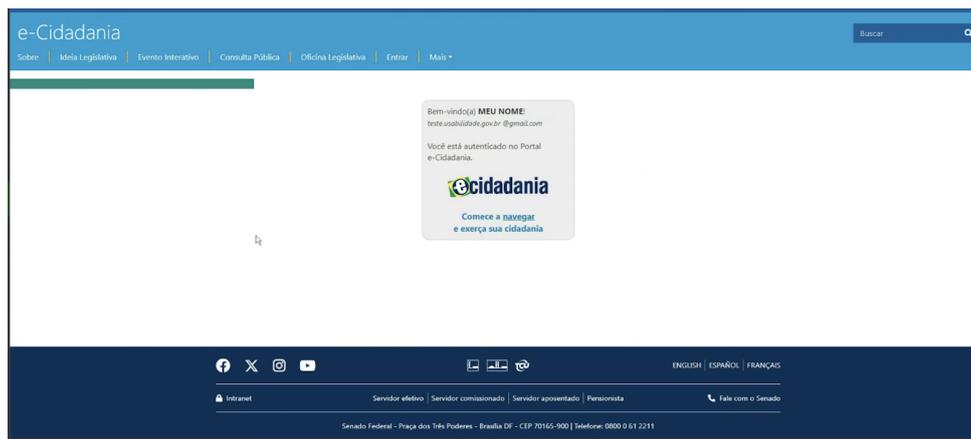


Figura 5.17: Tela de sucesso - *Conta gov.br* - Anterior. (Fonte: O Autor.)



Figura 5.18: Tela de sucesso - *Conta gov.br* - Atual. (Fonte: O Autor.)

Como não foi possível modificar o código-fonte do sistema e-Cidadania para incluir uma lógica que registrasse quando essas páginas fossem acessadas, a solução encontrada foi utilizar a gravação das entrevistas para identificar quando esses momentos ocorreram. A ferramenta selecionada para isso foi o *VLC Media Player* [145], em conjunto com seu plugin *Jump to time Previous frame v3* [146], já que esse plugin permite identificar, com precisão de milissegundos, qual o instante está sendo apresentado na tela.

Para facilitar a identificação das páginas nos vídeos, foi desenvolvido um *script* utilizando a biblioteca *OpenCV* [147] que calcula a diferença entre quadros nas entrevistas gravadas. Em teoria, isso permitiria detectar com maior precisão as transições entre páginas. A abordagem considera que pequenas diferenças ocorrem ao rolar a mesma página (como ao ler um formulário), enquanto grandes variações indicam mudanças de aba ou a submissão de login para validação. Essa hipótese está ilustrada na Figura 5.19, referente ao participante P1, que mostra como a variação de quadros ocorre no decorrer do tempo, e destaca quando os eventos de login e sucesso ocorreram para cada um dos cenários.

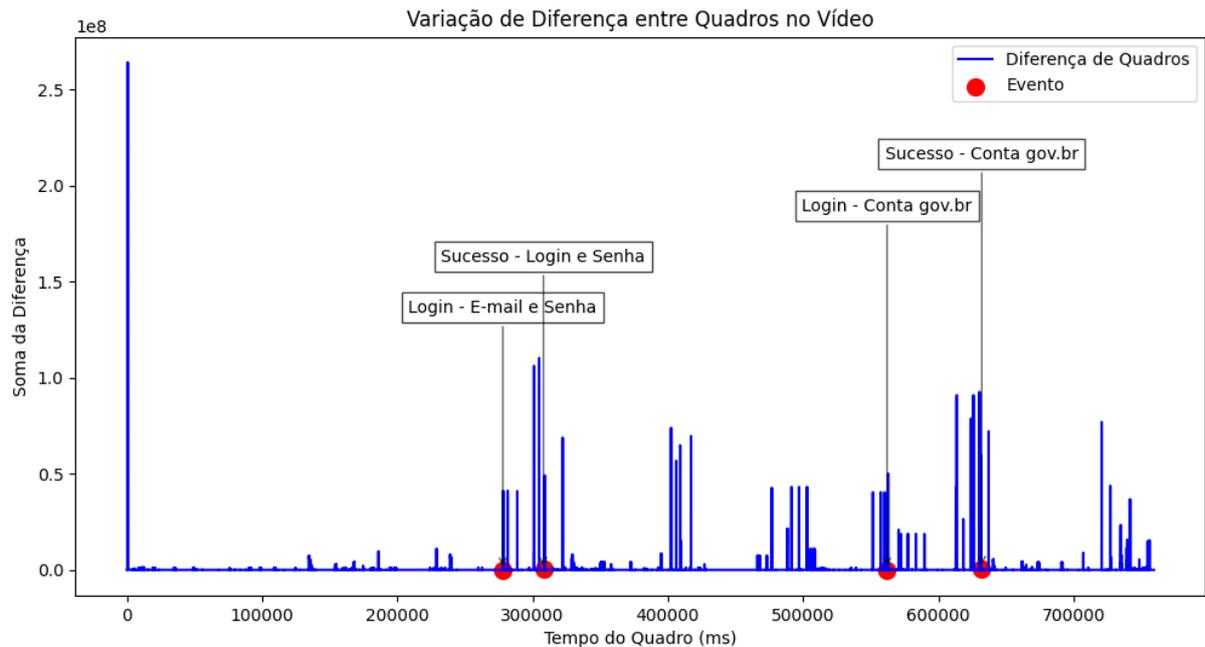


Figura 5.19: Diferença entre quadros no decorrer do tempo - Participante P1. (Fonte: O Autor.)

O algoritmo, desenvolvido usando a linguagem Python, analisou cada um dos vídeos e gerou uma planilha contendo os tempos em milissegundos, o tempo em formato legível (minutos e segundos) e a diferença do quadro. Há também um parâmetro que define um limiar mínimo, de forma que apenas os dados mais relevantes sejam incluídos nesse relatório. No caso concreto, vendo os resultados do participante P1, definimos essa fronteira como 270.000, já que era o valor onde todos os quadros relevantes apareceram. Com isso, o procedimento para identificar os tempos ficou conforme o descrito a seguir:

1. O vídeo era avançado até o ponto onde a tela de interesse era apresentada.
2. Usando o plugin *Jump to time Previous frame v3*, o tempo exato do quadro era extraído.
3. Esse tempo servia de base para uma pesquisa na planilha correspondente ao participante, onde um tempo anterior ao selecionado com uma diferença alta (maior que 1.000.000) era escolhido e analisado no vídeo.
4. Caso o quadro resultante fosse idêntico ao analisado, os tempos anteriores da planilha eram selecionados até que se encontrasse a fronteira de mudança da página do formulário, buscando encontrar o tempo mais cedo em que a página apareceu.

A análise desses dados levou à confecção da Tabela 5.9, que contém os intervalos para cada participante e a duração de cada um dos cenários em milissegundos. Já as estatísticas descritivas estão na Tabela 5.10.

ID	Tempos - Conta gov.br (ms)			Tempos - E-mail e Senha (ms)		
	Início	Término	$\Delta$	Início	Término	$\Delta$
P1	562.708	632.541	<b>69.833</b>	278.291	318.375	<b>40.084</b>
P2	222.833	248.458	<b>25.625</b>	473.375	484.708	<b>11.333</b>
P3	537.250	565.000	<b>27.750</b>	328.083	348.708	<b>20.625</b>
P4	219.500	272.500	<b>53.000</b>	571.583	618.791	<b>47.208</b>
P5	502.666	551.125	<b>48.459</b>	256.583	269.250	<b>12.667</b>
P6	424.958	487.708	<b>62.750</b>	787.416	825.250	<b>37.834</b>
P7	382.375	428.750	<b>46.375</b>	755.666	859.750	<b>104.084</b>
P8	855.333	939.250	<b>83.917</b>	391.625	409.333	<b>17.708</b>
P9	288.416	331.000	<b>42.584</b>	674.208	699.541	<b>25.333</b>
P10	959.458	1.043.875	<b>84.417</b>	563.708	623.208	<b>59.500</b>
P11	441.250	479.666	<b>38.416</b>	780.875	795.291	<b>14.416</b>
P12	549.750	588.125	<b>38.375</b>	261.208	313.291	<b>52.083</b>
P13	521.833	600.333	<b>78.500</b>	1.138.083	1.198.458	<b>60.375</b>
P14	513.125	561.916	<b>48.791</b>	198.166	221.583	<b>23.417</b>
P15	348.125	381.458	<b>33.333</b>	628.000	649.208	<b>21.208</b>
P16	829.708	905.500	<b>75.792</b>	440.000	463.541	<b>23.541</b>
P17	406.875	446.666	<b>39.791</b>	690.750	720.333	<b>29.583</b>
P18	795.125	865.583	<b>70.458</b>	342.333	403.625	<b>61.292</b>
P19	348.125	389.500	<b>41.375</b>	652.583	670.333	<b>17.750</b>
P20	801.166	1.032.250	<b>231.084</b>	379.208	397.708	<b>18.500</b>
P21	266.958	323.333	<b>56.375</b>	727.500	778.708	<b>51.208</b>
P22	743.458	797.208	<b>53.750</b>	340.625	377.666	<b>37.041</b>
P23	667.083	1.082.625	<b>415.542</b>	1.496.500	1.659.125	<b>162.625</b>
P24	662.125	712.166	<b>50.041</b>	268.625	292.250	<b>23.625</b>
P25	356.875	429.833	<b>72.958</b>	761.833	783.458	<b>21.625</b>
P26	600.541	653.625	<b>53.084</b>	235.791	279.000	<b>43.209</b>
P27	295.750	353.750	<b>58.000</b>	609.833	623.583	<b>13.750</b>
P28	906.375	963.958	<b>57.583</b>	294.916	336.500	<b>41.584</b>
P29	613.541	696.541	<b>83.000</b>	1.002.833	1.041.667	<b>38.834</b>
P30	706.333	867.583	<b>161.250</b>	393.208	410.791	<b>17.583</b>

Tabela 5.9: Tempos de Conclusão das Tarefas (em milissegundos). (Fonte: o Autor.)

Estatística	Conta gov.br	E-mail e Senha
Média	76740,27	38320,83
Desvio Padrão	75617,50	30923,76
Min	25625,00	11333,00
Max	415542,00	162625,00
1º Quartil	43531,75	19031,25
Mediana	55062,50	27458,00
3º Quartil	75083,50	46208,25

Tabela 5.10: Estatísticas descritivas das diferenças de tempo (ms) entre os métodos. (Fonte: o Autor).

Utilizando os dados mensurados, é possível analisar a distribuição das informações usando um gráfico de caixa, conforme ilustrado na Figura 5.20. O tempo foi modificado para segundos para que a legibilidade ficasse melhor, e os *outliers* foram destacados com o valor e o participante.

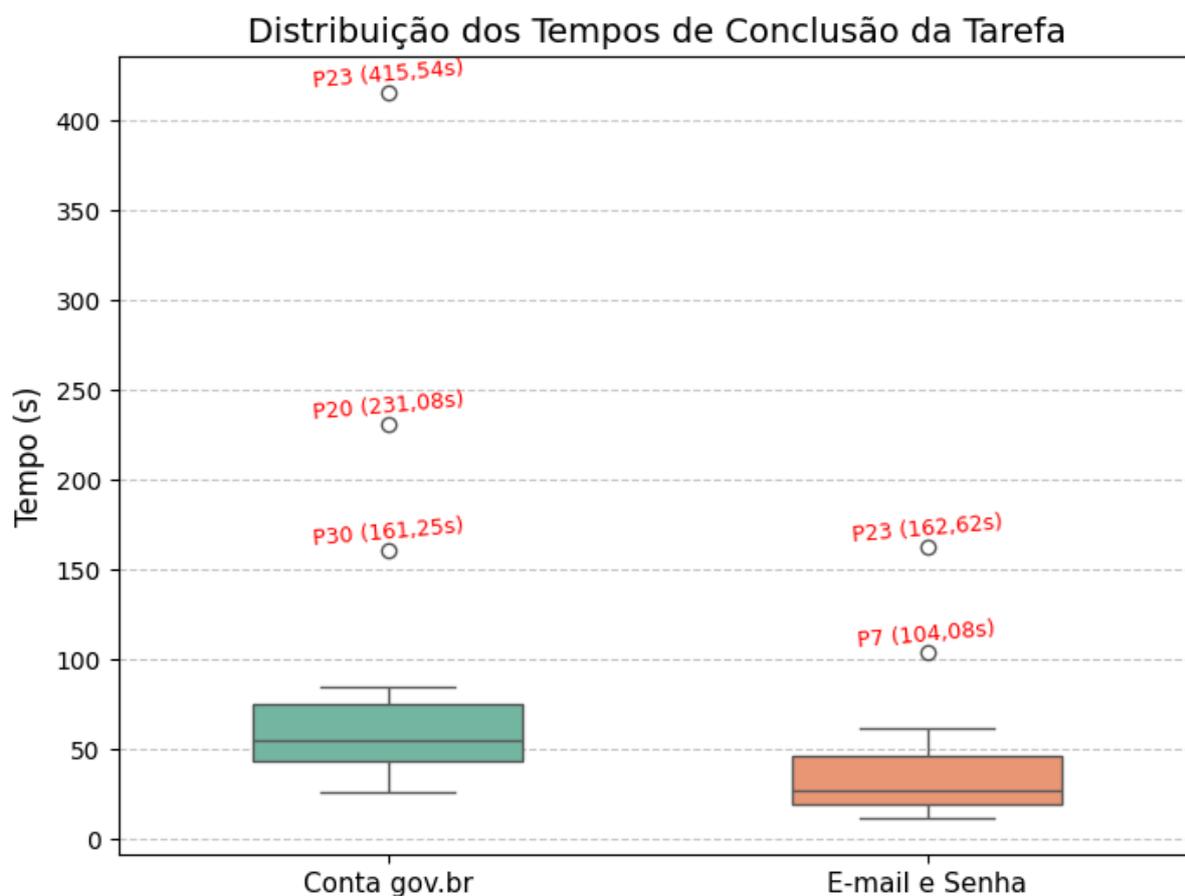


Figura 5.20: Distribuição dos tempos de conclusão da tarefa. (Fonte: O Autor.)

A existência desses valores discrepantes nos levou a catalogar os fatos atípicos que ocorreram no decorrer dos testes de usabilidade, de forma que fosse possível compreender como os fatores ambientais poderiam influenciar nas medidas. Essas informações estão no Quadro 5.4.

<b>Participante</b>	<b>Observações</b>
P4	Erro ao copiar a credencial do E-mail e Senha. Reclamou da quantidade de mensagens que aparece quando usa a <i>Conta gov.br</i> .
P5	Faltou dar o último clique na autenticação da <i>Conta gov.br</i> .
P6	Digitou as credenciais ao invés de copiar e colar.
P7	Copiou as credenciais de forma duplicada, o que fez com que o tempo fosse muito maior do que o normal.
P8	Errou a credencial da <i>Conta gov.br</i> .
P12	Leu o termo de uso na hora de autenticar usando login e senha.
P13	Teceu várias considerações sobre as instruções antes de concluir o login com e-mail e senha.
P15	O site da <i>Conta gov.br</i> apresentou uma lentidão incomum, o que fez com que o usuário tivesse que reiniciar o processo.
P18	Preferiu digitar as credenciais tanto do e-mail e senha quanto da <i>Conta gov.br</i> ao invés de copiar e colar.
P20	O site da <i>Conta gov.br</i> ficou indisponível durante o teste, e com isso o participante teve um tempo muito superior para concluir.
P21	Participante foi confirmar se estava fazendo certo antes de clicar em submeter no cenário do e-mail e senha.
P22	Erro ao copiar as credenciais de e-mail e senha. Apareceu um Captcha durante a autenticação da <i>Conta gov.br</i> .
P23	O site da <i>Conta gov.br</i> ficou indisponível. Participante teve dificuldade maior ao seguir o roteiro, errou as credenciais e leu as instruções durante a execução, o que causou um tempo fora do normal.

Continua na próxima página

Quadro 5.4 – Continuação da página anterior

Participante	Observações
P26	Errou ao inserir as credenciais.
P28	Participante abriu os termos de uso durante a autenticação com e-mail e senha.
P29	Lentidão no site da <i>Conta gov.br</i> .
P30	Lentidão no site da <i>Conta gov.br</i> .

Quadro 5.4: Fatos atípicos que ocorreram durante o teste. (Fonte: o Autor)

Verificando as informações coletadas, é possível afirmar que o fator que mais influenciou na variação dos tempos dos dois cenários foi a inclusão errada das credenciais utilizadas. A decisão do participante de digitar os dados de acesso ao invés de copiar e colar também impactaram nos tempos aferidos. Concluindo, para os *outliers*, a instabilidade do site da *Conta gov.br* teve um reflexo preponderante, indicando que esse ponto deve ser considerado na decisão da integração com a plataforma.

Finalmente, analisaremos a comparação dos tempos de conclusão para as duas tarefas. A estatística utilizada para definir a tendência central desse tipo de dado varia geralmente entre a média e a mediana. A mediana é frequentemente uma escolha melhor para dados assimétricos como os tempos analisados, segundo Sauro e Lewis [88], pois representa o ponto central onde metade dos valores está acima e metade abaixo, sendo menos afetada por valores extremos. No entanto, os autores apontam que ela apresenta dois desafios principais:

- Variabilidade: A mediana não utiliza todos os valores da amostra e pode variar bastante com amostras pequenas.
- Viés: Em amostras pequenas, a mediana calculada tende a superestimar a mediana da população, enquanto a média é uma estatística não tendenciosa.

Diante desses fatos, a fim de determinar a melhor estimativa do tempo médio de tarefa em pequenas amostras de testes de usabilidade, Sauro e Lewis [88] analisaram diversas médias, incluindo média aritmética, mediana, média geométrica e médias aparadas. O estudo mostrou que a média geométrica é a melhor estimativa do centro, especialmente para amostras menores que 25, pois apresenta menos erro e viés do que a média ou a mediana. Os dados de todas as médias são apresentados na Tabela 5.11.

Métrica	Conta gov.br (ms)	E-mail e Senha (ms)
Média Aritmética	76.740,27	38.320,83
Mediana	55.062,50	27.458,00
Média Geométrica	61.514,36	30.888,14

Tabela 5.11: Médias e Mediana dos Tempos de Conclusão (ms).

Uma vez que nosso estudo apresentou um número de 30 participantes, estando acima, portanto, do limiar de 25 amostras sugerido pelos pesquisadores citados, foi definido que a métrica utilizada seria a mediana. Para fins de completude, também é recomendado que seja calculado um intervalo de confiança de 95%, de forma que os limites superior e inferior das medidas sejam conhecidos. Para a mediana, Haukoos e Lewis [148] sugerem o método do *bootstrapping*, mais adequado para trabalhar com distribuições que não são normais. Os valores calculados estão na Tabela 5.12 e ilustrados pela Figura 5.21.

Métrica	Conta gov.br (ms)	E-mail e Senha (ms)
Limite Superior	70.145,50	40.834,00
Limite Inferior	48.625,00	21.416,50
Intervalo de Confiança	21.520,50	19.417,50

Tabela 5.12: Intervalo de Confiança dos Tempos de Conclusão (ms).

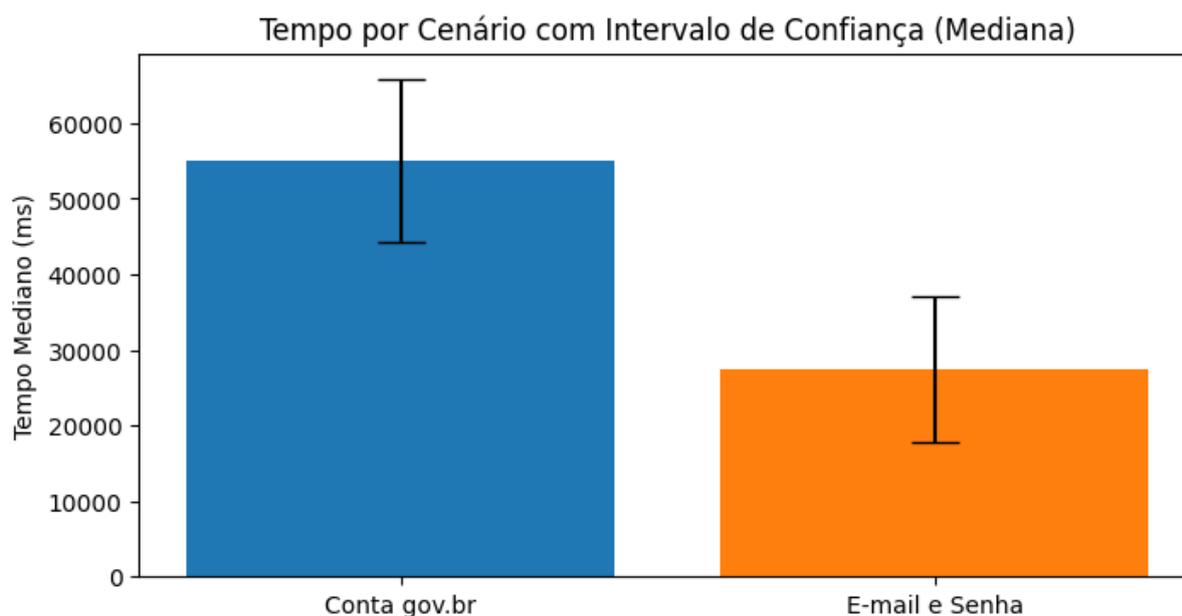


Figura 5.21: Tempo de conclusão mediano por cenário. (Fonte: O Autor.)

Mesmo que o gráfico sugira que a diferença de tempos é significativa, é preciso confirmar estatisticamente a suspeita. De forma análoga ao cálculo realizado para o SUS e para o SEQ, calcularemos se os resíduos seguem uma distribuição normal, utilizando o teste de Shapiro-Wilk. O teste confirmou que havia assimetria nas diferenças ( $W(30) = 0,69$ ,  $p = 0,0000010$ ), um resultado que já era esperado dada a presença de valores discrepantes na amostra.

Diante dessa situação, é necessário utilizar um teste não-paramétrico para aferição da significância estatística. De forma similar ao executado na Facilidade Percebida, usamos o teste de Wilcoxon de Postos Sinalizados, que resultou na estatística  $Z = 34,0$ ,  $p = 6,9179 \times 10^{-6}$ . Ao contrário do que foi visto com o SEQ, o valor-p encontrado aqui é muito menor que 0,05, rejeitando a hipótese nula do teste e confirmando que existe uma diferença estatisticamente significativa.

Também é possível verificar o Tamanho do Efeito, mas ao contrário do que foi visto no cálculo do SUS, o  $d$  de Cohen não é muito indicado, uma vez que assume como premissa a normalidade da distribuição. A alternativa para o nosso caso é o uso da Correlação Bisserial de Postos (*Rank-Biserial Correlation* [149]). Nesse indicador, valores próximos de 1 ou  $-1$  indicam um efeito forte, enquanto valores próximos de 0 indicam pouco ou nenhum efeito. No caso concreto, o resultado indicou um efeito muito forte ( $RBC = 0,8538$ ), confirmando que a **Conta gov.br** é significativamente mais lenta, correspondendo a mais do que o dobro do tempo (100,53%) da autenticação por E-mail e Senha, tendo como base a mediana calculada dos dois tipos de autenticação.

Na seção 5.6, faremos a análise da correlação dos dados coletados, de forma a tentar entender como cada fator influenciou nas avaliações dos participantes.

## 5.6 Análise de Correlações

A apresentação dos dados individuais de cada métrica nos levou a perceber que a sensação de usabilidade (aferida pelo SUS) e de facilidade (SEQ) não variou muito entre os dois cenários testados. O mesmo não pode ser dito sobre o Tempo de Conclusão da Tarefa (TCT), que teve um aumento significativo quando a **Conta gov.br** foi usada. Os dados consolidados dos dois cenários podem ser conferidos na Tabela 5.13.

ID	SUS		SEQ		TCT (ms)	
	Gov.br	E-mail	Gov.br	E-mail	Gov.br	E-mail
P1	97,50	97,50	7	7	69.833	40.084
P2	97,50	92,50	7	7	25.625	11.333
P3	100,00	80,00	7	7	27.750	20.625
P4	65,00	90,00	7	7	53.000	47.208
P5	75,00	67,50	6	5	48.459	12.667
P6	77,50	85,00	6	6	62.750	37.834
P7	85,00	95,00	6	7	46.375	104.084
P8	77,50	90,00	6	7	83.917	17.708
P9	100,00	100,00	7	7	42.584	25.333
P10	85,00	85,00	7	7	84.417	59.500
P11	100,00	72,50	7	7	38.416	14.416
P12	62,50	87,50	6	7	38.375	52.083
P13	100,00	87,50	7	6	78.500	60.375
P14	82,50	100,00	7	7	48.791	23.417
P15	95,00	85,00	7	7	33.333	21.208
P16	80,00	92,50	7	7	75.792	23.541
P17	97,50	97,50	7	7	39.791	29.583
P18	95,00	95,00	7	7	70.458	61.292
P19	95,00	97,50	7	7	41.375	17.750
P20	77,50	82,50	7	7	231.084	18.500
P21	72,50	60,00	6	6	56.375	51.208
P22	95,00	87,50	7	7	53.750	37.041
P23	90,00	95,00	7	7	415.542	162.625
P24	100,00	97,50	7	7	50.041	23.625
P25	60,00	65,00	5	6	72.958	21.625
P26	80,00	87,50	7	6	53.084	43.209
P27	87,50	100,00	7	7	58.000	13.750
P28	95,00	82,50	6	7	57.583	41.584
P29	82,50	92,50	6	7	83.000	38.834
P30	97,50	100,00	7	7	161.250	17.583

Tabela 5.13: Resultado Consolidado das Métricas por Participante. (Fonte: o Autor).

