Universidade Federal de Santa Catarina
Centro de Ciências da Saúde
Programa de Pós Graduação: Mestrado Profissional em Informática em Saúde

Carla Knust Bastos

Nível de Garantia de Autenticação de Pessoas Idosas

Florianópolis/SC

2023

Nível de Garantia de Autenticação de Pessoas Idosas

Carla Knust Bastos

Dissertação de Mestrado submetida ao Programa de Pós Graduação: Mestrado Profissional em Informática em Saúde (PPGINFOS), da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Informática em Saúde.
Orientador: Prof Dr. Ricardo Felipe Custódio
Co-orientador: Prof Ms. Frederico Schardong

Florianópolis/SC

2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Bastos, Carla Knust
Nível de Garantia de Autenticação de Pessoas Idosas / Carla Knust Bastos ; orientador, Ricardo Felipe Custódio, coorientador, Frederico Schardong, 2023.
117 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências da Saúde, Programa de Pós-Graduação em Informática em Saúde, Florianópolis, 2023.

Inclui referências.

1. Informática em Saúde. 2. Nível de Garantia de Autenticação para Idosos. 3. Identidade Eletrônica para Idosos. 4. Autenticação de Idosos. 5. Memorização de Senhas. I. Custódio, Ricardo Felipe . II. Schardong, Frederico . III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Informática em Saúde. IV. Título.

Carla Knust Bastos

Nível de Garantia de Autenticação de Pessoas Idosas

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Prof Dr. Ricardo Felipe Custódio, Dr.
Universidade Federal de Santa Catarina

Prof. Jefferson Luiz Brum Marques, Dr.
Universidade Federal de Santa Catarina

Prof. Alexandre Augusto Giron, Dr.
Universidade Tecnológica Federal do Paraná

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Informática em Saúde.

Documento assinado digitalmente
Grace Teresinha Marcon Dal Sasso
Data: 05/02/2024 13:04:48-0300
CPF: ***.068.549-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
Ricardo Felipe Custodio
Data: 02/02/2024 08:14:35-0300
CPF: ***.981.609-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Prof Dr. Ricardo Felipe Custódio, Dr.
Orientador

Dedico este trabalho a minha tia Nina.

Agradecimentos

No momento em que concluo esta importante etapa da minha jornada acadêmica e pessoal, desejo expressar minha mais profunda gratidão àqueles que estiveram ao meu lado, oferecendo apoio, compreensão e inspiração.

A Evandro, meu esposo, meu porto seguro, que compreendeu cada ausência, cada noite mal dormida e cada ansiedade. Sua paciência, amor e constante incentivo foram fundamentais para que eu conseguisse ultrapassar os obstáculos e seguir em frente.

À minha mãe, Ilda, que desde o início me ensinou o valor da educação, do trabalho árduo e da perseverança. A cada dia, seu exemplo de força e determinação ressoa em mim e me inspira a ser melhor. Seu amor incondicional e sua fé em mim sempre me deram a segurança de que eu estava no caminho certo.

Aos meus preciosos Joaquim e Miguel, que mesmo sendo tão jovens, mostraram uma compreensão imensa quando a mamãe precisava se dedicar aos estudos. Vocês são minha luz e minha principal motivação.

Um agradecimento especial ao Prof. Ricardo Felipe Custódio, que mais do que um orientador, revelou-se um verdadeiro ampliador de ideias. Sua abordagem inovadora e seu pensamento crítico foram essenciais para abrir minha mente e expandir os horizontes do meu entendimento. Além disso, estendo meus agradecimentos ao coorientador Prof. Frederico Schardong, cuja orientação e insights valiosos contribuíram significativamente para o enriquecimento deste trabalho.

Por fim, mas não menos importante, expresso minha profunda gratidão ao Programa de Mestrado em Informática em Saúde. Este programa abriu minha mente para as infinitas possibilidades que o tema oferece. Sou grata pela oportunidade de crescer, aprender e contribuir com esta área tão relevante e promissora.

A todos vocês, meu eterno agradecimento.

Só sei que nada sei.

Sócrates

Resumo

Nesta dissertação apresentamos uma pesquisa sobre a autenticação eletrônica de idosos. O objetivo principal do estudo é avaliar a capacidade de idosos em memorizar senhas, fazendo uma comparação direta entre senhas baseadas em imagens e aquelas baseadas em caracteres. O trabalho começa com uma introdução que destaca a importância da autenticação de pessoas idosas na era digital e justifica a necessidade de um nível de garantia de autenticação específico para essa população. Em seguida, apresentamos a metodologia utilizada, que consiste em uma revisão narrativa da literatura pertinente a memorização de senhas na população idosa. Posteriormente foi realizado um experimento com um grupo de 22 idosos, em que foram submetidos a um questionário para entender suas práticas habituais e experiências passadas com a utilização de senhas. Deste grupo inicial, 10 participantes, todas mulheres com idades entre 61 e 83 anos, demonstraram interesse e compromisso em participar de um teste mais aprofundado sobre memorização de senhas. Os resultados da pesquisa indicam que as senhas baseadas em imagens são mais fáceis de serem memorizadas pelos idosos do que as senhas baseadas em caracteres. Além disso, o estudo aponta