A análise inicial que pode ser feita é se existe alguma correlação entre os resultados, ou seja, se há associação entre uma característica mensurada e outra. Schober et al. [150] explicam o uso de dois coeficientes mais comumente usados em análises desse tipo: Pearson e Spearman. Os autores esclarecem que a escolha entre eles depende de como os dados da amostra estão distribuídos. Se houver uma distribuição normal, sem *outliers*, a primeira alternativa pode ser usada. Caso contrário, o coeficiente de Spearman se mostra mais adequado.

Com o intuito de verificar essa premissa, executamos o teste de Shapiro-Wilk em cada um dos conjuntos, de forma que fosse possível obter o diagnóstico sobre a normalidade da distribuição. Aqueles que tivessem um valor- $p$  maior ou igual a 0,05 confirmariam essa característica. Os resultados estão apresentados na Tabela 5.14.

Métrica	valor- $p$
SUS - Conta gov.br	$6,24 \times 10^{-3}$
SUS - E-mail e Senha	$3,03 \times 10^{-3}$
SEQ - Conta gov.br	$1,42 \times 10^{-7}$
SEQ - E-mail e Senha	$8,37 \times 10^{-9}$
TCT - Conta gov.br	$1,28 \times 10^{-8}$
TCT - E-mail e Senha	$3,17 \times 10^{-6}$

Tabela 5.14: Dados do Teste de Shapiro-Wilk no conjunto de resultados. (Fonte: o Autor).

Esses dados confirmaram que a melhor opção para a análise de correlação seria usar o coeficiente de Spearman, uma vez que a premissa de normalidade foi violada. Dessa forma, os cálculos foram feitos e geraram o mapa de calor representado na Figura 5.22. Com ele, é possível perceber alguns *insights* que serão descritos a seguir.

O primeiro deles, que talvez seja esperado, é a indicação da existência de uma correlação positiva entre os resultados do SUS e SEQ (0,60 para a **Conta gov.br**, e 0,52 para E-mail e Senha). Ou seja, pessoas que tiveram uma melhor percepção de usabilidade tenderam a avaliar melhor a facilidade de uso do mecanismo.

Outro ponto que se destaca é uma leve força positiva quando correlacionamos os tempos de conclusão da **Conta gov.br** com o cenário de E-mail e Senha. Com um índice de 0,26, há uma indicação que a demora em um cenário pode envolver um tempo maior no outro também, porém em uma magnitude baixa.

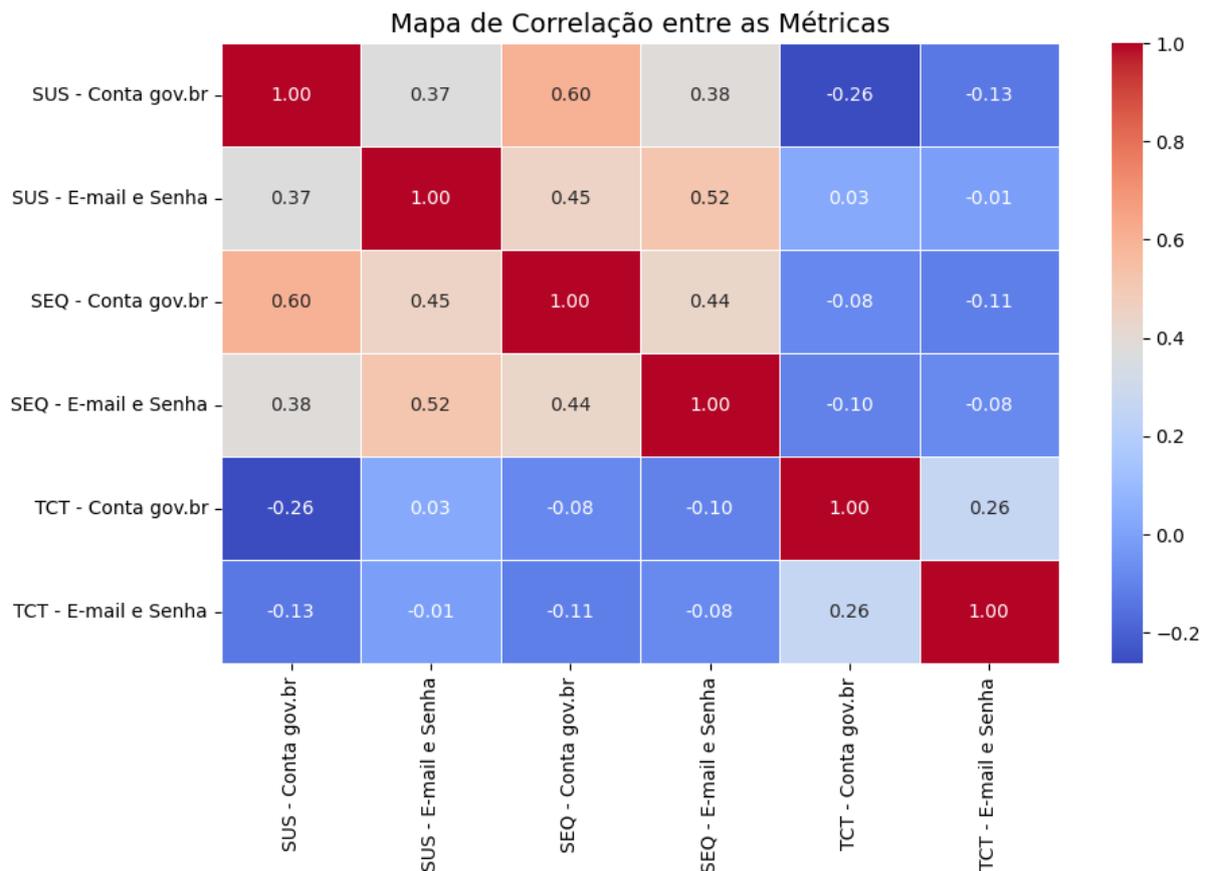


Figura 5.22: Correlação entre os resultados das métricas.(Fonte: O Autor.)

Um comportamento similar aparece, em uma direção oposta, na correlação entre o tempo de conclusão da tarefa da **Conta gov.br** com a avaliação do SUS. Os dados sugerem que um aumento no tempo da conclusão para esse cenário pode ter diminuído, de forma sutil  $(-0, 26)$ , a percepção de usabilidade dos participantes.

E esse quadro em particular nos leva a uma reflexão mais profunda, pois a expectativa é que a força dessa correlação fosse maior. Se utilizarmos como exemplo o que aconteceu com o participante P23, que teve o maior Tempo de Conclusão de toda a amostra, é possível observar que sua pontuação do SUS da **Conta gov.br** foi de 90 pontos, um valor que é classificado como *Best Imaginable* na escala de adjetivos. É no mínimo curioso que um participante que teve problemas de indisponibilidade do site da **Conta gov.br** não tenha dado uma nota ruim em critérios que mediam o quão usável era o mecanismo.

Em contrapartida, o participante P25 não teve nenhuma intercorrência na execução do seu teste, mas deu uma das piores notas do estudo para os dois cenários mensurados, além de ter sido o único a usar uma resposta abaixo de 6 na escala de facilidade percebida. Esses pontos indicam que este participante foi bem mais crítico na execução do teste do que os demais.

Esses resultados sugerem que existem aspectos ocultos que interferem no julgamento dos usuários quando estão utilizando o sistema. Vamos tentar encontrar essas características utilizando o cruzamento das métricas com os dados demográficos, a fim de identificar quais possuem variações relevantes que merecem uma investigação. A correlação entre esses itens está apresentada na Figura 5.23.

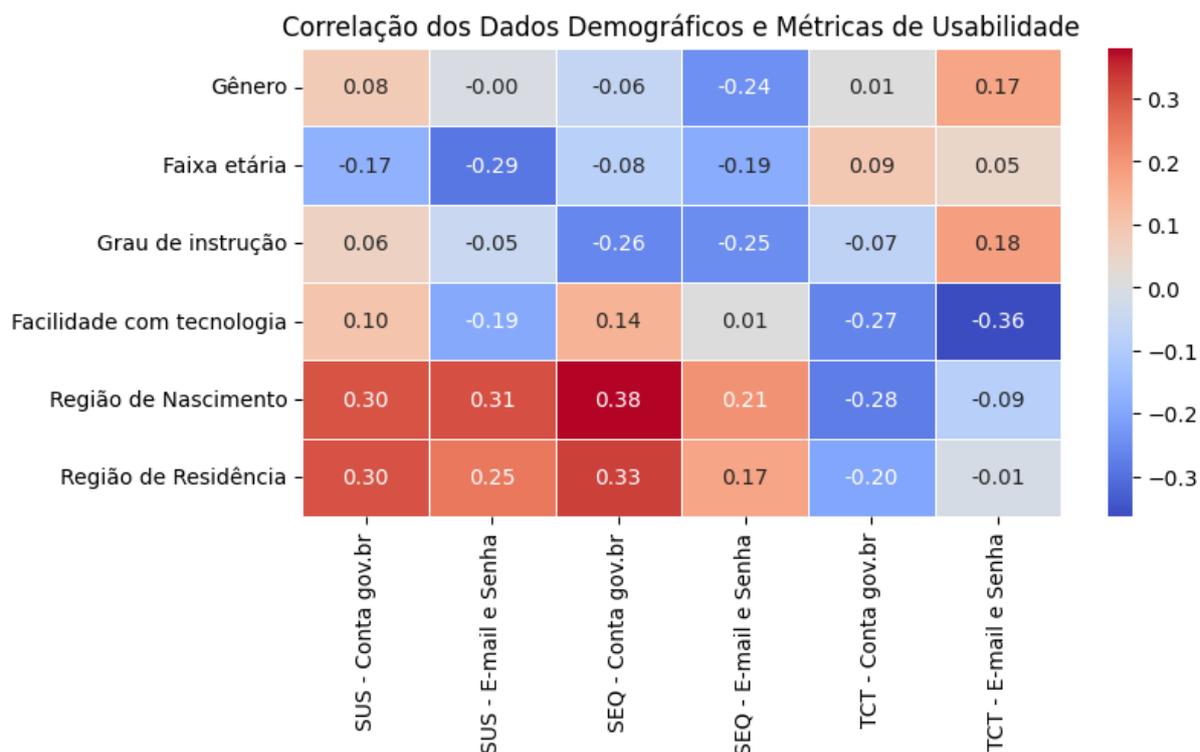


Figura 5.23: Correlação entre os dados demográficos e as métricas de usabilidade. (Fonte: O Autor.)

Percebe-se que o gênero dos participantes não influenciou na maioria das métricas, tendo uma pequena força no cenário do E-mail e Senha, sendo negativa na avaliação da Facilidade Percebida e positiva no Tempo de Conclusão. Analisaremos essas duas métricas com mais detalhes com base nos gráficos apresentados na Figura 5.24. Eles apresentam as médias dos indicadores separadas por gênero, sendo que o Tempo de Conclusão utilizou a média geométrica pelo fato da quantidade de cada amostra ser menor que 25, conforme orientação de Sauro e Lewis [88] explicitada na seção 5.5.3. Os intervalos de confiança também foram calculados usando o método do *bootstrapping*, dada a falta de distribuição normal dos dados das métricas demonstrada na Tabela 5.14.

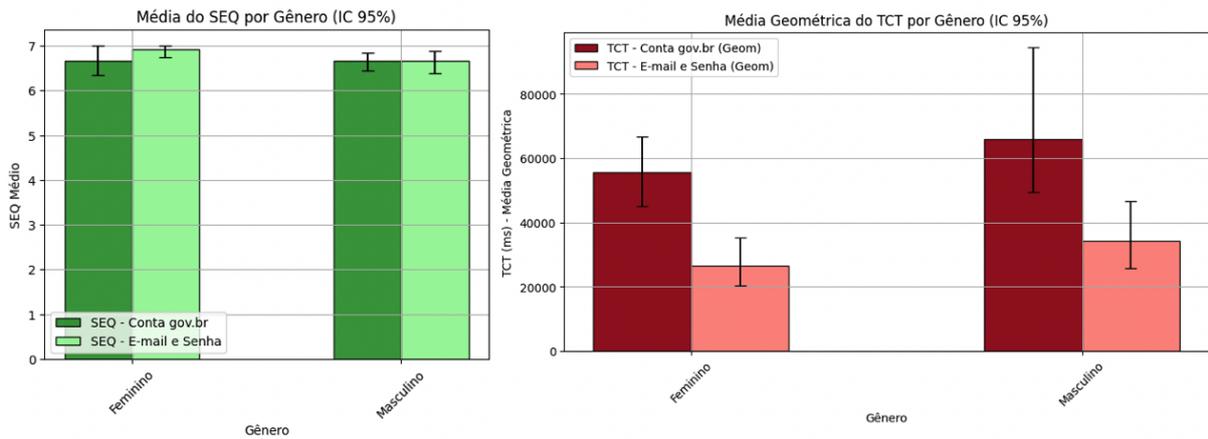


Figura 5.24: Dados de SEQ e TCT por gênero.(Fonte: O Autor.)

A verificação dos dados nos permite inferir que o público feminino foi mais sensível ao julgar a facilidade percebida dos dois mecanismos de autenticação. Esse mesmo segmento foi mais rápido ao completar as duas tarefas, sugerindo uma agilidade maior que a masculina. Cabe frisar, porém, que há uma diferença na distribuição entre os gêneros (60% dos participantes são do gênero masculino), o que pode ter impactado o resultado geral.

Já a faixa etária influenciou o resultado da usabilidade geral, medida pelo SUS, e da Facilidade Percebida do E-mail e Senha. Como as categorias da faixa etária foram mapeadas de forma ordinal (quanto maior a faixa etária, maior o valor utilizado no cálculo da correlação), o mapa de calor aponta que o SUS diminui na medida que a categoria etária aumenta. Esse foi o mesmo resultado do SEQ, e ambos os cenários são ilustrados na Figura 5.25.

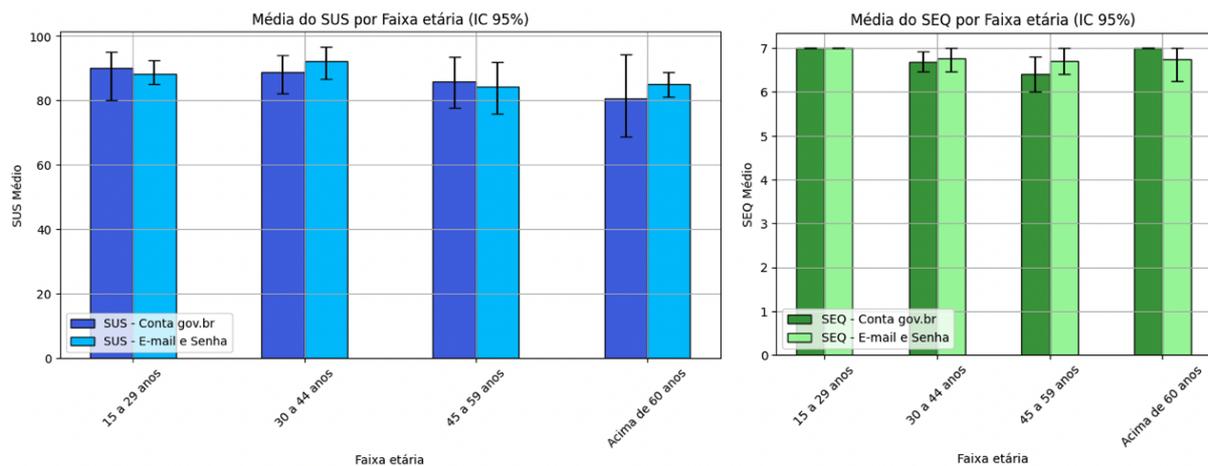


Figura 5.25: Dados de SUS e SEQ por faixa etária.(Fonte: O Autor.)

Os gráficos apontam que houve, realmente, uma tendência de declínio na avaliação de usabilidade da *Conta gov.br* na medida que a idade do participante aumentava.

O cenário de E-mail e Senha mostrou uma flutuação maior, obtendo um valor alto na população entre 30 a 44 anos (92, 31) e uma diminuição nas faixas posteriores (84, 25 e 85), sendo que essa diferença pode explicar a maior força da correlação negativa detectada no mapa de calor. Esse pico sugere uma maior familiaridade desse público com a solução de E-mail e Senha. Já a Facilidade Percebida teve uma flutuação maior com o aumento da idade para a **Conta gov.br**, apresentando seu pior resultado na faixa de 45 a 59 anos (6, 4), se mantendo estável no cenário de E-mail e Senha.

O grau de instrução dos participantes apresentou uma influência negativa na avaliação da Facilidade Percebida, e uma leve força positiva no Tempo de Conclusão usando o E-mail e Senha. Tal qual a faixa etária, o mapeamento dessa categoria foi feita da menor (Ensino Fundamental) para a maior (Pós-Graduação), apontando que pessoas com mais tempo de estudo avaliaram a facilidade com valores mais baixos. De alguma forma, essa escolaridade também afetou o Tempo de Conclusão do E-mail e Senha, conforme podemos verificar na Figura 5.26.

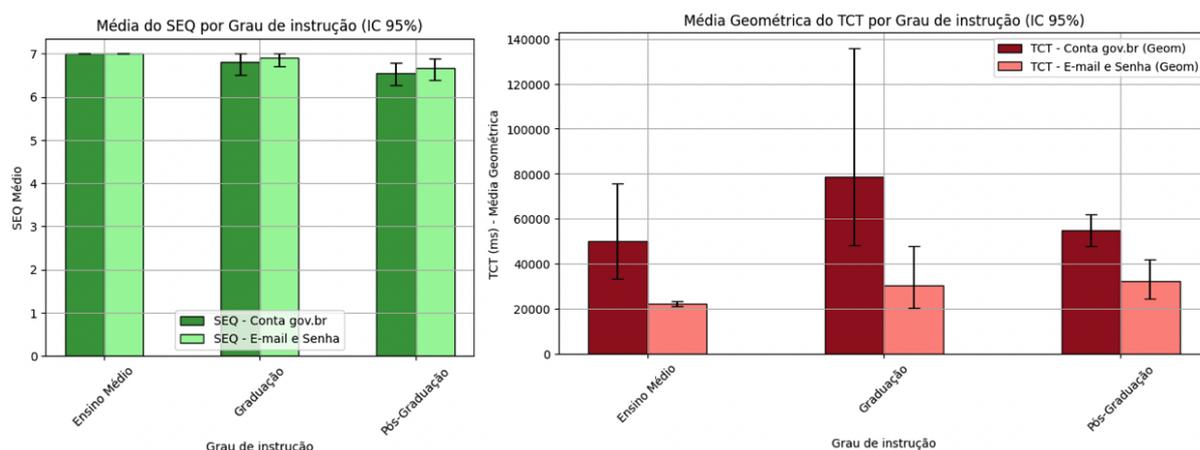


Figura 5.26: Dados de SEQ e TCT por grau de instrução.(Fonte: O Autor.)

De fato, a avaliação de facilidade varia com a escolaridade, principalmente no que concerne à **Conta gov.br**. Uma explicação para isso pode ser que esse fator faz com que as pessoas sejam mais criteriosas ao responder essa pergunta do questionário. Já o gráfico de Tempo de Conclusão nos traz um aspecto interessante: mesmo com um valor extremo entre o grupo que tem Graduação, o mapa de calor não detectou uma correlação forte nesse grupo, identificando apenas o aumento do tempo no cenário de E-mail e Senha. Esse fenômeno confirma a premissa que a Correlação de Spearman é mais robusta a *outliers*, uma vez que esse foi o grupo que conteve os participantes P20, 23 e 30, responsáveis pelos picos de tempo mensurados.

No quesito Facilidade com tecnologia, temos pequenas correlações nas três métricas. Uma curiosa, referente ao SUS, pois mostra direções opostas nos cenários testados (posi-

tiva para a *Conta gov.br*, negativa para E-mail e Senha), e pode ser vista com detalhes na Figura 5.27. Já as outras métricas apresentaram um comportamento mais uniforme e são apresentadas na Figura 5.28.

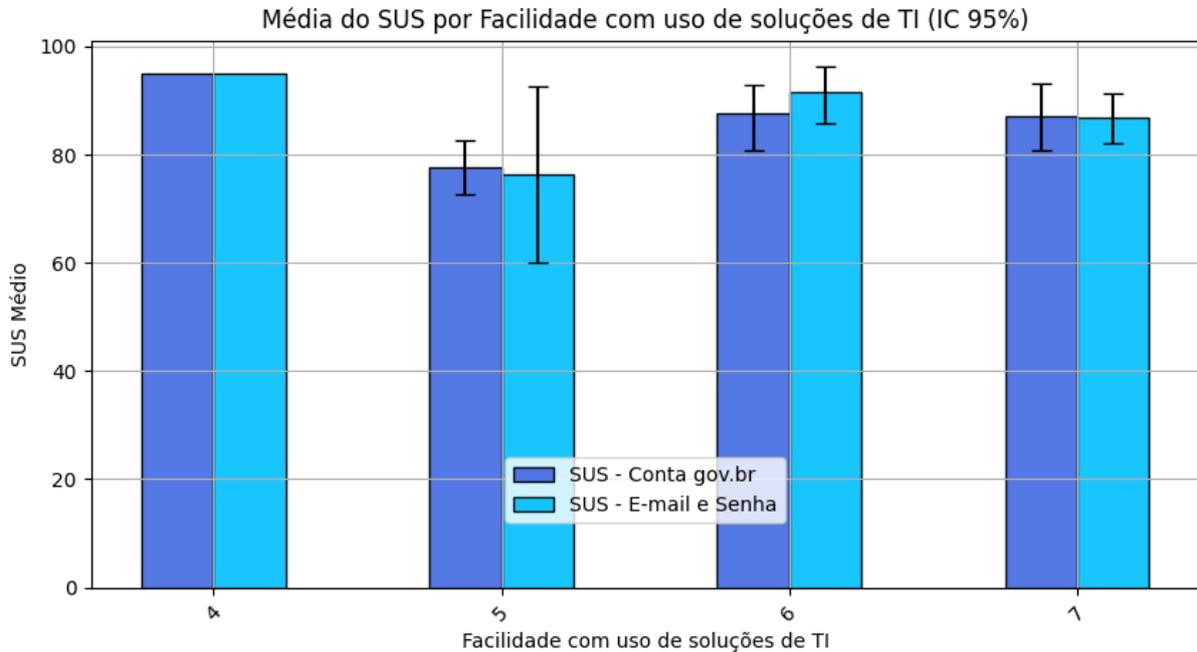


Figura 5.27: Dados do SUS por nível de facilidade de uso de soluções de TI.(Fonte: O Autor.)

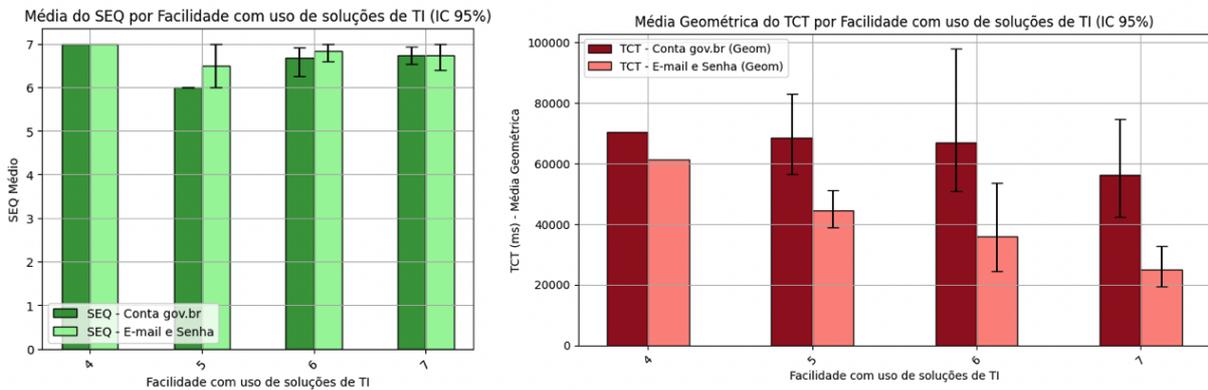


Figura 5.28: Dados do SEQ e TCT por nível de facilidade de uso de soluções de TI.(Fonte: O Autor.)

Os dados do SUS mostram a razão das correlações com forças opostas. Enquanto que para a *Conta gov.br* a média cresceu e se estabilizou na medida que as pessoas declaravam que tinham mais facilidade no uso de soluções de tecnologia da informação, no cenário de E-mail e Senha houve um declínio entre o penúltimo e o último grau de facilidade. Isso quer dizer que as pessoas que declararam que tinham muita facilidade de

usar soluções de internet deram notas de usabilidade mais baixas (86, 83) que aquelas que tinham um nível 6 de facilidade (91, 46). Uma vez que a pontuação do nível 7 foi muito próxima para os dois cenários (a **Conta gov.br** teve uma média de 87), uma explicação possível é que para as pessoas com essa expertise, a usabilidade dos dois mecanismos é igual, enquanto no nível anterior (6), a simplicidade do E-mail e Senha desequilibrou a avaliação para este cenário em detrimento à **Conta gov.br**.

Encerrando as correlações, encontramos forças relevantes tanto nas regiões de nascimento quanto nas de residência dos participantes. Sendo assim, faremos uma análise conjunta de todas as métricas, que estão ilustradas nas Figuras 5.29, 5.30 e 5.31.

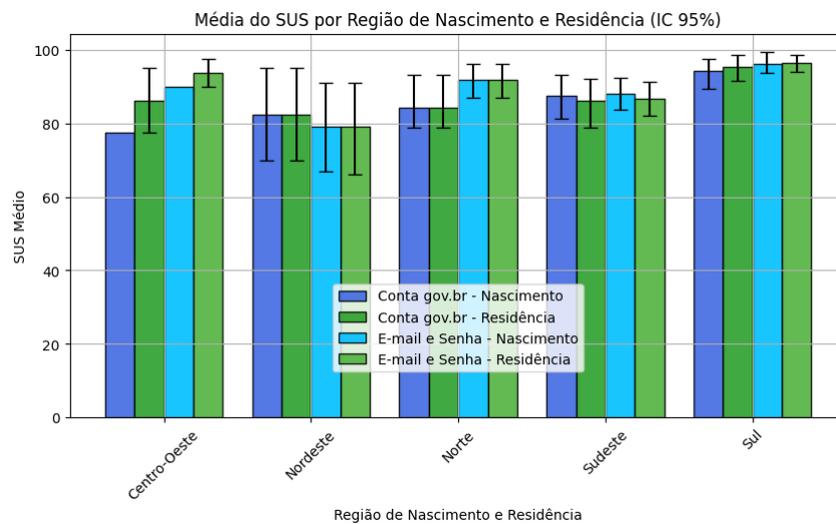


Figura 5.29: Resultado do SUS por região de nascimento e residência.(Fonte: O Autor.)

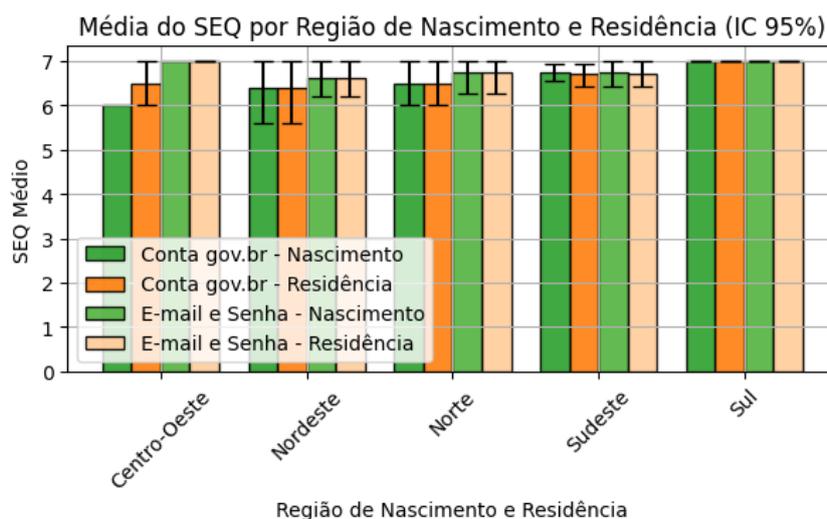


Figura 5.30: Resultado do SEQ por região de nascimento e residência.(Fonte: O Autor.)

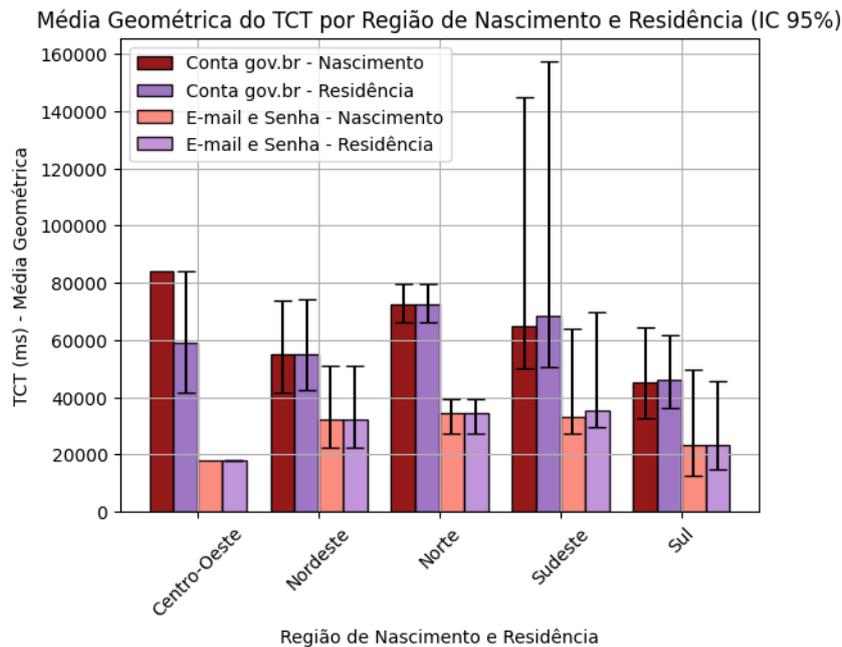


Figura 5.31: Resultado do TCT por região de nascimento e residência.(Fonte: O Autor.)

As distribuições de participantes por região, outro dado importante para essa análise, estão apresentadas na Tabela 5.15.

Região	Nascimento	Residência
Centro-Oeste	1	2
Nordeste	5	5
Norte	4	4
Sudeste	16	14
Sul	4	5

Tabela 5.15: Número de participantes por região de nascimento e residência. (Fonte: o Autor).

O ponto mais relevante que esses dados mostram é que a análise do Centro-Oeste ficou prejudicada, pois o baixo número de participantes da amostra pode enviesar qualquer ponderação. Ao mesmo tempo, o efeito da migração de Estado também é pequeno, com apenas 2 pessoas indo da região Sudeste para as regiões Centro-Oeste e Sul. Isso explica a proximidade das correlações entre a Região de Nascimento e de Residência.

Outra observação interessante é que o Nordeste apresentou a pior experiência de usabilidade de todas as regiões, mesmo tendo um Tempo de Conclusão razoavelmente bom. Tal resultado pode estar vinculado aos valores de Facilidade Percebida, uma vez que essa região também teve um dos valores mais baixos da amostra. A fim de investigar se há

algo que poderia influenciar neste cenário, verificamos nas regiões os três itens que o mapa de calor da Figura 5.23 apresentou como forças nas métricas do SUS e SEQ, ou seja: Faixa Etária, Grau de Instrução e Facilidade com Tecnologia. Essas informações estão consolidadas na Figura 5.32.

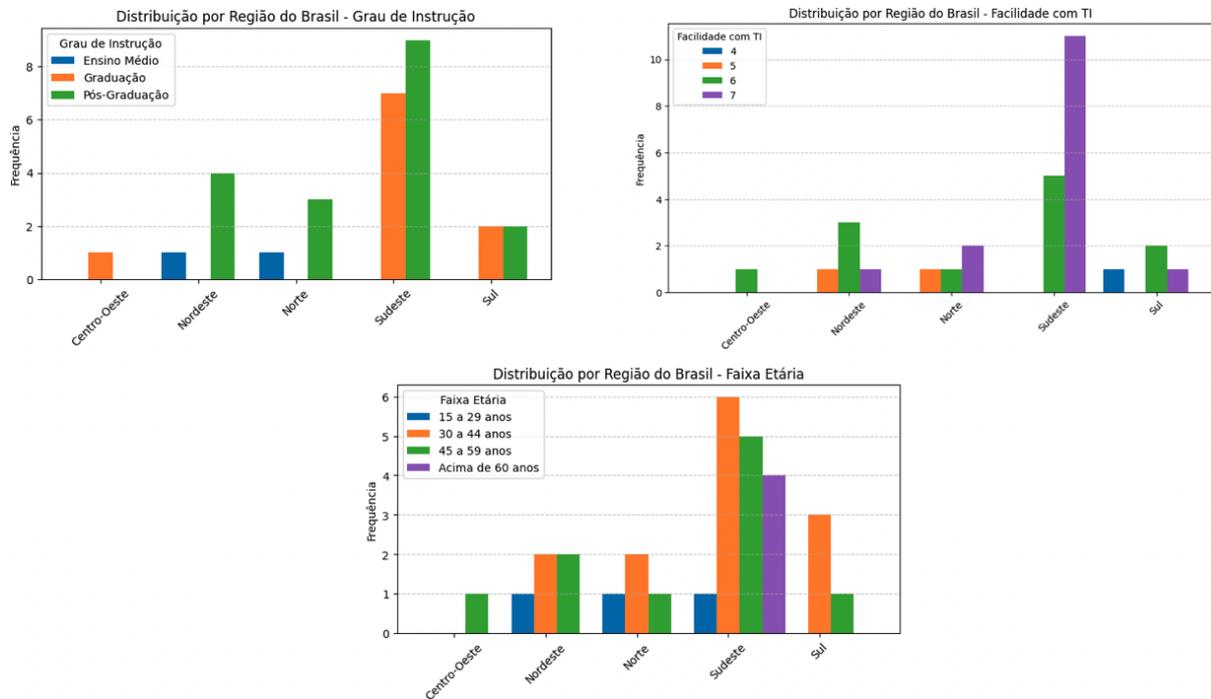


Figura 5.32: Dados de Grau de instrução, Facilidade com tecnologia e Faixa etária por região. (Fonte: O Autor.)

Ao compararmos a região Nordeste com a Norte e a Sul (que possuem uma amostra similar), podemos verificar que os itens que afetam o SUS (Faixa etária e Facilidade com tecnologia) possuem distribuições diferentes nas três regiões. Embora similar à distribuição da região Norte, o Nordeste possui uma pessoa a mais com a faixa etária de 45 a 59 anos, ao mesmo tempo que a distribuição na região Sul está mais concentrada na faixa de 30 a 44 anos. Como o SUS possui uma leve correlação negativa com a Faixa etária, essa configuração pode ter impactado no caso da região Nordeste.

Ainda no que tange à *System Usability Scale*, observa-se que o Nordeste apresenta uma maior concentração de participantes no nível 6, de Facilidade com soluções de TI, em comparação com as regiões Norte e Sul. Essa predominância pode ter influenciado a redução da pontuação média, uma vez que a usabilidade tende a ser melhor avaliada por indivíduos com maior familiaridade tecnológica. Enquanto a região Norte conta com dois participantes com o nível máximo, o Nordeste possui apenas um. Por outro lado, a presença de um entrevistado no nível 4 na região Sul não impactou negativamente a

média, pois esse participante (P18) atribuiu uma pontuação elevada de usabilidade (95) para ambos os cenários, contrariando a tendência indicada pela correlação.

Finalmente, ao observarmos o Grau de instrução por região, percebe-se que a região Nordeste apresenta participantes concentrados na maior escolaridade, de forma similar ao Norte, mas com o dobro em relação ao Sul. Se esse quesito faz com que o participante seja mais criterioso em relação à pontuação da Facilidade Percebida, esse contexto também explicaria a pontuação global menor dessa região.

A análise sugere que a dispersão geográfica, tanto em relação ao local de nascimento quanto de residência, não influenciou diretamente as métricas. No entanto, a composição dos grupos regionais, determinada por outros fatores demográficos, pode ter exercido um impacto mais significativo. A confirmação dessa hipótese depende de uma amostra maior nas regiões que foram alvo da análise.

Faremos, na seção 5.7, uma discussão geral de todos os resultados buscando uma visão ampla do estudo como um todo, e organizando todas as inferências e limitações que foram detectadas nos dados da amostra.

## 5.7 Discussão

O estudo realizado, embora tenha contemplado todas as regiões, teve uma parcela significativa dos participantes situados na região Sudeste, tanto no nascimento (53,3%) quanto na residência (46,7%). Dessa forma, essa concentração deve ser levada em conta em qualquer análise e, um possível aprimoramento seria a ampliação de participantes nas outras regiões, a fim de identificar padrões regionais que possam interferir na aferição de usabilidade. Essa expansão poderia mirar também a representação de pessoas com o Ensino Fundamental, que não apareceram na amostra e diminuem a completude da pesquisa.

Outro ponto importante a ser reconhecido é o impacto da ausência de indivíduos que não conheciam a *Conta gov.br*. Um perfil assim traria uma contribuição significativa para identificar problemas com as métricas de usabilidade mensuradas, uma vez que esses participantes não estariam acostumados a usar o mecanismo de autenticação. Por outro lado, a dificuldade de encontrar uma pessoa nessas condições pode ser um indicador de que o uso da *Conta gov.br* já está bem difundido, tornando sua integração mais fácil para os usuários de serviços públicos digitais.

Iniciando o exame das métricas coletadas, o estudo revelou que a média para a usabilidade geral medida pelo SUS variou pouco entre os dois mecanismos de autenticação, sendo avaliada em 86,83 para a *Conta gov.br* e 88,25 para o E-mail e Senha, conferindo a avaliação *Best Imaginable* para ambos os cenários. Mesmo que o E-mail e Senha tenham apresentado uma leve vantagem em quesitos como simplicidade e familiaridade,

a diferença não foi considerada estatisticamente significativa, o que indica que implantar a autenticação com a **Conta gov.br** não trará um impacto significativo na sensação de usabilidade global, caso o público-alvo do serviço a ser fornecido se encaixe no perfil identificado na pesquisa.

Tal conclusão se aplica também, de forma mais evidente, na Facilidade de Uso Percebida, medida pelo SEQ. Com 6,67 para a **Conta gov.br** e 6,77 para o E-mail e Senha, os participantes não detectaram nenhuma dificuldade a mais ao usar a **Conta gov.br** em comparação com a opção clássica de login e senha. Essa constatação, porém, merece uma reflexão mais aprofundada, uma vez que a expectativa natural é que a facilidade do E-mail e Senha fosse maior do que a aferida na **Conta gov.br**. Essa suposição é baseada na quantidade de cliques e telas que são apresentadas em cada um dos cenários, conforme podemos conferir nas Figuras 5.33 e 5.34.

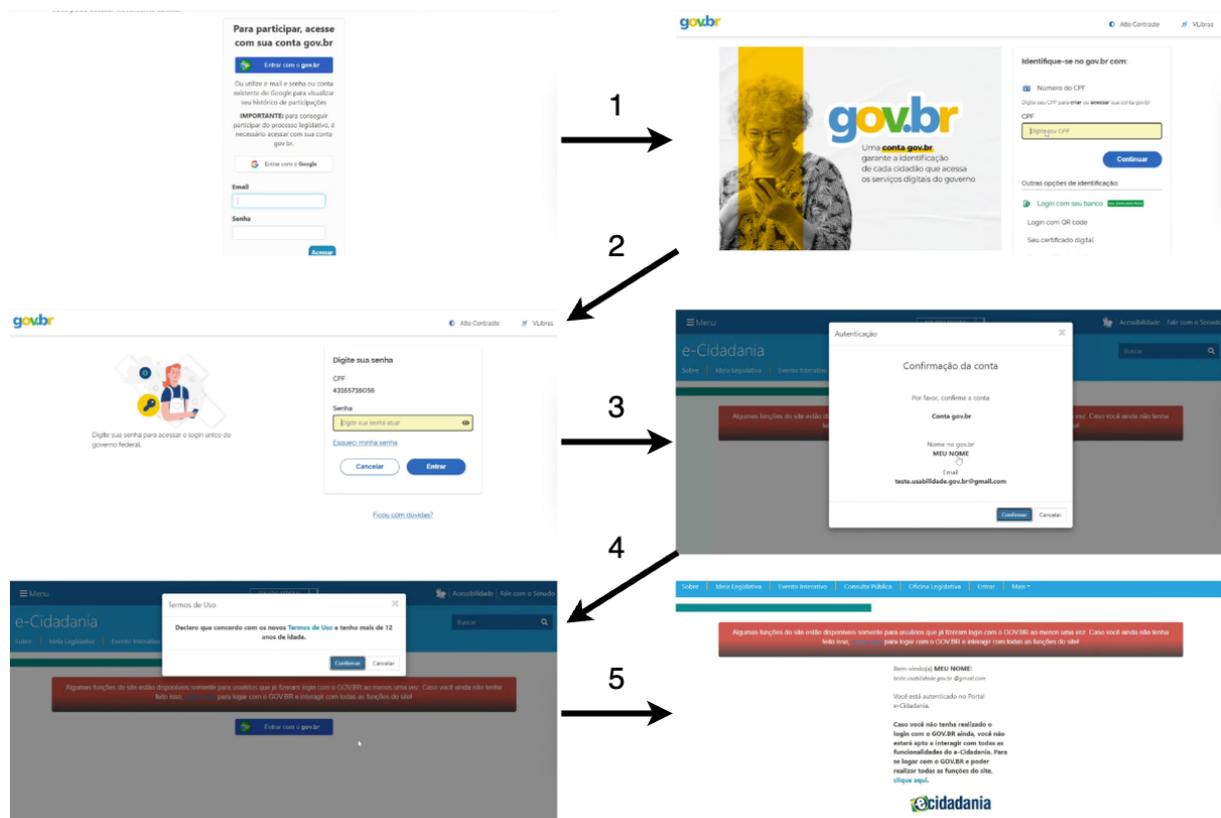


Figura 5.33: Fluxo de páginas - Cenário **Conta gov.br**.(Fonte: O Autor.)

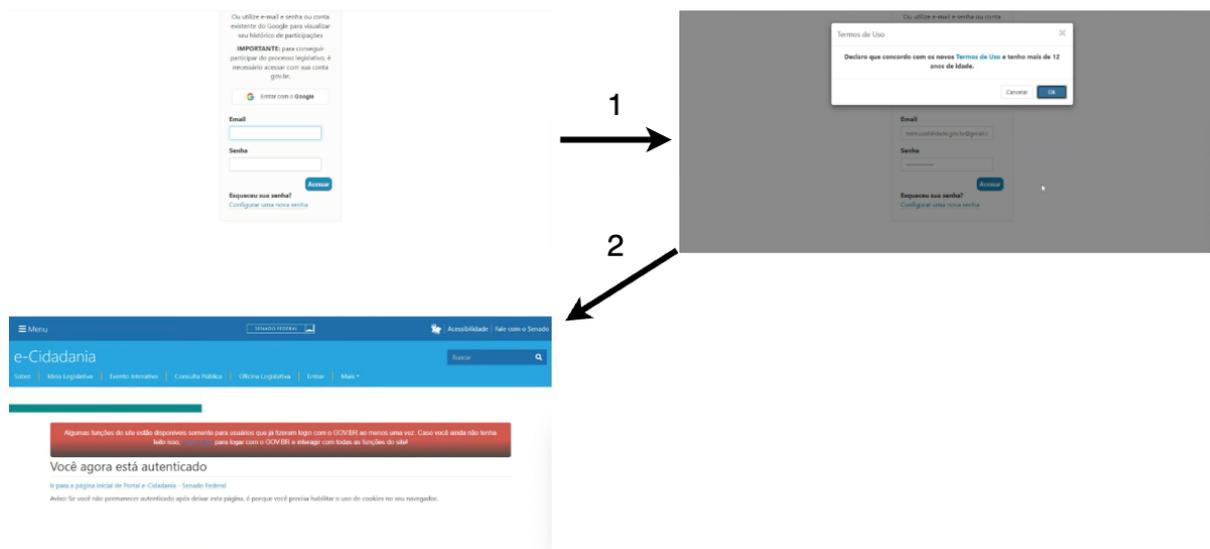


Figura 5.34: Fluxo de páginas - Cenário E-mail e senha.(Fonte: O Autor.)

A sensação da facilidade estar atrelada a uma quantidade menor de interações foi investigada por Lam [151], que identificou que mesmo ações simples como cliques de mouse podem impactar na usabilidade e na eficiência do usuário. Portanto, quando o cenário da **Conta gov.br** apresenta mais do que o dobro de transições do que é feito usando E-mail e Senha, é curioso que a usabilidade e a facilidade aferidas tenham sido tão similares.

Há duas hipóteses para essa situação: ou os participantes estão tão habituados com o uso da **Conta gov.br** que já absorveram esse custo de interação, ou os testes do SUS e SEQ podem não ter sido adequados e/ou bem aplicados para mensurar a Usabilidade e a Facilidade Percebida. Mais uma vez, o caso do participante P23, mencionado na seção 5.6, merece ser citado: mesmo com problemas de disponibilidade da **Conta gov.br**, que levaram ao Tempo de Conclusão da Tarefa mais alto de toda a amostra, o participante deu a nota máxima de facilidade (7) para os dois cenários. Testes adicionais seriam necessários para confirmar alguma dessas premissas.

Já o Tempo de Conclusão da Tarefa, com seu caráter eminentemente objetivo, não deixa dúvidas: integrar a **Conta gov.br** a um serviço público digital aumentará substancialmente o tempo necessário para fazer a autenticação do usuário. Ainda que esse aumento possa ter a sensação de demora reduzida pelo fato de ser uma solução de *Single Sign-On*, uma vez que o processo será mais rápido se houver uma autenticação válida e ativa, é um ponto que deve ser considerado com prudência pela equipe que fará a integração. Esse indicador também evidenciou uma desvantagem que ocorre em qualquer mecanismo de autenticação que use SSO: a inserção de um ponto de falha externo, que fica em uma infraestrutura computacional fora do controle da organização que está integrando

o mecanismo às suas soluções. Obviamente, espera-se que a estabilidade de um ambiente de produção seja diferente de um de testes como o usado nas entrevistas. A expectativa é que o ambiente real tenha recursos de Alta Disponibilidade, como balanceamento de carga e *cluster* de servidores, de forma que o período de inatividade seja reduzido ao máximo, mas tal risco deve ser avaliado ao integrar a **Conta gov.br** com um sistema existente.

Finalizando as considerações sobre o Tempo de Conclusão, a análise de correlação entre os resultados mostrou que a demora na autenticação afeta negativamente tanto a usabilidade quanto a facilidade experimentadas pelos usuários de um sistema. Embora tenha se mostrado sutil no contexto do estudo, é uma correlação esperada, já que o tempo de resposta é um indicador de eficiência, e quanto mais ele aumenta, maior a sensação de que o sistema não está funcionando bem.

Outra suposição confirmada foi a existência de uma correlação positiva entre a sensação de usabilidade e a facilidade percebida, indicando que usuários que avaliaram a experiência como mais fluida também atribuíram notas mais altas à facilidade de uso. Esse resultado é coerente, pois, quando uma solução computacional não apresenta obstáculos para a execução de uma tarefa, a percepção de usabilidade tende a ser mais favorável.

A inclusão dos dados demográficos dos participantes na análise revelou tendências relevantes para a adoção da **Conta gov.br**. A idade, por exemplo, apresentou correlação negativa com o SUS e o SEQ, sugerindo que participantes mais velhos avaliaram a usabilidade e a facilidade de uso de forma menos favorável. Embora seja recomendável ampliar a amostra de participantes entre 15 a 29 anos e acima de 60 anos para validar essa tendência, caso a faixa etária dos usuários do sistema onde a **Conta gov.br** será implementada seja conhecida, é possível antecipar potenciais desafios ou facilidades na integração.

A mesma estratégia pode ser feita se o grau de instrução de quem vai utilizar o serviço público digital for conhecido de antemão. Como esse dado exibiu uma correlação negativa com a facilidade percebida, provavelmente indivíduos com maior nível educacional serão mais críticos com uma mudança no modo de autenticação, o que pode ser mitigado com campanhas que mostrem as vantagens da integração da **Conta gov.br** à solução existente.

Além disso, a correlação negativa entre a facilidade com o uso de soluções de TI e a nota do SUS para a autenticação via E-mail e Senha pode indicar que usuários familiarizados com tecnologia preferem não utilizar credenciais próprias, optando por concentrar seus acessos em uma única conta para evitar a necessidade de gerenciar múltiplas senhas.

Por fim, não foi possível concluir se algum aspecto regional influenciou os resultados. Um aumento na amostragem dos candidatos das regiões Centro-Oeste, Nordeste, Norte e Sul é necessário antes de verificar se fatores associados à infraestrutura das regiões

avaliadas poderiam modificar as impressões dos dois mecanismos para os usuários.

Em síntese, os dados coletados indicam que, no contexto deste estudo, a inserção da *Conta gov.br* como opção de autenticação em um serviço público digital não apresentou impacto significativo na usabilidade e na facilidade percebida. No entanto, gestores responsáveis por essa implementação devem considerar o aumento expressivo no Tempo de Conclusão da Tarefa durante o processo de autenticação, assim como também a inserção de um ponto de falha que fica fora da esfera de atuação do órgão. Além disso, uma análise demográfica do público-alvo pode auxiliar na identificação de possíveis pontos de atrito, permitindo a antecipação de desafios e a adoção de estratégias de sensibilização para melhorar a aceitação da mudança.

Apresentaremos, na seção 5.8, uma compilação das sugestões coletadas dos entrevistados sobre o sistema e-Cidadania e a *Conta gov.br*.

## 5.8 Sugestões dos participantes

Para finalizar, as sugestões dos participantes serão apresentadas a seguir, em forma de tópicos, com o objetivo de servir como insumo para melhorias tanto na *Conta gov.br* quanto no sistema e-Cidadania. Embora o roteiro da pesquisa não incluísse perguntas específicas para estimular essas contribuições, alguns participantes manifestaram interesse em compartilhá-las espontaneamente. O que segue é uma síntese das principais sugestões apresentadas:

- **Simplificação da apresentação das proposições legislativas** – Melhorar, no e-Cidadania, a forma como as informações sobre projetos em tramitação são apresentadas, tornando-as mais acessíveis e compreensíveis, especialmente para usuários com dificuldade em entender a proposta.
- **Resumo em linguagem simples** – Disponibilizar um resumo claro e objetivo para cada proposição em análise no e-Cidadania, facilitando a compreensão do tema por todos os cidadãos, independentemente do nível de familiaridade com termos técnicos.
- **Informações sobre viabilidade econômica** – Incluir detalhes no e-Cidadania sobre custos administrativos associados à tramitação dos projetos, como gastos com viagens e participação de envolvidos, tornando o processo mais transparente.
- **Interação e acompanhamento do trabalho dos Senadores** – Criar ferramentas que agilizem o acesso a informações sobre proposições analisadas pelos Senadores, melhorando a experiência do usuário no e-Cidadania e possibilitando um acompanhamento mais intuitivo e eficiente.

- **Visibilidade da opção de saída** – Ajustar o design do botão “Sair” no e-Cidadania para melhorar sua visibilidade e acessibilidade, reduzindo dificuldades relatadas pelos usuários durante os testes.
- **Sensação de segurança na autenticação** – Ressaltar que o uso da *Conta gov.br* aumenta a segurança, conforme relatado por um participante que atribuiu esse sentimento à autenticação em duas etapas.
- **Orientações prévias à autenticação** – Disponibilizar janelas explicativas antes do processo de login pode auxiliar os usuários a compreender melhor cada etapa, reduzindo possíveis dificuldades durante a autenticação.
- **Facilidade de navegação em sites oficiais** – Desenvolver interfaces intuitivas nos sites governamentais. Essa demanda foi relatada por um participante que afirmou ter dificuldade nos sítios eletrônicos governamentais, e que isso deve afligir especialmente usuários com menor familiaridade digital.
- **Divulgação das consultas públicas** – Adotar estratégias mais eficazes de divulgação das consultas, incluindo notificações personalizadas e integração com redes sociais, ampliando a participação cidadã. Na visão do participante que deu essa sugestão, a disseminação das consultas não está alcançando toda a população.
- **Redução da exigência de autenticação** – Tornar o processo de autenticação menos frequente, proporcionando uma experiência mais fluida para os usuários.
- **Melhoria no espaçamento dos blocos de autenticação** – Ajustar o layout dos campos de autenticação para evitar erros acidentais e melhorar a interação visual. O participante afirmou que os campos de autenticação estão muito próximos, o que dificultou a autenticação.
- **Otimização do conteúdo textual** – Reduzir a quantidade de texto e informações, apresentando conteúdos de maneira mais clara e objetiva. O participante informou que o excesso de texto e informações dificultavam sua navegação.
- **Destaque para informações essenciais** – Melhorar a apresentação visual e a hierarquização dos conteúdos principais, facilitando a compreensão e a usabilidade, já que algumas terminologias técnicas não estavam sendo entendidas.
- **Dicas visuais (*hints*)** – Incorporar *hints* visuais durante a autenticação para orientar usuários e minimizar erros.
- **Facilidade de uso para o público geral** – Tornar o site do e-Cidadania mais intuitivo e acessível, principalmente para usuários com pouca familiaridade tecno-

lógica, já que na visão do participante que deu a sugestão, o site é complicado de usar.

- **Integração com o sistema da Caixa Econômica Federal** – Explorar as soluções da Caixa Econômica Federal para ampliar o alcance das proposições legislativas, considerando que a instituição já atende uma parcela significativa da população, principalmente para receber os benefícios sociais. Na ideia desse participante, esse mesmo aplicativo poderia disseminar as proposições legislativas, trazendo para o debate uma população carente que nem sempre é ouvida.
- **Contribuição para a formação cidadã** – Garantir que a usabilidade do sistema incentive o engajamento e a participação cívica dos usuários.
- **Usabilidade da *Conta gov.br*** – Simplificar os fluxos da *Conta gov.br* para tornar a experiência do usuário mais clara. Na visão desse participante, as interações com a solução são confusas.

A diversidade de perspectivas dos participantes gerou *insights* relevantes e destacou desafios que podem passar despercebidos pelos gestores dos dois produtos por conta destes já estarem acostumados a usar os sistemas. As sugestões serão encaminhadas aos gestores que colaboraram na realização do estudo, com a expectativa de que contribuam para melhorias futuras. Na seção 5.9, será apresentada uma síntese dos principais pontos abordados neste capítulo, consolidando as reflexões e recomendações resultantes da análise.

## 5.9 Síntese do Capítulo

Este capítulo apresentou os resultados da pesquisa sobre a usabilidade dos mecanismos de autenticação aplicados ao e-Cidadania, comparando o uso da *Conta gov.br* com o E-mail e Senha, e abordando desde os fatores que influenciaram a coleta de dados até a análise dos achados e as sugestões dos participantes.

Inicialmente, discutiu-se o impacto da necessidade de submissão da pesquisa ao Comitê de Ética em Pesquisa em Ciências Humanas e Sociais da UnB (CEP/CHS). Foram detalhados os documentos exigidos e as adaptações necessárias para garantir conformidade com as diretrizes éticas. Além disso, destacou-se a influência da enquete realizada pelo Instituto DataSenado, que forneceu um panorama inicial sobre a percepção dos usuários da plataforma e alterou a estratégia de recrutamento dos participantes.

Na sequência, descreveu-se o protocolo final do teste de usabilidade, que foi ajustado com base nas exigências do Comitê de Ética e nos dados oriundos da enquete. A execução

do teste foi detalhada, incluindo o recrutamento, o perfil dos participantes e os métodos de coleta de dados.

Os resultados da pesquisa foram apresentados por meio das métricas de usabilidade definidas no modelo proposto no Capítulo 4, incluindo a *System Usability Scale (SUS)*, a Facilidade Percebida de Uso e o Tempo de Conclusão da Tarefa. Os principais achados foram:

- A usabilidade geral, medida pelo SUS, teve médias de 86,83 para a autenticação via **Conta gov.br** e 88,25 para a autenticação via E-mail e Senha. Ambas as pontuações foram classificadas como *Best Imaginable*, indicando uma excelente percepção de usabilidade. A diferença entre os dois cenários foi considerada estatisticamente irrelevante por um Teste T Pareado ( $t(29) = -0,64, p = 0,5258$ ).
- A Facilidade Percebida de Uso, mensurada pelo SEQ, apresentou médias de 6,67 para a **Conta gov.br** e 6,77 para E-mail e Senha, em uma escala de 1 a 7. Assim como no SUS, não houve diferença estatisticamente significativa entre os cenários, medida pelo Teste de Wilcoxon de Postos Sinalizados ( $Z = 15,0, p = 0,3173$ ).
- O Tempo de Conclusão da Tarefa (TCT) apresentou uma diferença estatisticamente significativa entre os métodos de autenticação, conforme demonstrado pelo Teste de Wilcoxon de Postos Sinalizados ( $Z = 34,0, p = 6,9179 \times 10^{-6}$ ). A análise das medianas revelou que a autenticação via **Conta gov.br** (mediana = 55,07s) foi aproximadamente duas vezes mais lenta (100,53%) em comparação ao método de autenticação via E-mail e Senha (mediana = 27,46s). Além disso, o teste evidenciou como o site da **Conta gov.br** pode ser um gargalo e impactar sobremaneira o tempo de autenticação dos usuários caso apresente lentidão ou indisponibilidade.

Na seção de **análise de correlações**, investigou-se a relação entre as métricas de usabilidade e características demográficas dos participantes. Destacaram-se os seguintes pontos:

- Houve uma **correlação positiva entre SUS e SEQ** (0,60 para a **Conta gov.br** e 0,52 para **E-mail e Senha**), sugerindo que participantes que perceberam maior usabilidade também relataram maior facilidade de uso.
- O **TCT e o SUS** apresentaram uma **correlação negativa** ( $-0,26$  para a **Conta gov.br**), sugerindo que tempos de conclusão mais longos impactaram, ainda que de forma sutil, a percepção de usabilidade. Essa relação indica que usuários que levaram mais tempo para concluir as tarefas tenderam a relatar uma experiência de uso menos satisfatória.

- A **idade dos participantes** teve correlação negativa com o SUS e SEQ, indicando que usuários mais velhos tenderam a avaliar a usabilidade e a facilidade de uso de forma menos favorável.
- Foi identificada uma correlação entre o nível de familiaridade com tecnologia e as métricas coletadas, sendo positiva para o SUS e SEQ, e negativa para o TCT. Participantes que se declararam mais experientes no uso de tecnologia apresentaram escores ligeiramente mais elevados de usabilidade e facilidade percebida, ao mesmo tempo que levaram um tempo menor para concluir a autenticação dos dois cenários.

Na **discussão**, os achados foram interpretados e evidenciaram que a diferença entre os métodos de autenticação foi mais perceptível no **tempo de conclusão da tarefa** do que na percepção de usabilidade ou facilidade de uso. Suposições sobre os resultados e correlações foram levantadas, como a hipótese de que a familiaridade dos participantes com a **Conta gov.br** pode ter reduzido o impacto negativo de sua interface mais complexa. No entanto, algumas limitações da pesquisa devem ser consideradas:

- O número reduzido de participantes de algumas regiões do Brasil prejudicou a identificação de como fatores regionais poderiam influenciar nas métricas, sendo recomendável ampliar a amostra em estudos futuros.
- O perfil dos respondentes pode ter influenciado os resultados, especialmente no que tange à familiaridade com tecnologia e idade, sugerindo a necessidade de análises segmentadas por grupos específicos.
- A avaliação da usabilidade foi baseada em métricas subjetivas, como SUS e SEQ, que, apesar de amplamente utilizadas, podem não ter sido aplicadas de uma forma que permitisse detectar com tranquilidade as diferenças dos dois cenários.

Por fim, a pesquisa incorporou o **feedback dos participantes**, que forneceram sugestões de melhorias para a plataforma e apontaram desafios enfrentados durante o uso. Os principais pontos levantados foram:

- **Aperfeiçoamento da acessibilidade e usabilidade do e-Cidadania:** Sugeriu-se simplificar a apresentação das proposições legislativas e incluir resumos em linguagem simples para maior clareza. Melhorias como dicas visuais e hierarquização das informações essenciais poderiam facilitar a navegação, além de alguns ajustes no design.
- **Fortalecimento da experiência de autenticação e segurança:** Recomendou-se melhorar os fluxos de autenticação e inserir orientações antes do login para reduzir dificuldades. Além disso, a diminuição da necessidade de autenticação poderia

tornar a navegação mais fluida. Pra completar, a autenticação em duas etapas foi percebida como positiva, aumentando a confiança no sistema.

- **Expansão do alcance e engajamento Cidadão:** Para ampliar a participação, sugeriu-se a divulgação mais eficaz das consultas públicas com notificações e redes sociais. A integração com o sistema da Caixa Econômica Federal poderia alcançar um público mais amplo, contribuindo na formação cidadã.

Por fim, os dados resultantes desta pesquisa fornecem insumos para estratégias e tomadas de decisão mais conscientes por parte dos gestores que desejam implantar a **Conta gov.br** em suas soluções de serviço público digital. Esses dados também foram utilizados na elaboração do Guia Prático para Adoção da **Conta gov.br**, disponível no Apêndice C.1. Já as conclusões gerais do estudo são apresentadas a seguir, no Capítulo 6.

# Capítulo 6

## Conclusão

Este trabalho se propôs a verificar quais seriam as vantagens e desvantagens da integração da *Conta gov.br* no ambiente do Senado Federal. Como exemplo prático para essa análise, optamos pela ferramenta e-Cidadania, pois sua proposta de facilitar a participação popular na discussão de alterações legislativas sugere um grande potencial de utilização pela sociedade brasileira em geral.

Foi importante buscar, para a análise, os princípios que norteiam uma solução de Login Único como a *Conta gov.br*, pois poderiam surgir aspectos relevantes capazes de justificar sua utilização, além das dificuldades inerentes à adoção do recurso. Por meio dessa investigação, foram verificados os protocolos mais utilizados na implementação, como SAML, OAuth e *OpenID Connect*. Este último protocolo serviu para compreender melhor os mecanismos internos da *Conta gov.br*, já que foi usado como base arquitetural no seu desenvolvimento [25], [28], [30], [33].

Adicionalmente, a pesquisa optou por focar em um critério importante na avaliação de sistemas interativos: a usabilidade. De acordo com Preece et al. [47], usabilidade envolve a facilidade com que os usuários aprendem a utilizar uma interface, a efetividade com que realizam suas tarefas e o nível de satisfação percebido durante a interação. Trata-se, portanto, de uma propriedade fundamental não apenas para a aceitação inicial de novas funcionalidades, mas também para garantir o uso contínuo, a redução de erros e o aumento da eficiência no uso do sistema.

Considerando os fatores apresentados, foi realizado um levantamento teórico com o objetivo de embasar o conceito de usabilidade, explorando desde os fundamentos da Interação Humano-Computador (IHC) — área na qual a usabilidade está inserida — até os principais atributos que a caracterizam, como a eficiência, a eficácia e a satisfação do usuário. Essa base teórica permitiu identificar, na literatura, técnicas e métricas adequadas para sua aferição, obtendo ferramentas para mensurar, de forma estruturada, o impacto que a integração da *Conta gov.br* poderia gerar na experiência dos usuários da

plataforma e-Cidadania.

Durante a investigação, optou-se por utilizar a metodologia de Revisão Sistemática da Literatura, visando identificar os principais métodos e abordagens empregados em testes de usabilidade aplicados a soluções de login único, bem como as métricas mais adequadas para avaliar a integração da **Conta gov.br** no contexto do Senado Federal. O trabalho resultou em 18 casos de pesquisa com uma rica descrição de metodologia, e informações suficientes para direcionar o planejamento do teste de usabilidade que foi realizado com a **Conta gov.br**.

A análise dos estudos selecionados pela Revisão Sistemática da Literatura permitiu observar como a teoria se manifestava na prática de avaliação da usabilidade em soluções de *login único*. Em relação aos métodos e abordagens de aferição de usabilidade, um dos resultados mais recorrentes foi a recomendação de seguir diretrizes éticas robustas, com destaque para a transparência no tratamento das informações e a garantia de privacidade dos participantes, citada em 61% dos estudos analisados. Verificou-se ainda que o método mais utilizado para mensurar a usabilidade foi a aplicação de questionários baseados em escala Likert, presente em 14 dos 18 artigos (77%). A necessidade de roteiros detalhados para orientar os indivíduos também apareceu com frequência, sendo mencionada em 55% das publicações. Por fim, os dados mostraram que a compensação financeira aos participantes foi aplicada em 10 dos 18 trabalhos analisados (55%), reforçando que esta pode ser uma opção legítima em pesquisas que envolvem participação voluntária em testes experimentais.

Sobre as métricas, três se destacaram pela frequência de uso nos trabalhos da RSL: a Facilidade Percebida no Uso e a *System Usability Scale* (SUS), ambas presentes em cerca de 39% dos estudos analisados (7 de 18), e o Tempo de Conclusão de Tarefas (TCT), identificado em aproximadamente 33% das publicações (6 de 18). Considerando esse padrão de recorrência e o respaldo teórico presente na literatura da área, decidiu-se adotá-las na avaliação da integração da **Conta gov.br** ao sistema e-Cidadania. O TCT foi utilizado como métrica objetiva de desempenho, enquanto a Facilidade de Uso Percebida foi mensurada por meio da *Single Ease Question* (SEQ). A escolha dessas métricas visou capturar dimensões complementares da interação com o sistema. O objetivo foi compreender como esses elementos variavam na experiência dos usuários da plataforma e-Cidadania, comparando a autenticação via **Conta gov.br** com o método original de login por E-mail e Senha.

A base teórica e os exemplos encontrados na literatura foram utilizados para construir o protocolo de testes adotado neste estudo, o qual pode servir de referência para a avaliação de outras soluções de login único em contextos semelhantes. A sistematização das informações permitiu que as bases de um estudo-piloto fossem montadas, dando um

direcionamento claro de como agir para viabilizar a pesquisa, com a montagem dos cenários de teste, mensagens de comunicação e recrutamento, assim como os questionários que seriam aplicados.

No entanto, ocorreram mudanças durante o percurso da pesquisa. O formato adotado, que utilizava técnicas qualitativas por meio da aplicação de questionários aos usuários, exigiu a submissão do estudo ao Comitê de Ética em Pesquisa em Ciências Humanas e Sociais (CEP/CHS) da Universidade de Brasília. Embora esse processo tenha incluído etapas burocráticas adicionais, também proporcionou uma reflexão importante sobre como garantir maior segurança e conforto aos participantes. Ainda, resultou na criação de documentos detalhando explicitamente a forma como os dados dos usuários seriam utilizados, aumentando, assim, a credibilidade da pesquisa.

Um efeito colateral do processo de revisão ética foi a impossibilidade de realizar o estudo-piloto originalmente projetado, uma vez que nenhum teste poderia ocorrer antes da aprovação formal pelo Comitê. Como alternativa, foram realizadas apresentações informais dos procedimentos para colegas de estudo e trabalho, cujas contribuições permitiram aprimorar o roteiro que seria aplicado posteriormente. Além disso, a estratégia de recrutamento também precisou ser revista. A proposta inicial, que previa o uso das redes sociais do pesquisador para selecionar voluntários para o teste, foi substituída após a divulgação dos resultados de uma enquete promovida pelo Instituto DataSenado em parceria com esta pesquisa.

A nova abordagem possibilitou a identificação de mais de 5.000 potenciais participantes, em contraste com os 102 obtidos na estratégia anterior. Além da diferença quantitativa, a nova base apresentava ampla cobertura geográfica, abrangendo todas as regiões do país, o que contribuiu para aumentar a diversidade da amostra. A partir dessa base, foram enviados convites por e-mail para 1.000 contatos. Desse total, obteve-se resposta de 111 destinatários, com 98 confirmando interesse e 30 efetivamente participando dos testes.

Os participantes apresentaram um perfil diversificado, predominantemente masculino (60%), concentrado principalmente nas faixas etárias entre 30 e 44 anos (43,3%) e 45 a 59 anos (33,3%). Destacou-se um alto nível educacional, com 60% possuindo pós-graduação e boa habilidade percebida no uso de tecnologias digitais. Regionalmente, predominou a participação da região Sudeste, tanto em nascimento quanto em residência atual dos respondentes. Por fim, todos os entrevistados já haviam utilizado previamente a Conta gov.br, o que limitou a análise à perspectiva de usuários familiarizados com a ferramenta.

Todos executaram o roteiro de atividades proposto enquanto tinham suas interações gravadas por videochamada. Durante a interação, responderam ao questionário que continha as perguntas de aferição quantitativa da usabilidade geral, medida pelo SUS, e da

facilidade de uso percebida, mensurada pelo *Single Ease Question* (SEQ). O Tempo de Conclusão da Tarefa foi extraído das gravações realizadas. Adicionalmente, alguns participantes forneceram sugestões espontâneas sobre características da Conta gov.br e do sistema e-Cidadania.

Os resultados mostraram que, em termos de usabilidade geral e de facilidade de uso, não foi possível encontrar, na amostra, uma diferença relevante entre os dois mecanismos de autenticação. Na usabilidade, as médias foram elevadas, com 86,83 para a Conta gov.br e 88,25 para E-mail e Senha. Não houve diferença estatisticamente significativa entre os dois cenários, fato confirmado por um Teste T Pareado ( $t(29) = -0,64, p = 0,5258$ ). Tal fenômeno se apresentou também para o SEQ, cujas médias foram 6,67 para Conta gov.br e 6,77 para E-mail e Senha. A insignificância estatística foi comprovada por um Teste de Wilcoxon ( $Z = 15,0, p = 0,3173$ ).

O Tempo de Conclusão da Tarefa, porém, mostrou que há custos na adoção da **Conta gov.br**. Comparando a mediana dos dois modos de autenticação, percebeu-se uma diferença de 27,60s entre eles. Em um contexto onde o cenário de E-mail e Senha teve um tempo mediano de 27,46s, percebe-se que a **Conta gov.br** levou mais do que o dobro do tempo (55,06s), apontando que existe uma diferença substancial entre eles. Para confirmar essa diferença, embora já evidente, foi realizado o Teste de Wilcoxon de Postos Sinalizados ( $Z = 34,0, p = 6,9179 \times 10^{-6}$ ), que demonstrou a relevância estatística do resultado e reforçou que o uso da **Conta gov.br** implica em um aumento significativo no tempo de autenticação.

A apresentada métrica também permitiu identificar os impactos causados por eventuais problemas de lentidão e indisponibilidade do sistema que suporta a **Conta gov.br**. Nos testes em que essas falhas ocorreram, houve um aumento significativo no Tempo de Conclusão, resultando em valores discrepantes (*outliers*) nas medições realizadas. Esse tipo de gargalo pode comprometer a experiência dos usuários e afetar negativamente a aplicação que utiliza essa forma de autenticação. Portanto, ainda que o ambiente de produção conte com mecanismos de alta disponibilidade, é essencial que os gestores reconheçam e avaliem esse risco ao considerarem a adoção da **Conta gov.br** como meio de autenticação em seus serviços públicos digitais.

Além das métricas individuais analisadas, foi investigado como elas se correlacionavam entre si e com os dados demográficos dos participantes. Como os dados não seguiram uma distribuição normal, conforme confirmado pelo teste de Shapiro-Wilk, as análises estatísticas foram realizadas usando o coeficiente de Spearman. Essas análises revelaram uma correlação positiva moderada entre as métricas SUS e SEQ, indicando que participantes com melhor percepção de usabilidade também relataram maior facilidade percebida. Outro resultado relevante foi uma leve correlação negativa entre o tempo gasto na auten-

tação via Conta gov.br e a percepção de usabilidade medida pelo SUS, sugerindo que tempos maiores podem reduzir ligeiramente a avaliação positiva dos usuários quanto à usabilidade.

A análise de correlação demográfica revelou que o gênero dos participantes teve pouca influência nas métricas, embora as mulheres tenham demonstrado maior rapidez e sensibilidade na avaliação da Facilidade Percebida. Já a faixa etária teve impacto negativo nas avaliações de usabilidade (SUS) e Facilidade Percebida (SEQ), especialmente no cenário da Conta gov.br, onde participantes mais velhos atribuíram notas menores a essas métricas. Além disso, o grau de instrução também influenciou negativamente a avaliação de facilidade, indicando que pessoas com maior escolaridade foram mais críticas ao avaliar esse quesito, sobretudo na Conta gov.br. Por fim, participantes com maior facilidade tecnológica apresentaram padrões distintos nos dois cenários: avaliaram de forma positiva a usabilidade da Conta gov.br, mas negativamente a do E-mail e Senha no nível mais alto de familiaridade tecnológica.

Com base nas evidências levantadas ao longo da pesquisa, foi possível consolidar uma das principais contribuições práticas deste trabalho: o **Guia Prático para Adoção da Conta gov.br**. O documento reúne, em um único lugar, informações fundamentais para orientar gestores e equipes técnicas interessadas na adoção desse mecanismo de autenticação. Seu conteúdo foi estruturado a partir dos resultados da revisão sistemática da literatura, dos testes de usabilidade e da consolidação de informações provenientes de fontes oficiais do Governo Federal. O propósito do Guia é facilitar a compreensão sobre o processo de integração da **Conta gov.br** e apoiar a tomada de decisão por instituições públicas que desejem incorporar essa solução aos seus sistemas.

O documento foi redigido em formato *markdown*, a fim de possibilitar sua publicação em plataformas como wikis institucionais, portais internos ou repositórios públicos, como o GitHub. Sua estrutura está organizada em seções que abordam desde as motivações para o uso da **Conta gov.br**, passando por um passo a passo técnico de integração, até a apresentação das vantagens, riscos e formas de mitigação. Um dos diferenciais do Guia é a consolidação de informações dispersas em sites oficiais — como a página de informações gerais da **Conta gov.br**, o portal da Secretaria de Governo Digital e o Roteiro de Integração do Login Único — facilitando o acesso e a compreensão por parte dos profissionais envolvidos no processo.

Além da organização textual, o Guia também recorre a representações gráficas que ajudam a visualizar, por exemplo, o catálogo de confiabilidades e o fluxo de aprovação da integração. Adicionalmente, apresenta dados extraídos dos testes de usabilidade realizados nesta pesquisa, como a usabilidade geral, a facilidade de uso percebida e o tempo médio de autenticação, oferecendo subsídios práticos sobre o impacto da Conta gov.br na

experiência do usuário. O documento ainda aponta riscos potenciais — como o aumento no tempo de login ou possíveis dificuldades enfrentadas por usuários com menor familiaridade tecnológica — e sugere estratégias de mitigação, com o intuito de apoiar processos de implementação mais conscientes e adequados ao contexto de cada instituição.

Como resultado aplicado desta pesquisa, o Guia será encaminhado à Secretaria de Governo Digital como uma contribuição aberta, ficando a critério do órgão avaliar sua utilidade e decidir sobre eventual divulgação, total ou parcial.

Apesar das contribuições consolidadas neste trabalho, como os testes realizados e o Guia Prático elaborado, a pesquisa também revelou oportunidades para estudos complementares que podem ampliar a compreensão sobre o uso da **Conta gov.br** em sistemas públicos.

Além da aplicação dos testes de usabilidade originalmente previstos no planejamento da pesquisa, há aspectos específicos da experiência de autenticação que merecem investigações mais aprofundadas. Um exemplo é o processo de criação inicial da **Conta gov.br**, que envolve etapas adicionais em comparação ao uso recorrente e pode impactar diretamente a percepção de usabilidade. Realizar testes com usuários que estejam acessando a Conta gov.br pela primeira vez, avaliando diferentes métodos de autenticação disponíveis (como cadastro básico, *Internet Banking* e Certificado Digital), pode enriquecer as análises realizadas até aqui.

Outro aspecto importante para avaliação seria a inclusão do 2º fator de autenticação no uso da **Conta gov.br**. A inclusão de mais um passo no processo de login, que exige do usuário acesso ao telefone celular, com conexão à internet habilitada e um aplicativo específico (Gov.br) instalado, sugere um impacto alto na usabilidade, principalmente em pessoas que tenham dificuldade no uso de tecnologias.

A coleta e análise dos dados também forneceram insumos para outros trabalhos futuros, visto que algumas limitações identificadas podem complementar essa pesquisa e torná-la mais completa. A primeira limitação foi a inexistência de pessoas que nunca tinham usado a Conta gov.br na amostra estudada. Um estudo contendo apenas pessoas com tal característica seria valioso para mostrar o efeito da mudança em alguém que não está acostumado com esse tipo de autenticação.

Outro ponto a ser explorado em pesquisas futuras seria ampliar o número de participantes das regiões Centro-Oeste, Nordeste, Norte e Sul, permitindo uma análise mais aprofundada sobre o impacto das particularidades regionais na experiência dos usuários. Da mesma forma, aumentar a participação de usuários mais jovens (entre 15 e 29 anos) e idosos (acima de 60 anos), assim como incluir pessoas com grau de instrução máximo do Ensino Fundamental, poderia proporcionar maior abrangência e representatividade ao estudo.

O efeito das avaliações subjetivas no Alfa de Cronbach também é uma oportunidade interessante de pesquisa. Coletar dados adicionais para verificar se o aumento da amostra elevaria o valor desse índice poderia comprovar ou refutar a hipótese apresentada na pesquisa de que estudos com respostas subjetivas apresentam uma variação que tende a se estabilizar com o crescimento dos participantes.

Por fim, a análise quadro a quadro dos Tempos de Conclusão da Tarefa poderia ser aprimorada por meio da detecção automática das páginas de login e sucesso. Durante a pesquisa, foram avaliados métodos de Reconhecimento Óptico de Caracteres (*Optical Character Recognition* – OCR) e de identificação de imagens nos quadros extraídos dos vídeos, porém nenhuma dessas abordagens produziu resultados satisfatórios no tempo disponível para o estudo. Uma alternativa promissora para futuras análises seria o treinamento de modelos baseados em Inteligência Artificial, como o *You Only Look Once* (YOLO) [152], que pode proporcionar resultados mais precisos e eficientes.

# Referências

- [1] Bank, World: *GovTech Maturity Index, 2022 Update: Trends in Public Sector Digital Transformation*. Relatório Técnico, World Bank, Washington, DC, dezembro 2022. <https://openknowledge.worldbank.org/entities/publication/10b535a7-e9d4-51bd-96ed-6b917d5eb09e>, acesso em 2023-04-18. 1
- [2] Bank, World: *About GovTech*, 2023. <https://www.worldbank.org/en/programs/govtech/priority-themes>, acesso em 2023-04-19. 1
- [3] República, Presidência da: *Decreto N<sup>o</sup> 8.936, de 19 de dezembro de 2016*, dezembro 2016. [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2016/Decreto/D8936.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8936.htm), acesso em 2023-04-22. 2, 19
- [4] República, Presidência da: *Decreto N<sup>o</sup> 10.332, de 28 de abril de 2020*, abril 2020. [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2020/Decreto/D10332.htm#art14](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10332.htm#art14), acesso em 2023-04-22. 2
- [5] República, Presidência da: *Decreto N<sup>o</sup> 10.996, de 14 de março de 2022*, março 2022. [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2022/decreto/d10996.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d10996.htm), acesso em 2024-03-25. 2
- [6] República, Presidência da: *Decreto N<sup>o</sup> 11.260, de 22 de novembro de 2022*, novembro 2022. [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2022/Decreto/D11260.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11260.htm), acesso em 2024-03-25. 2
- [7] Brasil, Governo Federal do: *Estratégia de Governo Digital 2020-2022*, 2023. <https://www.gov.br/governodigital/pt-br/EGD2020/estrategia-de-governo-digital-2020-2022>, acesso em 2023-04-22. 2
- [8] Serviços Públicos Digitais, Departamento de: *Por quem foi criado? — Dúvidas Frequentes da Conta gov.br 1.0.0 documentation*, 2019. [http://faq-login-unico.servicos.gov.br/en/latest/\\_perguntasdafaq/porquemfoicriado.html](http://faq-login-unico.servicos.gov.br/en/latest/_perguntasdafaq/porquemfoicriado.html), acesso em 2023-04-22. 2
- [9] Brasil, Governo Federal do: *Onde usar a conta gov.br*, 2023. <https://www.gov.br/governodigital/pt-br/conta-gov-br/onde-usar-a-conta-govbr/onde-usar-a-conta-gov.br>, acesso em 2023-04-19. 2
- [10] Brasil, Governo Federal do: *Termo de Uso e Política de Privacidade - gov.br*, setembro 2021. [http://faq-login-unico.servicos.gov.br/en/latest/\\_downloads/d6442e668037599687c09290b6c5d6ef/TERMO\\_DE\\_USO\\_E\\_POLITICA\\_DE\\_PRIVACIDADE.pdf](http://faq-login-unico.servicos.gov.br/en/latest/_downloads/d6442e668037599687c09290b6c5d6ef/TERMO_DE_USO_E_POLITICA_DE_PRIVACIDADE.pdf), acesso em 2023-04-24. 3

- [11] Nacional, Congresso: *Lei Nº 13.709, de 14 de agosto de 2018*, agosto 2018. [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm), acesso em 2024-03-25. 3
- [12] Brasil, Governo Federal do: *Lei Geral de Proteção de Dados Pessoais (LGPD)*, agosto 2018. [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm), acesso em 2023-04-26. 3
- [13] Federal, Senado: *Portal e-Cidadania - Senado Federal*, 2023. <https://www12.senado.leg.br/ecidadania>, acesso em 2023-04-25. 3
- [14] Federal, Senado: *Conheça os resultados e o funcionamento do Portal e-Cidadania*. Relatório Técnico, abril 2023. <https://www.senado.gov.br/bi-arqs/Arquimedes/ecidadania/relatorio-simplificado-pdf.pdf>, acesso em 2023-04-26. 4
- [15] Canedo, Edna Dias, Anderson Jefferson Cerqueira, Rogério Machado Gravina, Vanessa Coelho Ribeiro, Renato Camões, Vinicius Eloy dos Reis, Fábio Lúcio Lopes Mendonça e Rafael T. de Sousa: *Proposal of an Implementation Process for the Brazilian General Data Protection Law (LGPD)*. Em *International Conference on Enterprise Information Systems, ICEIS - Proceedings*, volume 1, páginas 19–30. Science and Technology Publications, Lda, 2021, ISBN 978-989-758-509-8. ISSN: 21844992. 4
- [16] Freitas, Vitor: *Perform Systematic Literature Reviews*, 2023. <https://parsif.al/about/>, acesso em 2023-06-06. 6
- [17] Statista: *Internet and social media users in the world 2024*, 2024. <https://www.statista.com/statistics/617136/digital-population-worldwide/>, acesso em 2024-02-26. 8
- [18] Dwivedi, Yogesh K., Elvira Ismagilova, D. Laurie Hughes, Jamie Carlson, Raffaele Filieri, Jenna Jacobson, Varsha Jain, Heikki Karjaluoto, Hajer Kefi, Anjala S. Krishen, Vikram Kumar, Mohammad M. Rahman, Ramakrishnan Raman, Philipp A. Rauschnabel, Jennifer Rowley, Jari Salo, Gina A. Tran e Yichuan Wang: *Setting the future of digital and social media marketing research: Perspectives and research propositions*. *International Journal of Information Management*, 59:102168, agosto 2021, ISSN 02684012. <https://linkinghub.elsevier.com/retrieve/pii/S0268401220308082>, acesso em 2024-02-26. 8
- [19] Lim, Shu Yun, M. L Mat Kiah e Tan Fong Ang: *Security Issues and Future Challenges of Cloud Service Authentication*. *Acta Polytechnica Hungarica*, 14(2), maio 2017, ISSN 17858860. [http://uni-obuda.hu/journal/Lim\\_MatKiah\\_Ang\\_73.pdf](http://uni-obuda.hu/journal/Lim_MatKiah_Ang_73.pdf), acesso em 2024-02-26. 8
- [20] Almuairfi, Sadiq, Prakash Veeraraghavan e Naveen Chilamkurti: *A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices*. *Mathematical and Computer Modelling*, 58(1-2):108–116, julho 2013, ISSN 08957177. <https://linkinghub.elsevier.com/retrieve/pii/S0895717712001719>, acesso em 2024-03-15. 8

- [21] Barkadehi, Mohammadreza Hazhirpasand, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi e Sarminah Samad: *Authentication systems: A literature review and classification*. Telematics and Informatics, 35(5):1491–1511, agosto 2018, ISSN 07365853. <https://linkinghub.elsevier.com/retrieve/pii/S0736585318301400>, acesso em 2024-02-26. 8
- [22] Grabatin, Michael, Michael Steinke, Daniela Pöhn e Wolfgang Hommel: *A Matrix for Systematic Selection of Authentication Mechanisms in Challenging Healthcare related Environments*. Em *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, páginas 88–97, Virtual Event USA, abril 2021. ACM, ISBN 978-1-4503-8319-6. <https://dl.acm.org/doi/10.1145/3445969.3450424>, acesso em 2023-08-22. 9
- [23] Krawiecka, Klaudia, Arseny Kurnikov, Andrew Paverd, Mohammad Mannan e N. Asokan: *SafeKeeper: Protecting Web Passwords Using Trusted Execution Environments*. Em *Proceedings of the 2018 World Wide Web Conference, WWW '18*, páginas 349–358, Republic and Canton of Geneva, CHE, 2018. International World Wide Web Conferences Steering Committee, ISBN 978-1-4503-5639-8. <https://doi.org/10.1145/3178876.3186101>, event-place: Lyon, France. 10, 67, 71
- [24] Sasse, M. Angela, Michelle Steves, Kat Krol e Dana Chisnell: *The Great Authentication Fatigue – And How to Overcome It*. Em Hutchison, David, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Alfred Kobsa, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Demetri Terzopoulos, Doug Tygar, Gerhard Weikum e P. L. Patrick Rau (editores): *Cross-Cultural Design*, volume 8528, páginas 228–239. Springer International Publishing, Cham, 2014, ISBN 978-3-319-07307-1 978-3-319-07308-8. [http://link.springer.com/10.1007/978-3-319-07308-8\\_23](http://link.springer.com/10.1007/978-3-319-07308-8_23), acesso em 2024-02-26, Series Title: Lecture Notes in Computer Science. 10, 19
- [25] Sun, San Tsai, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey e Konstantin Beznosov: *Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model*. ACM Transactions on Internet Technology, 13(1):1–35, novembro 2013, ISSN 1533-5399, 1557-6051. <https://dl.acm.org/doi/10.1145/2532639>, acesso em 2023-08-22. 11, 14, 66, 68, 157
- [26] Pandey, Prashant e T N Nisha: *Challenges in Single Sign-On*. Journal of Physics: Conference Series, 1964(4):042016, julho 2021, ISSN 1742-6588, 1742-6596. <https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042016>, acesso em 2024-03-16. 11
- [27] Wang, Guilin, Jiangshan Yu e Qi Xie: *Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks*. IEEE Transactions on Industrial Informatics, 9(1):294–302, fevereiro 2013, ISSN 1551-3203, 1941-0050. <http://ieeexplore.ieee.org/document/6289362/>, acesso em 2024-03-16. 12

- [28] Beltran, Victoria: *Characterization of web single sign-on protocols*. IEEE Communications Magazine, 54(7):24–30, julho 2016, ISSN 0163-6804. <http://ieeexplore.ieee.org/document/7514160/>, acesso em 2024-03-16. 12, 14, 15, 16, 157
- [29] Neuman, B.C. e T. Ts'o: *Kerberos: an authentication service for computer networks*. IEEE Communications Magazine, 32(9):33–38, setembro 1994, ISSN 0163-6804. <http://ieeexplore.ieee.org/document/312841/>, acesso em 2024-03-16. 13
- [30] Bazaz, Tayibia e Aqeel Khaliq: *A Review on Single Sign on Enabling Technologies and Protocols*. International Journal of Computer Applications, 151(11):18–25, outubro 2016, ISSN 09758887. <http://www.ijcaonline.org/archives/volume151/number11/bazaz-2016-ijca-911938.pdf>, acesso em 2024-03-16. 13, 14, 157
- [31] Gross, T.: *Security analysis of the SAML single sign-on browser/artifact profile*. Em *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, páginas 298–307, Las Vegas, Nevada, USA, 2003. IEEE, ISBN 978-0-7695-2041-4. <http://ieeexplore.ieee.org/document/1254334/>, acesso em 2024-03-16. 13
- [32] Radha, V. e D. Hitha Reddy: *A Survey on Single Sign-On Techniques*. Procedia Technology, 4:134–139, 2012, ISSN 22120173. <https://linkinghub.elsevier.com/retrieve/pii/S2212017312002988>, acesso em 2024-03-16. 14
- [33] Siriwardena, Prabath: *Advanced API Security: OAuth 2.0 and Beyond*. Apress, Berkeley, CA, 2020, ISBN 978-1-4842-2049-8 978-1-4842-2050-4. <http://link.springer.com/10.1007/978-1-4842-2050-4>, acesso em 2024-03-17. 15, 16, 24, 157
- [34] Wilson, Yvonne e Abhishek Hingnikar: *Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0*. Apress, Berkeley, CA, 2019, ISBN 978-1-4842-5094-5 978-1-4842-5095-2. <http://link.springer.com/10.1007/978-1-4842-5095-2>, acesso em 2024-03-18. 16, 17, 24, 27
- [35] Preukschat, Alexander e Drummond Reed: *Self-sovereign identity: decentralized digital identity and verifiable credentials*. Manning, Shelter Island, 2021, ISBN 978-1-61729-659-8. OCLC: on1249104674. 18
- [36] Governo Digital, Secretaria de: *Roteiro de Integração do Login Único — Roteiro de Integração do Login Único documentation*, 2024. <https://acesso.gov.br/roteiro-tecnico/>, acesso em 2024-03-19. 19, 23, 24
- [37] Brasil, Governo Federal do: *Saiba mais sobre os níveis da conta gov.br*, 2024. <https://www.gov.br/governodigital/pt-br/identidade/conta-gov-br/niveis-da-conta-govbr/saiba-mais-sobre-os-niveis-da-conta-govbr>, acesso em 2024-03-19. 20, 21
- [38] Brasil, Governo Federal do: *Serviço de Integração aos Produtos de Identidade Digital gov.br*, 2024. <https://www.gov.br/governodigital/pt-br/transformacao-digital/servico-de-integracao-aos-produtos-de-identidade-digital-gov.br/>

servico-de-integracao-aos-produtos-de-identidade-digital-gov.br, acesso em 2024-03-19. 22

- [39] Dados (SERPRO), Serviço Federal de Processamento de e Empresa de Tecnologia e Informações da Previdência (Dataprev): *Componentes / Signin - Tipo Externo Com Texto Storybook*, 2024. <https://webcomponent-ds.estaleiro.serpro.gov.br/?path=/story/componentes-signin--tipo-externo-com-texto>, acesso em 2024-03-19. 23
- [40] GitHub: *Repository Search results - GitHub*, 2024. <https://github.com/search?q=openid+connect+client&type=repositories>, acesso em 2024-03-20. 27
- [41] Shneiderman, Ben e Catherine Plaisant: *Designing the user interface: strategies for effective human-computer interaction*. Pearson/Addison-Wesley, Boston, Mass. Munich, 4. ed edição, 2005, ISBN 978-0-321-19786-3. 27
- [42] Barbosa, Simone Diniz Junqueira e Bruno Santana da Silva: *Interação humano-computador*. Elsevier, 2011, ISBN 978-85-352-1120-7. 27
- [43] Grudin, Jonathan: *A Moving Target—The Evolution of Human-Computer Interaction*. Em *Human-Computer Interaction Handbook*, volume 20126252, páginas xxvii – lxi. CRC Press, maio 2012, ISBN 978-1-4398-2943-1 978-1-4398-2944-8. 27
- [44] Shackel, Brian: *Ergonomics for a computer*. Design, (120):36–39, 1959. <https://www.hcibook.com/e3-images/online/not-all-about-technology/shackel-1959.pdf>. 28
- [45] Carroll, John M.: *Human-computer interaction: psychology as a science of design*. International Journal of Human-Computer Studies, 46(4):501–522, abril 1997, ISSN 10715819. <https://linkinghub.elsevier.com/retrieve/pii/S1071581996901019>, acesso em 2024-03-14. 28
- [46] Olson, Gary M. e Judith S. Olson: *Human-Computer Interaction: Psychological Aspects of the Human Use of Computing*. Annual Review of Psychology, 54(1):491–516, 2003. <https://doi.org/10.1146/annurev.psych.54.101601.145044>, \_eprint: <https://doi.org/10.1146/annurev.psych.54.101601.145044>. 28
- [47] Preece, Jenny, Yvonne Rogers e Helen Sharp: *Interaction design: beyond human-computer interaction*. J. Wiley & Sons, New York, NY, 2002, ISBN 978-0-471-49278-8 978-0-471-40249-7. 28, 32, 35, 37, 42, 157
- [48] Lecerof, A. e F. Paterno: *Automatic support for usability evaluation*. IEEE Transactions on Software Engineering, 24(10):863–888, outubro 1998, ISSN 00985589. <http://ieeexplore.ieee.org/document/729686/>, acesso em 2024-02-25. 29
- [49] Lewis, James R.: *Usability Testing*. Em *E-effective Writing for E-Learning Environments*. Idea Group Inc., 2001. 29, 42

- [50] Lazar, Jonathan, Jinjuan Heidi Feng e Harry Hochheiser (editores): *Research Methods in Human Computer Interaction (Second Edition)*. Morgan Kaufmann, Boston, second edition edição, 2017, ISBN 978-0-12-805390-4. <https://www.sciencedirect.com/science/article/pii/B9780128053904099854>. 29, 30, 33, 36
- [51] Ghasemifard, Najmeh, Mahboubeh Shamsi e Abol Reza Rasouli Kenari: *A New View at Usability Test Methods of Interfaces for Human Computer Interaction*. 2015. 29, 30, 33
- [52] Buchler, Justus: *The Concept of Method*. Columbia University Press, dezembro 1961, ISBN 978-0-231-89271-1. <https://www.degruyter.com/document/doi/10.7312/buch93240/html>, acesso em 2024-02-11. 29
- [53] Rubin, Jeffrey e Dana Chisnell: *Handbook of usability testing: how to plan, design, and conduct effective tests*. Wiley Pub, Indianapolis, IN, 2nd ed edição, 2008, ISBN 978-0-470-18548-3. OCLC: ocn212204392. 29, 37, 44, 45, 84, 88
- [54] Nielsen, Jakob e Rolf Molich: *Heuristic evaluation of user interfaces*. Em *Proceedings of the SIGCHI conference on Human factors in computing systems Empowering people - CHI '90*, páginas 249–256, Seattle, Washington, United States, 1990. ACM Press, ISBN 978-0-201-50932-8. <http://portal.acm.org/citation.cfm?doid=97243.97281>, acesso em 2024-02-12. 30
- [55] Nielsen, Jakob: *Enhancing the explanatory power of usability heuristics*. Em *Proceedings of the SIGCHI conference on Human factors in computing systems celebrating interdependence - CHI '94*, páginas 152–158, Boston, Massachusetts, United States, 1994. ACM Press, ISBN 978-0-89791-650-9. <http://portal.acm.org/citation.cfm?doid=191666.191729>, acesso em 2024-02-12. 30
- [56] Abulfaraj, Anas e Adam Steele: *Detailed Usability Heuristics: A Breakdown of Usability Heuristics to Enhance Comprehension for Novice Evaluators*. Em Stephanidis, Constantine, Aaron Marcus, Elizabeth Rosenzweig, Pei Luen Patrick Rau, Abbas Moallem e Matthias Rauterberg (editores): *HCI International 2020 - Late Breaking Papers: User Experience Design and Case Studies*, volume 12423, páginas 3–18. Springer International Publishing, Cham, 2020, ISBN 978-3-030-60113-3 978-3-030-60114-0. [http://link.springer.com/10.1007/978-3-030-60114-0\\_1](http://link.springer.com/10.1007/978-3-030-60114-0_1), acesso em 2024-02-12, Series Title: Lecture Notes in Computer Science. 30
- [57] Abulfaraj, Anas e Adam Steele: *Coherent Heuristic Evaluation (CoHE): Toward Increasing the Effectiveness of Heuristic Evaluation for Novice Evaluators*. Em Marcus, Aaron e Elizabeth Rosenzweig (editores): *Design, User Experience, and Usability. Interaction Design*, volume 12200, páginas 3–20. Springer International Publishing, Cham, 2020, ISBN 978-3-030-49712-5 978-3-030-49713-2. [http://link.springer.com/10.1007/978-3-030-49713-2\\_1](http://link.springer.com/10.1007/978-3-030-49713-2_1), acesso em 2024-02-12, Series Title: Lecture Notes in Computer Science. 30

- [58] Polson, Peter G., Clayton Lewis, John Rieman e Cathleen Wharton: *Cognitive walkthroughs: a method for theory-based evaluation of user interfaces*. International Journal of Man-Machine Studies, 36(5):741–773, maio 1992, ISSN 00207373. <https://linkinghub.elsevier.com/retrieve/pii/002073739290039N>, acesso em 2024-02-12. 30
- [59] Polson, Peter e Clayton Lewis: *Theory-Based Design for Easily Learned Interfaces*. Human-Computer Interaction, 5(2):191–220, junho 1990, ISSN 0737-0024. [http://www.informaworld.com/openurl?genre=article&doi=10.1207/s15327051hci0502&3\\_3&magic=crossref|D404A21C5BB053405B1A640AFFD44AE3](http://www.informaworld.com/openurl?genre=article&doi=10.1207/s15327051hci0502&3_3&magic=crossref|D404A21C5BB053405B1A640AFFD44AE3), acesso em 2024-02-12. 30
- [60] Jeffries, Robin, James R. Miller, Cathleen Wharton e Kathy Uyeda: *User interface evaluation in the real world: a comparison of four techniques*. Em *Proceedings of the SIGCHI conference on Human factors in computing systems Reaching through technology - CHI '91*, páginas 119–124, New Orleans, Louisiana, United States, 1991. ACM Press, ISBN 978-0-89791-383-6. <http://portal.acm.org/citation.cfm?doid=108844.108862>, acesso em 2024-02-12. 31
- [61] Jacobsen, Niels Ebbe: *Usability Evaluation Methods*. Tese de Doutorado, University of Copenhagen, 1999. 31
- [62] Beyer, Hugh e Karen Holtzblatt: *Contextual design: defining customer-centered systems*. Morgan Kaufmann, San Francisco, Calif, 1998, ISBN 978-1-55860-411-7. 31
- [63] Beyer, Hugh e Karen Holtzblatt: *Contextual design*. Interactions, 6(1):32–42, janeiro 1999, ISSN 1072-5520, 1558-3449. <https://dl.acm.org/doi/10.1145/291224.291229>, acesso em 2024-02-13. 32
- [64] Holtzblatt, Karen e Hugh Beyer: *Contextual Design: Evolved*. Synthesis Lectures on Human-Centered Informatics. Springer International Publishing, Cham, 2015, ISBN 978-3-031-01079-8 978-3-031-02207-4. <https://link.springer.com/10.1007/978-3-031-02207-4>, acesso em 2024-02-12. 33
- [65] Bastien, J.M. Christian: *Usability testing: a review of some methodological and technical aspects of the method*. International Journal of Medical Informatics, 79(4):e18–e23, abril 2010, ISSN 13865056. <https://linkinghub.elsevier.com/retrieve/pii/S1386505608002098>, acesso em 2024-02-09. 33, 81
- [66] Tullis, Tom e Bill Albert: *Measuring the user experience: collecting, analyzing, and presenting usability metrics*. The Morgan Kaufmann interactive technologies series. Elsevier/Morgan Kaufmann, Amsterdam ; Boston, 2008, ISBN 978-0-12-373558-4. 34, 81
- [67] Hass, Christopher: *A Practical Guide to Usability Testing*. Em Edmunds, Margo, Christopher Hass e Erin Holve (editores): *Consumer Informatics and Digital Health*, páginas 107–124. Springer International Publishing, Cham, 2019, ISBN 978-3-319-96904-6 978-3-319-96906-0. [http://link.springer.com/10.1007/978-3-319-96906-0\\_6](http://link.springer.com/10.1007/978-3-319-96906-0_6), acesso em 2024-02-25. 34, 82

- [68] Blomberg, Jeanette e Mark Burrell: *An Ethnographic Approach to Design*. Em *Human-Computer Interaction Handbook*, volume 20126252, páginas 1025–1052. CRC Press, maio 2012, ISBN 978-1-4398-2943-1 978-1-4398-2944-8. <http://www.crcnetbase.com/doi/abs/10.1201/b11963-52>, acesso em 2024-03-12, Series Title: Human Factors and Ergonomics. 35
- [69] Albert, William e Thomas S. Tullis: *Measuring the user experience: collecting, analyzing, and presenting UX metrics*. Morgan Kaufmann, Cambridge, 3e ed edição, 2023, ISBN 978-0-12-818080-8. 35, 43, 45, 82, 125
- [70] Lindgaard, Gitte e Jarinee Chattratchart: *Usability testing: what have we overlooked?* Em *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, páginas 1415–1424, San Jose California USA, abril 2007. ACM, ISBN 978-1-59593-593-9. <https://dl.acm.org/doi/10.1145/1240624.1240839>, acesso em 2024-02-25. 37
- [71] Kwang Bok Lee e R.A. Grice: *Developing a new usability testing method for mobile devices*. Em *International Professional Communication Conference, 2004. IPCC 2004. Proceedings.*, páginas 115–127, Minneapolis, MN, USA, 2004. IEEE, ISBN 978-0-7803-8467-5. <http://ieeexplore.ieee.org/document/1375285/>, acesso em 2024-02-22. 37, 38, 44
- [72] Rotaru, Oana Alexandra, Silviu Vert, Radu Vasii e Diana Andone: *Standardised Questionnaires in Usability Evaluation. Applying Standardised Usability Questionnaires in Digital Products Evaluation*. Em Lopata, Audrius, Rita Butkienė, Daina Gudonienė e Vilma Sukackė (editores): *Information and Software Technologies*, volume 1283, páginas 39–48. Springer International Publishing, Cham, 2020, ISBN 978-3-030-59505-0 978-3-030-59506-7. [http://link.springer.com/10.1007/978-3-030-59506-7\\_4](http://link.springer.com/10.1007/978-3-030-59506-7_4), acesso em 2024-03-03, Series Title: Communications in Computer and Information Science. 38
- [73] Sullivan, Gail M. e Anthony R. Artino: *Analyzing and Interpreting Data From Likert-Type Scales*. *Journal of Graduate Medical Education*, 5(4):541–542, dezembro 2013, ISSN 1949-8357, 1949-8349. <https://meridian.allenpress.com/jgme/article/5/4/541/34037/> Analyzing-and-Interpreting-Data-From-LikertType, acesso em 2024-03-02. 38
- [74] Sauro, Jeff e Joseph S. Dumas: *Comparison of three one-question, post-task usability questionnaires*. Em *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, páginas 1599–1608, Boston MA USA, abril 2009. ACM, ISBN 978-1-60558-246-7. <https://dl.acm.org/doi/10.1145/1518701.1518946>, acesso em 2024-03-02. 38
- [75] Wijayarathna, Chamila, Nalin A. G. Arachchilage e Jill Slay: *A Generic Cognitive Dimensions Questionnaire to Evaluate the Usability of Security APIs*. Em Tryfonas, Theo (editor): *Human Aspects of Information Security, Privacy and Trust*, volume 10292, páginas 160–173. Springer International Publishing, Cham, 2017, ISBN 978-3-319-58459-1 978-3-319-58460-7. <https://link.springer.com/>

- 10.1007/978-3-319-58460-7\_11, acesso em 2024-01-27, Series Title: Lecture Notes in Computer Science. 38, 73
- [76] Brooke, John: *Sus: A quick and dirty usability scale*. Usability Eval. Ind., 189, novembro 1995. 39
- [77] Bangor, Aaron, Philip T. Kortum e James T. Miller: *An Empirical Evaluation of the System Usability Scale*. International Journal of Human-Computer Interaction, 24(6):574–594, julho 2008, ISSN 1044-7318, 1532-7590. <http://www.tandfonline.com/doi/abs/10.1080/10447310802205776>, acesso em 2024-03-10. 39
- [78] Ruoti, Scott, Brent Roberts e Kent Seamons: *Authentication Melee: A Usability Analysis of Seven Web Authentication Systems*. Em *Proceedings of the 24th International Conference on World Wide Web*, páginas 916–926, Florence Italy, maio 2015. International World Wide Web Conferences Steering Committee, ISBN 978-1-4503-3469-3. <https://dl.acm.org/doi/10.1145/2736277.2741683>, acesso em 2023-08-14. 39, 66, 69
- [79] Constantinides, Argyris, Marios Belk, Christos Fidas, Roy Beumers, David Vidal, Wanting Huang, Juliana Bowles, Thais Webber, Agastya Silvina e Andreas Pitsillides: *Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations*. ACM Transactions on Computing for Healthcare, 4(1):1–40, janeiro 2023, ISSN 2691-1957, 2637-8051. <https://dl.acm.org/doi/10.1145/3564610>, acesso em 2023-08-22. 39, 67, 74
- [80] Lourenço, Douglas Fabiano, Elenice Carmona Valentim e Maria Helena Baena de Moraes Lopes: *Tradução e adaptação transcultural da System Usability Scale para o português do Brasil*. Aquichan, 22(2):e2228, maio 2022. <https://aquichan.unisabana.edu.co/index.php/aquichan/article/view/16497>. 39, 120
- [81] Bangor, Aaron, Phil Kortum e James Miller: *Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale*. J. Usability Stud., 4:114–123, abril 2009. <https://uxpajournal.org/determining-what-individual-sus-scores-mean-adding-an-adjective-rating-scale/>. 41, 113
- [82] Wadkar, Sagar K., Khajan Singh, Ritu Chakravarty e Shivaji D. Argade: *Assessing the Reliability of Attitude Scale by Cronbach's Alpha*. Journal of Global Communication, 9(2):113, 2016, ISSN 0974-0600, 0976-2442. <http://www.indianjournals.com/ijor.aspx?target=ijor:jgc&volume=9&issue=2&article=008>, acesso em 2024-03-11. 41
- [83] Heo, Moonseong, Namhee Kim e Myles S. Faith: *Statistical power as a function of Cronbach alpha of instrument questionnaire items Data analysis, statistics and modelling*. BMC Medical Research Methodology, 15(1), outubro 2015, ISSN 14712288. 41

- [84] Streiner, David L.: *Starting at the beginning: an introduction to coefficient alpha and internal consistency*. *Journal of Personality Assessment*, 80(1):99–103, fevereiro 2003, ISSN 0022-3891. 41
- [85] Dumas, Joseph S. e Marilyn C. Salzman: *Usability Assessment Methods*. *Reviews of Human Factors and Ergonomics*, 2(1):109–140, abril 2006, ISSN 1557-234X, 2163-3134. <http://journals.sagepub.com/doi/10.1177/1557234X0600200105>, acesso em 2024-03-11. 41, 42
- [86] Fonteyn, Marsha E., Benjamin Kuipers e Susan J. Grobe: *A Description of Think Aloud Method and Protocol Analysis*. *Qualitative Health Research*, 3(4):430–441, novembro 1993, ISSN 1049-7323, 1552-7557. <http://journals.sagepub.com/doi/10.1177/104973239300300403>, acesso em 2024-03-11. 42
- [87] Bevan, Nigel e Miles Macleod: *Usability measurement in context*. *Behaviour & Information Technology*, 13(1-2):132–145, janeiro 1994, ISSN 0144-929X, 1362-3001. <http://www.tandfonline.com/doi/abs/10.1080/01449299408914592>, acesso em 2024-03-12. 43, 44, 45
- [88] Sauro, Jeff e James R. Lewis: *Quantifying the user experience: practical statistics for user research*. Elsevier, Morgan Kaufmann, Amsterdam Boston Heidelberg, 2nd edition edição, 2016, ISBN 978-0-12-802308-2. 44, 45, 46, 84, 101, 116, 117, 134, 140
- [89] Davis, Fred D.: *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*. *MIS Quarterly*, 13(3):319, setembro 1989, ISSN 02767783. <https://www.jstor.org/stable/249008?origin=crossref>, acesso em 2024-03-02. 45
- [90] Drexel University, David Gefen, Detmar Straub e Georgia State University: *The Relative Importance of Perceived Ease of Use in IS Adoption: A Study of E-Commerce Adoption*. *Journal of the Association for Information Systems*, 1(1):1–30, outubro 2000, ISSN 15369323. <https://aisel.aisnet.org/jais/vol1/iss1/8/>, acesso em 2024-03-13. 45
- [91] Tedesco, Donna P e Thomas S Tullis: *A Comparison of Methods for Eliciting Post-Task Subjective Ratings in Usability Testing*. 2006. 46, 84
- [92] Kitchenham, Barbara, Stuart Charters, David Budgen, Pearl Brereton, Mark Turner, Steve Linkman, Magne Jørgensen, Emilia Mendes e Giuseppe Visaggio: *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Technical Report, 2007. 48, 49, 59
- [93] Garousi, Vahid, Michael Felderer e Mika V. Mäntylä: *Guidelines for including grey literature and conducting multivocal literature reviews in software engineering*. *Information and Software Technology*, 106:101–121, fevereiro 2019, ISSN 09505849. <https://linkinghub.elsevier.com/retrieve/pii/S0950584918301939>, acesso em 2023-03-14. 49

- [94] Easterbrook, Steve, Janice Singer, Margaret Anne Storey e Daniela Damian: *Selecting Empirical Methods for Software Engineering Research*. Em Shull, Forrest, Janice Singer e Dag I. K. Sjøberg (editores): *Guide to Advanced Empirical Software Engineering*, páginas 285–311. Springer London, London, 2008, ISBN 978-1-84800-043-8 978-1-84800-044-5. [http://link.springer.com/10.1007/978-1-84800-044-5\\_11](http://link.springer.com/10.1007/978-1-84800-044-5_11), acesso em 2023-06-02. 49
- [95] Petticrew, Mark e Helen Roberts: *Systematic reviews in the social sciences: a practical guide*. Blackwell Pub, Malden, MA ; Oxford, 2006, ISBN 978-1-4051-2110-1 978-1-4051-2111-8. OCLC: ocm60360309. 50
- [96] Picalho, Antonio Carlos, Elaine Rosangela De Oliveira Lucas e Igor Soares Amorim: *Lógica booleana aplicada na construção de expressões de busca*. AtoZ: novas práticas em informação e conhecimento, 11:1, março 2022, ISSN 2237-826X. <https://revistas.ufpr.br/atoz/article/view/81838>, acesso em 2023-09-20. 50
- [97] Springer: *HCI (International Conference on Human-Computer Interaction)*, 2023. <https://www.springer.com/series/16277>, acesso em 2023-09-20. 57
- [98] Freitas, Vitor: *How to create a quality assessment checklist*, 2023. <https://parsif.al/help/how-to-create-a-quality-assessment-checklist/>, acesso em 2024-03-25. 59
- [99] Murack, Jennie: *LibGuides: Citation Management and Writing Tools: LaTeX and BibTeX*. <https://libguides.mit.edu/cite-write/bibtex>, acesso em 2023-09-15. 61
- [100] Shafranovich, Yakov: *Common Format and MIME Type for Comma-Separated Values (CSV) Files*. Request for Comments RFC 4180, Internet Engineering Task Force, outubro 2005. <https://datatracker.ietf.org/doc/rfc4180>, acesso em 2023-09-15, Num Pages: 8. 62, 107
- [101] Foundation, DOI: *The Identifier - WHAT IS A DOI?*, 2023. <https://www.doi.org/the-identifier/what-is-a-doi/>, acesso em 2023-09-15. 62
- [102] *RIS (file format)*, julho 2023. [https://en.wikipedia.org/w/index.php?title=RIS\\_\(file\\_format\)&oldid=1165815812#cite\\_note-1](https://en.wikipedia.org/w/index.php?title=RIS_(file_format)&oldid=1165815812#cite_note-1), acesso em 2023-09-15, Page Version ID: 1165815812. 62
- [103] Association, USENIX: *USENIX - The Advanced Computing Systems Association*, 2023. <https://www.usenix.org/>, acesso em 2023-09-18. 66
- [104] CONSORTIUM, THE DIVA: *DiVA - Academic Archive Online*, 2023. <https://www.info.diva-portal.org/?languageId=1>, acesso em 2023-09-18. 66
- [105] Zhao, Rui e Chuan Yue: *Toward a secure and usable cloud-based password manager for web browsers*. Computers & Security, 46:32–47, outubro 2014, ISSN 01674048. <https://linkinghub.elsevier.com/retrieve/pii/S0167404814001059>, acesso em 2023-08-22. 66, 68

- [106] Polakis, Iasonas, Panagiotis Ilia, Federico Maggi, Marco Lancini, Georgios Kontaxis, Stefano Zanero, Sotiris Ioannidis e Angelos D. Keromytis: *Faces in the Distorting Mirror: Revisiting Photo-Based Social Authentication*. Em *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14*, páginas 501–512, New York, NY, USA, 2014. Association for Computing Machinery, ISBN 978-1-4503-2957-6. <https://doi.org/10.1145/2660267.2660317>, event-place: Scottsdale, Arizona, USA. 66, 69
- [107] Catuogno, Luigi e Clemente Galdi: *On user authentication by means of video events recognition*. *Journal of Ambient Intelligence and Humanized Computing*, 5(6):909–918, dezembro 2014, ISSN 1868-5137, 1868-5145. <http://link.springer.com/10.1007/s12652-014-0248-5>, acesso em 2023-08-15. 66, 69
- [108] Wang, Tianhao, Huangyi Ge, Omar Chowdhury, Hemanta K. Maji e Ninghui Li: *On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols*. Em *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, páginas 603–615, Vienna Austria, outubro 2016. ACM, ISBN 978-1-4503-4139-4. <https://dl.acm.org/doi/10.1145/2976749.2978417>, acesso em 2023-08-20. 66, 70
- [109] Karegar, Farzaneh, Daniel Lindergren, John Sören Pettersson e Simone Fischer-Hübner: *Assessments of a cloud-based data wallet for personal identity management*. Em *Information Systems Development: Advances in Methods, Tools and Management - Proceedings of the 26th International Conference on Information Systems Development, ISD 2017*, 2017. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073976551&partnerID=40&md5=66d8c19bc509f4fd62950201896d85db>, Type: Conference paper. 67, 70
- [110] Peeters, Roel, Jens Hermans, Pieter Maene, Katri Grenman, Kimmo Halunen e Juha Häikiö: *n-Auth: Mobile Authentication Done Right*. Em *Proceedings of the 33rd Annual Computer Security Applications Conference*, páginas 1–15, Orlando FL USA, dezembro 2017. ACM, ISBN 978-1-4503-5345-8. <https://dl.acm.org/doi/10.1145/3134600.3134613>, acesso em 2023-08-22. 67, 70
- [111] Weidman, Jake e Jens Grossklags: *I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication*. Em *Proceedings of the 33rd Annual Computer Security Applications Conference, ACSAC '17*, páginas 212–224, New York, NY, USA, 2017. Association for Computing Machinery, ISBN 978-1-4503-5345-8. <https://doi.org/10.1145/3134600.3134629>, event-place: Orlando, FL, USA. 67, 71, 85
- [112] Karegar, Farzaneh, Nina Gerber, Melanie Volkamer e Simone Fischer-Hübner: *Helping John to Make Informed Decisions on Using Social Login*. Em *Proceedings of the 33rd Annual ACM Symposium on Applied Computing, SAC '18*, páginas 1165–1174, New York, NY, USA, 2018. Association for Computing Machinery, ISBN 978-1-4503-5191-1. <https://doi.org/10.1145/3167132.3167259>, event-place: Pau, France. 67, 72, 82

- [113] Das, Sanchari, Gianpaolo Russo, Andrew C. Dingman, Jayati Dev, Olivia Kenny e L. Jean Camp: *A Qualitative Study on Usability and Acceptability of Yubico Security Key*. Em *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, STAST '17, páginas 28–39, New York, NY, USA, 2018. Association for Computing Machinery, ISBN 978-1-4503-6357-0. <https://doi.org/10.1145/3167996.3167997>, event-place: Orlando, Florida, USA. 67, 72
- [114] Wijayarathna, Chamila e Nalin A. G. Arachchilage: *An Empirical Usability Analysis of the Google Authentication API*. Em *Proceedings of the 23rd International Conference on Evaluation and Assessment in Software Engineering*, EASE '19, páginas 268–274, New York, NY, USA, 2019. Association for Computing Machinery, ISBN 978-1-4503-7145-2. <https://doi.org/10.1145/3319008.3319350>, event-place: Copenhagen, Denmark. 67, 72
- [115] Aebischer, Seb, Claudio Dettoni, Graeme Jenkinson, Kat Krol, David Llewellyn-Jones, Toshiyuki Masui e Frank Stajano: *Deploying authentication in the wild: towards greater ecological validity in security usability studies*. *Journal of Cybersecurity*, 6(1):tyaa010, janeiro 2020, ISSN 2057-2085, 2057-2093. <https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyaa010/5989371>, acesso em 2023-08-22. 67, 73
- [116] Owens, Kentrell, Olabode Anise, Amanda Krauss e Blase Ur: *User perceptions of the usability and security of smartphones as FIDO2 roaming authenticators*. Em *Proceedings of the 17th Symposium on Usable Privacy and Security, SOUPS 2021*, páginas 57 – 76, 2021. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114520581&partnerID=40&md5=ca152ff19294a38ce667779dd6b18a71>, Type: Conference paper. 67, 73
- [117] Korir, Maina, Simon Parkin e Paul Dunphy: *An Empirical Study of a Decentralized IdentityWallet: Usability, Security, and Perspectives on User Control*. Em *Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS 2022*, páginas 195 – 211, 2022. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140874129&partnerID=40&md5=d1ca37a97e5971895064184f9e4a1ce4>, Type: Conference paper. 67, 73
- [118] Huh, Jun Ho, Hyejin Shin, HongMin Kim, Eunyong Cheon, Youngeun Song, Choong Hoon Lee e Ian Oakley: *WristAcoustic: Through-Wrist Acoustic Response Based Authentication for Smartwatches*. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 6(4), janeiro 2023. <https://doi.org/10.1145/3569473>, Place: New York, NY, USA Publisher: Association for Computing Machinery. 67, 74
- [119] Chiasson, Sonia, P C van Oorschot e Robert Biddle: *A Usability Study and Critique of Two Password Managers*. *Security '06: 15th USENIX Security Symposium*, 2006. 69
- [120] Amazon: *Amazon Mechanical Turk*, 2024. <https://www.mturk.com/>, acesso em 2024-01-23. 70

- [121] Consortium, CREDENTIAL: *Credential*, 2024. <https://credential.eu/>, acesso em 2024-01-23. 70
- [122] Malhotra, Naresh K., Sung S. Kim e James Agarwal: *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*. Information Systems Research, 15(4):336–355, 2004, ISSN 10477047, 15265536. <http://www.jstor.org/stable/23015787>, acesso em 2024-01-26, Publisher: INFORMS. 72
- [123] Alliance, FIDO: *What is FIDO*, 2024. <https://fidoalliance.org/what-is-fido/>, acesso em 2024-01-27. 73
- [124] Kenneally, Erin e David Dittrich: *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. SSRN Electronic Journal, 2012, ISSN 1556-5068. <http://www.ssrn.com/abstract=2445102>, acesso em 2024-01-29. 74
- [125] Federal, Senado: *Sobre: Portal e-Cidadania - Senado Federal*, 2024. <https://www12.senado.leg.br/ecidadania/sobre>, acesso em 2024-03-20. 82
- [126] IBGE: *Panorama do Censo 2022*, 2022. <https://censo2022.ibge.gov.br/panorama/>, acesso em 2024-03-20. 82, 85
- [127] Federal, Senado: *Sobre o DataSenado*, 2024. <https://www12.senado.leg.br/institucional/datasenado/sobre>, acesso em 2024-11-06. 82, 96
- [128] Brasília, Universidade de: *CEP CHS - QUE PROJETOS DEVEM SER ENVIADOS AO CEP/CHS*, 2024. <https://www.cepchs.unb.br/que-projetos-devem-ser-enviados-ao-cep-chs>, acesso em 2024-11-06. 94
- [129] Brasília, Universidade de: *CEP CHS - Histórico*, 2024. <https://www.cepchs.unb.br/historico>, acesso em 2024-11-06. 94
- [130] Brasil, Governo Federal do: *Plataforma Brasil*, 2024. <https://plataformabrasil.saude.gov.br/visao/publico/indexPublico.jsf>, acesso em 2024-11-06. 95
- [131] Brasília, Universidade de: *CEP CHS - Fluxograma*, 2025. <https://www.cepchs.unb.br/fluxograma>, acesso em 2025-03-18. 95
- [132] Oliveira, Marcos Ruben de, Marina Barros de Oliveira, Roberto de, S Marques Buffone e Aretha Pessanha Cordeiro: *Delineamento amostral das pesquisas DataSenado*. Anais da VI Escola de Amostragem e Métodos de Pesquisa, 2023. 98
- [133] DataSenado, Instituto: *Pesquisa sobre a Integração do e-Cidadania ao GOV.BR*. A ser publicado, 2024. 98
- [134] Bordens, Kenneth S. e Bruce B. Abbott: *Research design and methods: a process approach*. McGraw-Hill, New York, 8th ed edição, 2011, ISBN 978-0-07-353202-8. OCLC: ocn436028182. 101, 126

- [135] SendPulse: *Ferramenta de Automação de Marketing* / SendPulse, 2024. <https://sendpulse.com/br>, acesso em 2024-11-30. 107
- [136] SendPulse: *Política de privacidade* / SendPulse, 2024. <https://sendpulse.com/br/legal/pp>, acesso em 2024-11-30. 107
- [137] Microsoft: *Como usar o recurso de mala direta no Word para criar e imprimir cartas que usam os dados de uma planilha do Excel - Suporte da Microsoft*, 2024. <https://support.microsoft.com/pt-br/topic/como-usar-o-recurso-de-mala-direta-no-word-para-criar-e-imprimir-cartas-que-usam>, acesso em 2024-11-30. 107
- [138] Blattgerste, Jonas, Jan Behrends e Thies Pfeiffer: *A web-based analysis toolkit for the system usability scale*. Em *Proceedings of the 15th International Conference on PErvasive Technologies Related to Assistive Environments*, PETRA '22, página 237–246, New York, NY, USA, 2022. Association for Computing Machinery, ISBN 9781450396318. <https://doi.org/10.1145/3529190.3529216>. 113, 117
- [139] Shapiro, S. S. e M. B. Wilk: *An analysis of variance test for normality (complete samples)*. *Biometrika*, 52(3-4):591–611, dezembro 1965, ISSN 0006-3444, 1464-3510. <https://academic.oup.com/biomet/article-lookup/doi/10.1093/biomet/52.3-4.591>, acesso em 2025-01-21. 117
- [140] Cohen, Jacob: *Statistical Power Analysis for the Behavioral Sciences*. Taylor and Francis, Hoboken, 2nd ed edição, 2013, ISBN 978-0-8058-0283-2. 118
- [141] Solís Salazar, Martín: *The dilemma of combining positive and negative items in scales*. *Psicothema*, 2(27):192–199, maio 2015, ISSN 0214-9915, 1886-144X. <https://www.psicothema.com/pii?pii=4253>, acesso em 2025-02-04. 120
- [142] Vallat, Raphael: *Pingouin: statistics in python*. *Journal of Open Source Software*, 3(31):1026, novembro 2018. 120
- [143] Schrepp, Martin: *On the usage of Cronbach's Alpha to measure reliability of UX scales*. *J. Usability Studies*, 15(4):247–258, agosto 2020. Place: Bloomingdale, IL Publisher: Usability Professionals' Association. 124
- [144] Streiner, David L.: *Being Inconsistent About Consistency: When Coefficient Alpha Does and Doesn't Matter*. *Journal of Personality Assessment*, 80(3):217–222, junho 2003, ISSN 0022-3891. 124
- [145] VideoLan: *Vlc media player*, 2006. <https://www.videolan.org/vlc/index.html>. 129
- [146] Mederi: *Jump to time Previous frame v3*, fevereiro 2018. <https://addons.videolan.org/p/1154013/>, acesso em 2025-02-14. 129
- [147] Bradski, G.: *The OpenCV Library*. *Dr. Dobb's Journal of Software Tools*, 2000. 129

- [148] Haukoos, Jason S. e Roger J. Lewis: *Advanced Statistics: Bootstrapping Confidence Intervals for Statistics with “Difficult” Distributions*. Academic Emergency Medicine, 12(4):360–365, abril 2005, ISSN 1069-6563, 1553-2712. <https://onlinelibrary.wiley.com/doi/10.1197/j.aem.2004.11.018>, acesso em 2025-03-09. 135
- [149] Cureton, Edward E.: *Rank-Biserial Correlation*. Psychometrika, 21(3):287–290, setembro 1956, ISSN 0033-3123, 1860-0980. [https://www.cambridge.org/core/product/identifier/S0033312300047839/type/journal\\_article](https://www.cambridge.org/core/product/identifier/S0033312300047839/type/journal_article), acesso em 2025-02-24. 136
- [150] Schober, Patrick, Christa Boer e Lothar A. Schwarte: *Correlation Coefficients: Appropriate Use and Interpretation*. Anesthesia & Analgesia, 126(5):1763–1768, maio 2018, ISSN 0003-2999. <https://journals.lww.com/00000539-201805000-00050>, acesso em 2025-02-25. 138
- [151] Lam, H.: *A Framework of Interaction Costs in Information Visualization*. IEEE Transactions on Visualization and Computer Graphics, 14(6):1149–1156, novembro 2008, ISSN 1077-2626. <http://ieeexplore.ieee.org/document/4658124/>, acesso em 2025-03-17. 149
- [152] Redmon, Joseph, Santosh Divvala, Ross Girshick e Ali Farhadi: *You Only Look Once: Unified, Real-Time Object Detection*, 2015. <https://arxiv.org/abs/1506.02640>, acesso em 2025-03-22, Version Number: 5. 163
- [153] Gruber, John: *Daring Fireball: Markdown*, 2004. <https://daringfireball.net/projects/markdown/>, acesso em 2025-04-03. 185

# Apêndices A

## Formulários de Pesquisa

### A.1 Formulário de Recrutamento

A pesquisa levará aproximadamente 5 minutos para ser concluída.

Este questionário visa mensurar o grau de conhecimento que as pessoas têm da *Conta gov.br* e do sistema e-Cidadania do Senado Federal. Ele também servirá de base para identificar pessoas que se interessem em fazer um teste de utilização do e-Cidadania integrado à *Conta gov.br*, que tem como objetivo avaliar a usabilidade da solução.

Essa pesquisa faz parte da dissertação de Mestrado do Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília do aluno Demétrius de Almeida Jubé (demetrius.jube@aluno.unb.br).

**DECLARAÇÃO DE CONSENTIMENTO INFORMADO** Ao responder a esta pesquisa, você permite que o pesquisador obtenha, use e divulgue as informações anônimas fornecidas conforme descrito abaixo.

#### CONDIÇÕES E ESTIPULAÇÕES

1. Eu entendo que todas as informações são confidenciais. Não serei identificado pessoalmente. Concordo em preencher a pesquisa para fins de pesquisa e que os dados derivados desta pesquisa anônima podem ser publicados em periódicos, conferências e postagens de blog.
2. Eu entendo que minha participação nesta pesquisa é totalmente voluntária e que a recusa em participar não implicará em nenhuma penalidade ou perda de benefícios. Se eu quiser, posso cancelar minha participação a qualquer momento. Também entendo que, se decidir participar, posso recusar-me a responder a qualquer pergunta que não me sinta confortável em responder.
3. Entendo que posso entrar em contato com o pesquisador se tiver alguma dúvida sobre a pesquisa. Estou ciente de que meu consentimento não me beneficiará

diretamente. Também estou ciente de que o autor manterá os dados coletados perpetuamente e poderá utilizar os dados para trabalhos acadêmicos futuros.

4. Ao clicar no botão abaixo, eu livremente concordo e reconheço meus direitos como um participante voluntário da pesquisa conforme descrito acima e concedo consentimento ao pesquisador para usar minhas informações na realização de pesquisas nas áreas mencionadas acima

## QUESTIONÁRIO

QUESTÃO 1: Qual a sua faixa de idade?

- 15 a 29 anos
- 30 a 44 anos
- 45 a 59 anos
- Acima de 60 anos
- Prefiro não informar

QUESTÃO 2: Qual o seu gênero?

- Masculino
- Feminino
- Outro (Qual?)
- Prefiro não informar

QUESTÃO 3: Qual o seu grau de instrução?

- Educação Básica
- Ensino Médio
- Graduação
- Pós-Graduação
- Prefiro não informar

QUESTÃO 4: Como você classifica sua habilidade com uso de soluções de tecnologia da informação (Ex: Uso de redes sociais, aplicativos, editores de texto, planilhas, navegação por sites)? Escala de 7 pontos desde Acho Muito Difícil até Acho Muito Fácil

QUESTÃO 5: Você conhece o sistema e-Cidadania do Senado Federal? (Sim/-Não)

QUESTÃO 6: Você já usou a **Conta gov.br**, utilizada como login para acessar serviços do SUS, inscrever-se no ENEM, consultar sua CNH ou Carteira de Trabalho digital, simular aposentadoria no Meu INSS, entre outros serviços? (Sim/Não/Não tenho certeza)

QUESTÃO 7: Você teria interesse em participar de um teste de utilização dessas soluções? Ele seria feito em um momento posterior, combinado com você, e

duraria cerca de 30 minutos. (Sim/Não)

(Se tem interesse em participar do teste)

A investigação segue critérios de distribuição para selecionar os participantes, de modo que nem todos os inscritos serão convidados a integrar o estudo. Todos os candidatos serão informados sobre sua situação, seja ela de seleção ou não para participar da pesquisa. Aqueles escolhidos receberão detalhes sobre as próximas etapas.

Para viabilizar sua participação no teste de usabilidade das ferramentas e-Cidadania e Conta gov.br, precisamos coletar dados pessoais. Esses dados serão conhecidos apenas pelos pesquisadores, sendo tratados como confidenciais, porém suas respostas deixarão de ser anônimas. Caso concorde com essas condições, preencha os dados que se seguem.

QUESTÃO 8: Qual o seu nome completo?

QUESTÃO 9: Qual o seu e-mail de contato?

QUESTÃO 10: Possui acesso a um computador com conexão à Internet, Câmera e Microfone? (Sim/Não)

## A.2 Formulário de Avaliação da Sessão de Teste

Este questionário busca avaliar as impressões em relação ao procedimento de teste em si. Fique à vontade para falar a sua opinião sincera para que possamos melhorá-lo.

1. De uma forma geral, fazer as tarefas do teste foi algo: Escala de 7 pontos desde Muito Difícil até Muito Fácil
2. Qual o nível de clareza das instruções fornecidas para a reunião? Escala de 7 pontos desde Muito confusas até Muito simples
3. As atividades de permitir a utilização do microfone e câmera e o Compartilhamento de Tela foram atividades: Escala de 7 pontos desde Muito Difíceis até Muito Fáceis
4. O tempo de realização do teste foi: Insuficiente, Adequado, Muito longo
5. Há alguma sugestão que queira dar para facilitar o teste? Pergunta aberta

## Apêndices B

### Termo de Consentimento Livre e Esclarecido

## Termo de Consentimento Livre e Esclarecido

Você está sendo convidado a participar da pesquisa "*Análise da usabilidade da Conta gov.br para adoção pelo Senado Federal*", de responsabilidade de *Demétrius de Almeida Jubé*, estudante de *mestrado* do *Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília*. O objetivo desta pesquisa é *avaliar os benefícios em relação à usabilidade que a incorporação da Conta gov.br trouxe para o sistema e-Cidadania do Senado Federal*. Assim, gostaria de consultá-lo/a sobre seu interesse e disponibilidade de cooperar com a pesquisa.

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, tais como questionários, entrevistas, fitas de gravação ou filmagem, ficarão sob a guarda do/da pesquisador/a responsável pela pesquisa.

A coleta de dados será realizada por meio de *gravação da interação dos usuários com a plataforma e-Cidadania e resposta a questionários após a realização de um roteiro de tarefas*. É para estes procedimentos que você está sendo convidado a participar. Sua participação na pesquisa pode implicar em riscos tais como: *exposição de dados pessoais, exposição de credenciais, exposição acidental de dados durante a gravação e exposição não-autorizada do vídeo do teste*. Estes riscos serão minimizados com as seguintes estratégias: *guarda das informações através de acesso conhecido apenas pelo pesquisador, com uso de duplo fator de autenticação, uso de um computador específico e não-compartilhado para análise dos dados, utilização de credenciais de teste fictícias, orientação prévia para evitar compartilhamento de tela com aplicativos em uso e manutenção das gravações em um computador local, com acesso restrito ao pesquisador, e posterior salvamento em um HD criptografado*.

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 irá acarretar qualquer penalidade ou perda de benefícios.

Se você tiver qualquer dúvida em relação à pesquisa, você pode me contatar através do telefone *61 99287-3194* ou pelo e-mail *demetrius.jube@aluno.unb.br*.

A equipe de pesquisa informa que os resultados do estudo podem ser publicados posteriormente na comunidade científica, e podem ser dados a qualquer um dos participantes mediante solicitação direta à equipe.

Este projeto foi revisado e aprovado pelo Comitê de Ética em Pesquisa em Ciências Humanas e Sociais (CEP/CHS) da Universidade de Brasília. As informações com relação à assinatura do TCLE ou aos direitos do participante da pesquisa podem ser obtidas por meio do e-mail do CEP/CHS: *cep\_chs@unb.br* ou pelo telefone: (61) 3107 1592.

Este documento foi elaborado em duas vias, uma ficará com o/a pesquisador/a responsável pela pesquisa e a outra com você.

\_\_\_\_\_  
Assinatura do/da participante

\_\_\_\_\_  
Assinatura do/da pesquisador/a

Brasília, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_

# Apêndices C

## Guia de Implantação da Conta gov.br

### C.1 Guia Prático para Adoção da *Conta gov.br*

O Guia Prático para Adoção da *Conta gov.br* foi escrito em formato *markdown* [153], uma linguagem de marcação simples que é comumente utilizada para documentação de código ou wikis. Essa forma foi escolhida para poder ser integrada com mais facilidade à documentação existente da Conta gov.br.

Incluiremos aqui o texto final após a renderização do conteúdo, tal qual ele será visualizado em páginas da Internet.

# Guia Prático para Adoção da Conta gov.br

**Autor:** Demétrius de Almeida Jubé

## 1. Apresentação

Este guia tem como objetivo apoiar gestores públicos na avaliação da viabilidade e pertinência de integrar sistemas e serviços à plataforma de Login Único do Governo Federal, conhecida como **Conta gov.br**.

## 2. Entendendo a Conta gov.br

### O que é

A Conta gov.br é um mecanismo de autenticação digital único, instituído pelo [Decreto 8.936/2016](#)[1], que tem como objetivo simplificar e padronizar o acesso do cidadão a serviços públicos digitais. Mantida pela [Secretaria de Governo Digital](#), a solução adota o conceito de Login Único (*Single Sign-On*), oferecendo aos sistemas que a integrem funcionalidades de autenticação (verificação da identidade do usuário) e autorização (controle de permissões de acesso).

### Problemas que resolve

A Conta gov.br endereça desafios estruturais comuns nos serviços públicos digitais [2], como:

#### Múltiplas formas de login e autenticação

A ausência de uma forma padronizada de autenticação obriga cada órgão a manter sua própria solução de autenticação e autorização, incluindo o armazenamento dos dados pessoais e das credenciais dos usuários. Essa fragmentação, além de gerar riscos institucionais relacionados à gestão dessas informações sensíveis, também expõe o cidadão à Fadiga da Autenticação [3] — um fenômeno em que a multiplicidade de logins e senhas para diferentes serviços leva à adoção de comportamentos inseguros, como o uso de senhas fracas ou repetidas. Esses hábitos comprometem diretamente a segurança do ambiente digital.

#### Inconsistência cadastral entre serviços

O uso de serviços públicos digitais pode demandar uma acurácia maior nos dados cadastrais de quem os utiliza, uma vez que podem envolver acesso a dados sensíveis, como informações fiscais e trabalhistas. Dessa forma, ao utilizar uma solução que garante a consistência das informações, o órgão assegura maior confiabilidade ao processo, reduzindo o risco de fraudes e melhorando a qualidade do atendimento.

## Falta de integração entre sistemas públicos

Ao compartilharem o mesmo sistema de autenticação, diferentes serviços públicos digitais podem oferecer uma experiência mais fluida ao cidadão, que poderá transitar entre um e outro sem ter uma nova etapa de autenticação, o que melhora a usabilidade e fortalece a percepção de integração entre os serviços do Estado.

Juntas, essas melhorias contribuem para um ecossistema digital mais seguro, eficiente e centrado no cidadão.

## Conceitos-chave

Para garantir uma autenticação segura e adaptada à diversidade dos serviços públicos digitais, a Conta gov.br é estruturada a partir de conceitos que permitem modular o acesso e a confiabilidade das informações. Os principais elementos que compõem essa arquitetura serão mostrados a seguir:

- **Selos de Confiabilidade:** Indicam a origem e segurança do processo de verificação dos dados, indicando se o procedimento foi feito por uma instituição bancária ou pela Justiça Eleitoral, por exemplo.
- **Níveis de Autenticação:** Definidos em Bronze, Prata e Ouro, essa informação varia de acordo com o Selo de Confiabilidade de quem verificou as informações. Quanto mais seguro for o Selo, maior o Nível fornecido ao usuário.
- **Catálogo de Confiabilidades:** Estrutura que permite personalizar a experiência do usuário com base nos Selos e Níveis disponíveis.

A Figura 1 apresenta a representação gráfica dessa arquitetura:

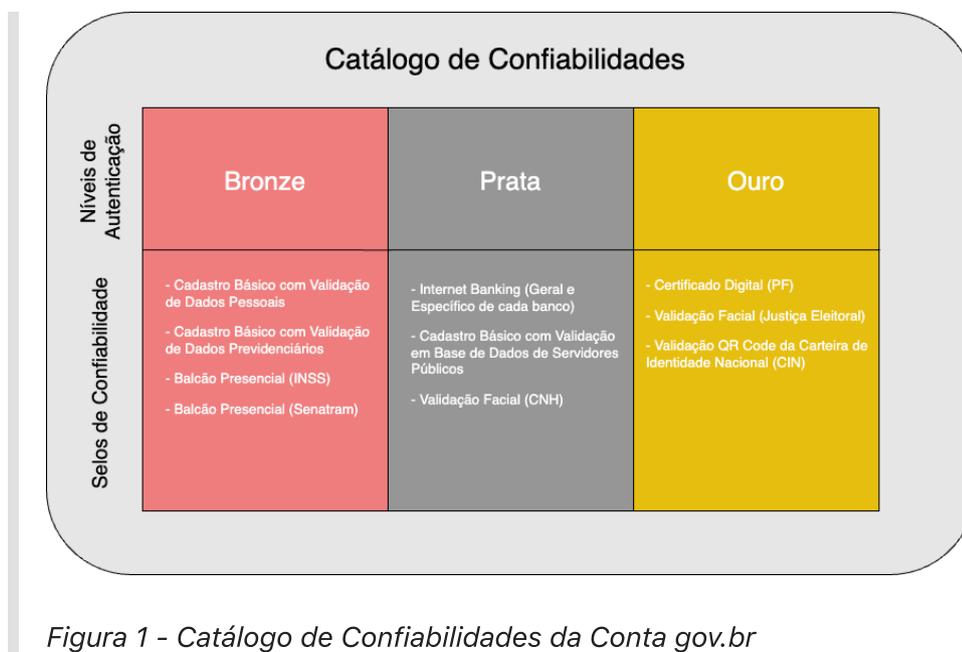


Figura 1 - Catálogo de Confiabilidades da Conta gov.br

De forma geral, o Nível de Autenticação atribuído a uma Conta gov.br é determinado pelo grau de verificação realizado no momento do cadastro e em etapas subsequentes. Quanto maior o Nível, maior a confiança na identidade do usuário, permitindo o acesso a serviços públicos mais sensíveis. Essas informações ficam disponíveis por meio de *endpoints* que podem ser utilizados pelas aplicações

integradas para adaptar a experiência do usuário, restringindo ou liberando funcionalidades conforme o Nível de Autenticação identificado.

### 3. Critérios de Uso

Nem toda solução está apta a ser integrada com a Conta gov.br. Há critérios que devem ser satisfeitos e são avaliados no momento do pedido de adesão.

#### Requisitos de Elegibilidade para Integração

Para que um sistema possa ser integrado à Conta gov.br, é necessário que:

-  **Seja caracterizado como um serviço público**, ou seja, uma ação realizada por órgãos ou entidades da administração pública para atender demandas da sociedade no exercício de direitos ou no cumprimento de deveres (Decreto nº 8.936/2016, art. 2º, inciso I).
-  **Se enquadre como um serviço público digital**, ou seja, prestado por meio eletrônico, sem a necessidade de atendimento presencial (Decreto nº 8.936/2016, art. 2º, inciso II).
-  **Esteja sob responsabilidade de um ente público habilitado**, como:
  - Órgãos da administração pública direta, autárquica ou fundacional.
  - Empresas públicas da União, Estados ou Municípios.
-  **Tenha a solicitação formalizada por um agente público ou gestor responsável pelo serviço.**
-  **No caso de prefeituras**, é necessário que o município tenha formalizado sua adesão à **Rede Nacional de Governo Digital (Rede gov.br)**. Servidores municipais devem entrar em contato com sua prefeitura para verificar a adesão antes de solicitar a integração.

 **Importante:** Cada solicitação é analisada individualmente pela Secretaria de Governo Digital, com base no interesse público e na aderência aos critérios legais e técnicos.

---

#### Exemplos de Integrações Não Permitidas

Integrações com a Conta gov.br **não serão autorizadas** para:

-  **Sistemas de uso estritamente administrativo**, sem acesso direto ao cidadão.
-  **Serviços que não ofereçam benefício público direto**, como processos internos.
-  **Soluções inseridas em mercados concorrenciais**, como:

- Plataformas bancárias
- Sistemas comerciais
- Serviços com exploração econômica direta

## 4. Etapas do Processo de Integração com a Conta gov.br

A integração de sistemas públicos ao mecanismo de autenticação da Conta gov.br segue um fluxo bem definido, com etapas que envolvem análise de elegibilidade, envio de dados técnicos e validações de segurança e usabilidade.

A Figura 2, baseada no processo apresentado na página de solicitação do [Serviço de Integração aos Produtos do Ecossistema da Identidade Digital GOV.BR](#) [4], apresenta uma visão geral do procedimento de integração, que é descrito passo a passo nos tópicos seguintes.

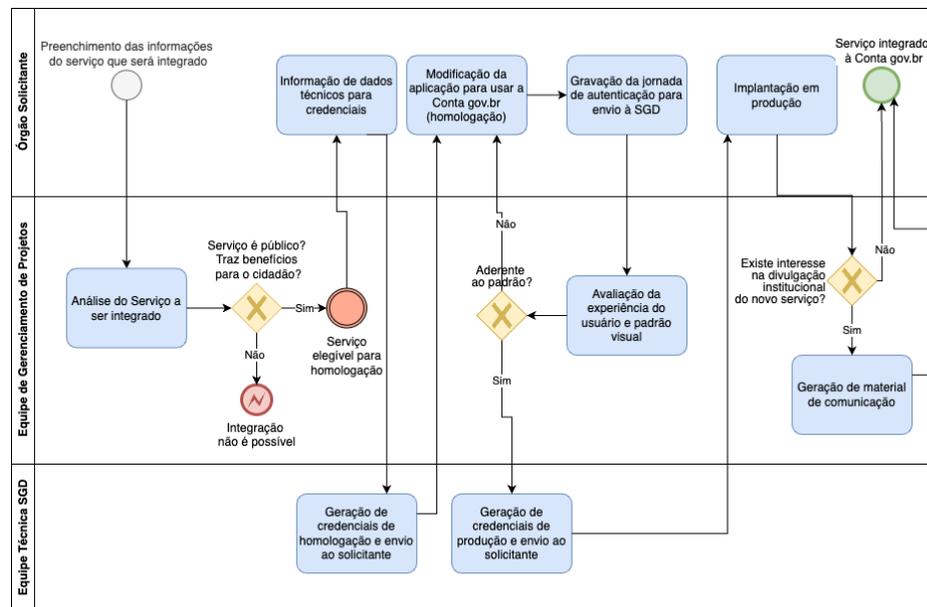


Figura 2 - Fluxo de aprovação da integração com a Conta gov.br

### ✓ 1. Análise de elegibilidade

- Verificação inicial pela Secretaria de Governo Digital (SGD) para confirmar se o serviço candidato atende aos critérios de elegibilidade que foram mencionados na [Seção 3](#).

### 📄 2. Envio de informações institucionais e técnicas

Caso a solicitação seja aprovada, o órgão deverá fornecer:

- Dados do **Responsável Técnico** e do **Representante Legal**.
- Certificado digital com **chave pública**, utilizado para proteger a credencial enviada.
- **Previsão de acessos diários**.

- URLs de **retorno** e **logout** da aplicação.
- 

### 3. Geração das credenciais de homologação

- A equipe técnica da SGD gera as credenciais:
    - `CLIENT_ID`
    - `CLIENT_SECRET`
  - Essas credenciais são utilizadas exclusivamente no **ambiente de homologação**.
- 

### 4. Implementação da integração

- O órgão realiza as modificações necessárias na aplicação, conforme o [Roteiro Técnico de Integração](#).
  - A jornada completa de autenticação é gravada e enviada para a equipe da SGD para análise.
- 

### 5. Avaliação de aderência

- A Equipe de Gerenciamento de Projetos da SGD realiza:
    - Análise de **aderência ao *Design System gov.br***.
    - Verificação da **Experiência do Usuário (UX)** no fluxo de login.
- 

### 6. Credenciais de produção e implantação

- Com a aprovação final, são emitidas as **credenciais de produção**.
  - O órgão pode então implantar a solução integrada.
- 

### 7. Divulgação institucional (opcional)

- Caso haja interesse do órgão e da SGD, pode ser produzida uma **peça de comunicação institucional** para divulgação da nova funcionalidade nos canais oficiais.

## 5. Aspectos Técnicos-Chave (visão executiva)

- Baseado em **OpenID Connect (OIDC)**, um protocolo de autenticação construído sobre o OAuth 2.0, que adiciona uma camada de **identidade digital**. Enquanto o OAuth 2.0 trata da **autorização de acesso a recursos**, materializada por um *token* de acesso (**ACCESS\_TOKEN**), o OpenID Connect permite que aplicações verifiquem a identidade do usuário por meio de um **ID Token (ID\_TOKEN)**. Esse *token* contém informações confiáveis sobre o usuário final e é emitido por um **Provedor de Identidade** (como gov.br, Google ou Microsoft).
- Uso de *Proof Key for Code Exchange (PKCE)*, um mecanismo que garante que a aplicação que solicitou um código de autorização é a mesma que obtém o ACCESS\_TOKEN, o que fornece proteção contra interceptação de código.

- Validação de **ID\_TOKEN** e **ACCESS\_TOKEN** via chave pública.
- Integração com APIs da Rede gov.br que fornecem funcionalidades de consulta dos dados do usuário, sendo possível obter informações cadastrais como o CPF ou CNPJ do usuário, qual o meio de autenticação que foi utilizado, os níveis de autenticação e até a foto cadastrada.
- Ambiente de **homologação** disponível para testar a integração e identificar problemas com a aplicação original.

## 6. Análise de Impactos da Integração

É importante destacar que a incorporação da Conta gov.br a uma solução digital — seja ela nova ou já existente — envolve impactos que devem ser cuidadosamente analisados pelos gestores, a fim de assegurar que sua adoção proporcione benefícios concretos ao público-alvo do serviço.

A seguir, apresentamos dados extraídos de um estudo conduzido durante a transição de um sistema legislativo para o uso da Conta gov.br [5], adotada de forma complementar ao modelo tradicional baseado em e-mail e senha. A pesquisa acompanhou o comportamento de 30 usuários distribuídos em diferentes regiões do país, permitindo observar a experiência com ambos os métodos de autenticação. Esses dados oferecem subsídios relevantes para decisões mais fundamentadas quanto à viabilidade e aos ganhos da integração.



### Aumento no tempo de autenticação

A autenticação via Conta gov.br apresentou um tempo mediano de 55,07 segundos para o ciclo completo, enquanto o método tradicional com e-mail e senha registrou 27,46 segundos. Isso representa um aumento de 100,53% no tempo de execução em relação ao modelo original testado, conforme podemos ver na Figura 3.

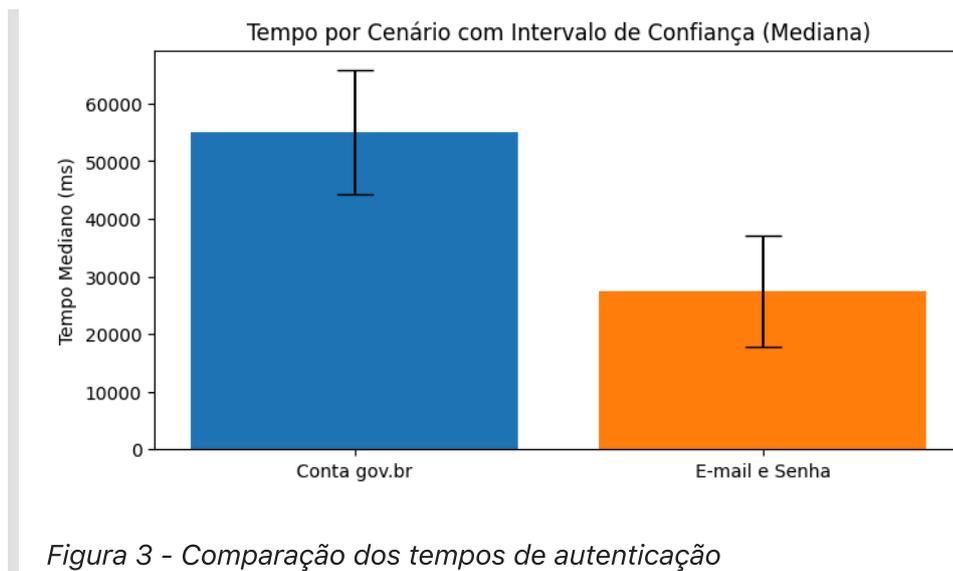


Figura 3 - Comparação dos tempos de autenticação

Em sistemas pré-existentes que já utilizam um modelo próprio de autenticação, recomenda-se a realização de uma medição semelhante para estimar o impacto da latência introduzida pela nova solução.

Por outro lado, é importante observar que, ao utilizar uma arquitetura de Login Único, esse tempo adicional pode ser mitigado quando o usuário já estiver autenticado e houver uma sessão válida ativa. Nesses casos, o acesso ao serviço ocorre de forma fluida, sem a necessidade de uma nova autenticação.

## Dependência de infraestrutura externa

Durante o estudo citado, foram observadas instabilidades com alguns participantes, como lentidão e períodos de indisponibilidade. Esses eventos evidenciam que a adoção de um mecanismo como a Conta gov.br implica a criação de uma dependência em relação a uma infraestrutura externa, fora do controle direto da organização integradora.

Embora tais ocorrências tenham se dado no ambiente de homologação — e que o ambiente de produção conte com maior robustez e alta disponibilidade — esse fator deve ser considerado na análise de riscos associados à integração.

## Usabilidade e facilidade percebida

A pesquisa comparou a usabilidade dos mecanismos de autenticação, usando o *System Usability Scale (SUS)*, índice proposto por John Brooke [6] e utilizado para mensurar a usabilidade geral de sistemas de informação. É um indicador que varia de 0 a 100 e busca ter uma noção sobre como o usuário percebe fatores como simplicidade, consistência e dificuldade no uso de um serviço digital, e onde valores altos indicam uma melhor usabilidade.

Ao testar os dois modos de autenticação, os participantes da pesquisa não detectaram uma diferença significativa entre eles, sendo que a usabilidade com o E-mail e Senha teve uma pequena vantagem sobre a feita com a Conta gov.br (88,25 contra 86,83). A análise pode ser conferida na Figura 4:

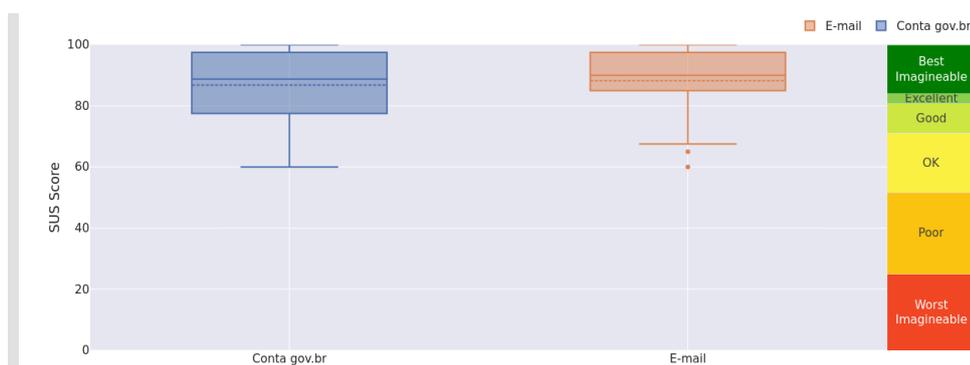


Figura 4 - Comparação do SUS entre os dois mecanismos

O mesmo fenômeno ocorreu com a facilidade percebida. Usando uma escala chamada *Single Ease Question (SEQ)* [7] que varia 1 a 7, onde 1 corresponde a uma tarefa Muito Difícil e 7 a uma tarefa Muito Fácil, a autenticação por E-mail e Senha obteve uma média de 6,77, enquanto a Conta gov.br teve como resultado 6,67. A significância estatística dos dois casos foi calculada e revelou que não houve diferença real entre eles. Porém, cabe destacar que todos os participantes já tinham

usado a Conta gov.br em algum momento. Dessa forma, já estavam habituados com a solução, e isso pode ter um impacto nessa sensação que eles demonstraram. Dada a ampla difusão de uso da Conta gov.br, a chance de ter uma pessoa que nunca a utilizou pode ser baixa, mas vale a pena verificar se o público-alvo da solução a ser integrada pertence a novos usuários da Conta gov.br. Se for o caso, ações de educação podem ser utilizadas para tornar esse uso mais simples.

Por fim, o uso adequado do *Design System Gov.br* na interface do serviço público digital contribui para que usuários familiarizados com a Conta gov.br em outras soluções reconheçam o mecanismo de autenticação com mais facilidade ao utilizá-lo no sistema integrado. Essa consistência visual reforça a confiança do cidadão e melhora a experiência de uso.

## Curva de aprendizado na integração com a Conta gov.br

Embora a Conta gov.br utilize o padrão amplamente adotado OpenID Connect (OIDC), é natural que as equipes técnicas enfrentem desafios durante o processo de integração — especialmente quando se trata de adaptar sistemas que já estão em operação, como foi o caso do estudo citado. A incorporação desse mecanismo de autenticação envolve ajustes na arquitetura da aplicação, no tratamento de tokens e na gestão de sessões, o que pode demandar tempo de aprendizado e adaptação, mesmo para profissionais experientes. Por isso, é recomendável que as equipes reservem uma etapa específica do projeto para estudo, testes e homologação, garantindo que a transição ocorra com segurança e sem impacto negativo à experiência do usuário.

## Resumo de riscos e ações sugeridas

Risco	Mitigação
Aumento do tempo de autenticação	- Pesquisa do perfil dos utilizadores do serviço público digital para avaliar o impacto - Ações de divulgação dos benefícios da integração com a Conta gov.br - Prever funcionalidades adicionais para quem autenticou com a Conta gov.br, a fim de estimular seu uso
Dependência externa (infraestrutura gov.br)	- Monitoramento ativo da disponibilidade do ambiente - Indicação para o usuário sobre a disponibilidade
Quebra de experiência do usuário	na do - Aderência ao <i>Design System</i> do Governo Federal
Curva de aprendizado técnica	- Suporte técnico da SGD - Utilização de bibliotecas ou frameworks com suporte à arquitetura da Conta gov.br (OpenID Connect)

## 7. Resumo de Benefícios para o Cidadão

- Redução da Fadiga de Autenticação, possibilitando o uso de uma única senha forte para vários serviços.
- Maior controle sobre dados pessoais, que não precisam ser cadastrados novamente para criar uma credencial em um novo site.
- Login seguro e padronizado.
- Habilitação de autenticação em duas etapas a partir do nível Prata.

## 8. Recomendações Finais

- Envolver equipes técnica, jurídica e de comunicação desde o início do processo de integração com a Conta gov.br.
- Documentar todo o processo de incorporação da Conta gov.br ao serviço digital.
- Realizar testes reais com cidadãos.
- Elaborar um plano de comunicação institucional para lançamento do serviço digital com o novo meio de autenticação.

## 9. Referências

[1]: Brasil. Decreto nº 8.936, de 19 de dezembro de 2016. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2016/Decreto/D8936.htm](https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8936.htm).

[2] Governo Federal. *Gerenciar o uso dos seus dados pessoais*. Secretaria de Governo Digital.

Disponível em: <https://www.gov.br/governodigital/pt-br/identidade/gerenciar-o-uso-dos-seus-dados-pessoais>.

[3] Sasse, M. Angela; Steves, Michelle; Krol, Kat; Chisnell, Dana. *The Great Authentication Fatigue – And How to Overcome It*. In: Rau, P. L. Patrick (ed.). **Cross-Cultural Design**. Lecture Notes in Computer Science, vol. 8528, Springer International Publishing, Cham, 2014, pp. 228–239.

ISBN: 978-3-319-07307-1, 978-3-319-07308-8.

Disponível em: [https://link.springer.com/10.1007/978-3-319-07308-8\\_23](https://link.springer.com/10.1007/978-3-319-07308-8_23).

[4] Governo Federal. *Serviço de Integração aos Produtos de Identidade Digital gov.br*. Secretaria de Governo Digital.

Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/transformacao-digital/servico-de-integracao-aos-produtos-de-identidade-digital-gov.br/servico-de-integracao-aos-produtos-de-identidade-digital-gov.br>.

[5] Jubé, Demétrius de Almeida. *Análise da usabilidade da Conta gov.br para adoção pelo Senado Federal*. 2025. Dissertação (Mestrado Profissional em Computação Aplicada) – Universidade de Brasília, Departamento de Ciência da Computação, Brasília, 2025.

[6] Brooke, John. *SUS: A quick and dirty usability scale*. In: Jordan, P. W. et al. (eds.). **Usability Evaluation in Industry**, p. 189–194. London: Taylor & Francis, 1995.

[7] Sauro, Jeff; Lewis, James R. *Quantifying the User Experience: Practical Statistics for User Research*. 2ª ed. Amsterdam; Boston; Heidelberg: Elsevier, Morgan Kaufmann, 2016. ISBN 978-0-12-802308-2.

## 10. Exemplos Técnicos

Esta seção apresenta dois exemplos desenvolvidos com o objetivo de apoiar equipes técnicas na compreensão do fluxo de autenticação da Conta gov.br e sua integração a sistemas existentes. São demonstradas duas abordagens: uma utilizando o framework Spring Boot (Java), e outra com a linguagem Python. Ambas utilizam bibliotecas compatíveis com o padrão OAuth 2.0 / OpenID Connect, e os exemplos podem servir como ponto de partida para a implementação por desenvolvedores.

### Estrutura do Projeto Spring Boot para integração com a Conta gov.br

#### 1. application.yml

```
spring:
  security:
    oauth2:
      client:
        registration:
          govbr:
            client-id: CLIENT_ID_DO_GOV_BR
            client-secret: CLIENT_SECRET
            # Escopos solicitados para o gov.br
            scope: openid, email, profile, govbr_confiabilidades,
govbr_empresa
            authorization-grant-type: authorization_code
            # Url de retorno, deve ser a mesma cadastrada na
solicitação de integração com o gov.br. Caso tenha sido
cadastrada outra, será necessário fazer o redirecionamento e
passagem dos parâmetros
            redirect-uri: "{baseUrl}/login/oauth2/code/govbr"
            client-name: Login Único gov.br
        provider:
          govbr:
            #Utilizar https://sso.staging.acesso.gov.br para o
ambiente de homologação
            authorization-uri:
https://sso.acesso.gov.br/authorize
            token-uri: https://sso.acesso.gov.br/token
            jwk-set-uri: https://sso.acesso.gov.br/jwk
            user-info-uri: https://sso.acesso.gov.br/userinfo
            user-name-attribute: sub
```

#### 2. CustomOAuth2SuccessHandler.java

Classe que permite realizar alguma tarefa com o usuário que foi autenticado. Nesse exemplo, coloca na sessão e redireciona para a página /usuario

```

@Component
public class CustomOAuth2SuccessHandler implements
AuthenticationSuccessHandler {

    @Override
    public void onAuthenticationSuccess(
        HttpServletRequest request,
        HttpServletResponse response,
        Authentication authentication) throws IOException,
        ServletException {

        OAuth2User oauthUser = (OAuth2User)
authentication.getPrincipal();

        request.getSession().setAttribute("usuario",
oauthUser.getAttributes());

        // Redireciona para a página de perfil
        response.sendRedirect(request.getContextPath() +
"/usuario");    }
}

```

### 3. SecurityConfig.java

```

@Configuration
@EnableWebSecurity
public class SecurityConfig {

    @Autowired
    private CustomOAuth2SuccessHandler
customOAuth2SuccessHandler;

    @Bean
    public SecurityFilterChain filterChain(HttpSecurity http)
throws Exception {
        /*
        Permite que alguns recursos sejam utilizados sem
autenticação. Se a URI de retorno for diferente do que é o padrão
do Spring Security, esse caminho deve estar desprotegido também.
        */
        http.authorizeHttpRequests(auth ->
auth.requestMatchers("/", "/public/**", "/css/**", "/js/**",
"/registro-conta-
govbr").permitAll().anyRequest().authenticated())
                .oauth2Login(oauth2 ->
oauth2.loginPage("/oauth2/authorization/govbr").successHandler(custo
// Adiciona o successHandler para que uma tarefa
adicional seja feita quando o usuário for autenticado
                return http.build());
        }}
}

```

### 4. HomeController.java

```

@Controller
public class HomeController {

```

```

@GetMapping("/")
public String index() {
    return "index";
}

@GetMapping("/user")
@ResponseBody
public Map<String, Object> user(@AuthenticationPrincipal
OAuth2User principal) {
    return principal.getAttributes();
}

    /*Exemplo de redirecionamento caso a redirect-uri seja
diferente do padrão do Spring Security
(/login/oauth2/code/govbr). Nesse caso todos os parâmetros
retornados devem ser passados para o endpoint padrão do Spring
Security.
*/
@GetMapping("/registro-conta-govbr")
public void redirecionaParaSpring(@RequestParam Map<String,
String> params, HttpServletRequest request, HttpServletResponse
response) throws IOException {
    String query = params.entrySet().stream().map(e -> {
        try {
            return e.getKey() + "=" +
URLEncoder.encode(e.getValue(), "UTF-8");
        } catch (UnsupportedEncodingException ex) {
            throw new RuntimeException(ex);
        }
    }).collect(Collectors.joining("&"));
    String contextPath = request.getContextPath(); //
Exemplo: "/meuapp"
    String redirectUri = contextPath +
"/login/oauth2/code/govbr?" + query;
    response.sendRedirect(redirectUri);
}
}

```

## 5. UsuarioController.java

```

@Controller
public class UsuarioController {

    @GetMapping("/usuario")
    public String mostrarUsuario(HttpSession session, Model
model) {
        @SuppressWarnings("unchecked") Map<String, Object>
usuario = (Map<String, Object>) session.getAttribute("usuario");

        model.addAttribute("usuario", usuario);
        return "usuario"; // Thymeleaf procurará por
templates/usuario.html
    }
}

```

## 6. index.html (coloque em src/main/resources/templates)

Esse index assume que o core.css e o core.js do Design System estão em pastas static/css e static/js, respectivamente.

```
<!DOCTYPE html>
<html lang="pt-br" xmlns:th="http://www.thymeleaf.org">
<head>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width, initial-
scale=1.0" />

  <!-- Fontes (remotas ou locais, como preferir) -->
  <link rel="stylesheet"
href="https://fonts.googleapis.com/css?
family=Raleway:300,400,700&display=swap" />
  <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/5.11.2/css/all.min.css" />

  <!-- CSS do Design System copiado via npm -->
  <link rel="stylesheet" th:href="@{/css/core.css}" />
  <link rel="stylesheet"
th:href="@{/fonts/rawline/css/rawline.css}" />

  <title>Exemplo gov.br + Thymeleaf</title>
</head>
<body>

<!-- Conteúdo -->
<main class="br-main">
  <div class="container-lg">
    <div class="br-card mt-5 p-5">
      <h1 class="br-heading">Bem-vindo!</h1>
      <p>
        <a class="br-button primary"
th:href="@{/oauth2/authorization/govbr}">
          Entrar com gov.br
        </a>
      </p>
    </div>
  </div>
</main>

<!-- JS do Design System copiado via npm -->
<script type="module" th:src="@{/js/core.js}"></script>
</body>
</html>
```

## 7. usuario.html (coloque em src/main/resources/templates)

```
<!DOCTYPE html>
<html xmlns:th="http://www.thymeleaf.org">
<head>
  <meta charset="UTF-8">
  <title>Perfil do Usuário</title>
</head>
<body>
```

```

<h1>Bem-vindo, <span th:text="${usuario.name}">Usuário</span>!
</h1>



<p><strong>CPF:</strong> <span
th:text="${usuario.sub}">CPF</span></p>
<p><strong>Email:</strong> <span
th:text="${usuario.email}">Email</span></p>
<p><strong>Username:</strong> <span
th:text="${usuario.preferred_username}">Usuário</span></p>
</body>
</html>

```

## 8. Dependências no pom.xml

```

<project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/xsd/maven-4.0.0.xsd">
<modelVersion>4.0.0</modelVersion>
<groupId>com.exemplo</groupId>
<artifactId>govbr-login</artifactId>
<version>1.0.0</version>
<packaging>jar</packaging>
<name>govbr-login</name>
<properties>
<java.version>17</java.version>
<spring-boot.version>3.4.0</spring-boot.version>
</properties>
<dependencies>
<dependency>
<groupId>org.springframework.boot</groupId>
<artifactId>spring-boot-starter-web</artifactId>
<version>${spring-boot.version}</version>
</dependency>
<dependency>
<groupId>org.springframework.boot</groupId>
<artifactId>spring-boot-starter-security</artifactId>
<version>${spring-boot.version}</version>
</dependency>
<dependency>
<groupId>org.springframework.boot</groupId>
<artifactId>spring-boot-starter-oauth2-
client</artifactId>
<version>${spring-boot.version}</version>
</dependency>
<dependency>
<groupId>org.springframework.boot</groupId>
<artifactId>spring-boot-starter-
thymeleaf</artifactId>
<version>${spring-boot.version}</version>
</dependency>
</dependencies>
<build>

```

```
        <plugins>
          <plugin>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-maven-plugin</artifactId>
          </plugin>
        </plugins>
      </build>
    </project>
```

---

## Integração com Flask (Python)

Para um exemplo com Python, utilizaremos o [Flask](#), um framework leve para desenvolvimento web. Ele permite criar aplicações e APIs de forma rápida, com baixo custo de complexidade e fácil manutenção. Por ser modular, facilita integrações com serviços externos, como é o caso da autenticação via gov.br.

### 1. Instalação das dependências

```
pip install Flask requests authlib
```

### 2. Código principal

```
# Permite a execução do Flask dentro de ambientes como Jupyter Notebook
import nest_asyncio
nest_asyncio.apply()

# Importações principais do Flask e Authlib para integração OAuth 2.0 / OpenID Connect
from flask import Flask, redirect, url_for, session, request
from authlib.integrations.flask_client import OAuth
import os
import secrets

# Inicialização da aplicação Flask
app = Flask(__name__)

# Chave secreta usada para proteger sessões (trocar por uma segura em produção)
app.secret_key = "segredo"

# Prefixo de rota da aplicação (por exemplo: /contexto)
ROUTE_PREFIX = "/contexto"

# Configuração do cliente OAuth para autenticação via Conta gov.br
oauth = OAuth(app)
govbr = oauth.register(
    name='govbr',
    client_id='CLIENT_ID', # Substituir pelo client_id gerado no gov.br
    client_secret='CLIENT_SECRET', # Substituir pelo client_secret correspondente
    access_token_url='https://sso.staging.acesso.gov.br/token',
```

```

    authorize_url='https://sso.staging.acesso.gov.br/authorize',
    api_base_url='https://sso.staging.acesso.gov.br',
    client_kwargs={'scope': 'openid profile email'}, # Escopos
solicitados
    server_metadata_url='https://sso.staging.acesso.gov.br/.well-
known/openid-configuration' # Descoberta automática de endpoints
)

# Página inicial da aplicação
@app.route(f"{ROUTE_PREFIX}/")
def index():
    # Verifica se o usuário está logado (sessão ativa)
    user = session.get('user')
    if user:
        # Exibe todos os dados retornados do id_token
        html = "<h1>Dados do usuário</h1><ul>"
        for key, value in user.items():
            html += f"<li><strong>{key}</strong> {value}</li>"
        html += "</ul>"
        return html
    # Caso não esteja logado, mostra link para iniciar login
    return f'<a href="{ROUTE_PREFIX}/login">Entrar com
gov.br</a>'

# Endpoint que inicia o fluxo de autenticação
@app.route(f"{ROUTE_PREFIX}/login")
def login():
    # Gera um nonce (valor aleatório) para proteger contra replay
attacks
    nonce = secrets.token_urlsafe(16)
    session['nonce'] = nonce
    # Define a URL de redirecionamento após autenticação (deve
ser registrada no gov.br)
    redirect_uri = url_for("registro_conta_govbr",
_external=True)
    # Redireciona o usuário para o gov.br com os parâmetros de
autenticação
    return govbr.authorize_redirect(redirect_uri, nonce=nonce)

# Endpoint de callback após autenticação no gov.br
@app.route(f"{ROUTE_PREFIX}/registro-conta-govbr")
def registro_conta_govbr():
    # Recupera o token retornado pelo gov.br
    token = govbr.authorize_access_token()
    # Recupera e remove o nonce salvo na sessão
    nonce = session.pop('nonce', None)
    # Valida o ID Token (incluindo o nonce) e extrai as
informações do usuário
    user_info = govbr.parse_id_token(token, nonce=nonce)
    # Salva os dados do usuário na sessão
    session["user"] = user_info
    # Redireciona para a página inicial autenticada
    return redirect(f"{ROUTE_PREFIX}/")

# Rota para logout (encerra a sessão)
@app.route(f"{ROUTE_PREFIX}/logout")

```

```
def logout():
    session.pop("user", None)
    return redirect(f"{ROUTE_PREFIX}/")

# Caminhos dos arquivos de certificado SSL para HTTPS (ajustar os
# nomes dos arquivos)
base_dir = os.path.dirname(os.path.abspath(__file__))
cert_path = os.path.join(base_dir, 'CERTIFICADO.pem')
key_path = os.path.join(base_dir, 'CHAVE_PRIVADA.pem')

# Inicialização do servidor Flask com HTTPS na porta 443
if __name__ == '__main__':
    app.run(ssl_context=(cert_path, key_path), debug=True,
            port=443)
```

---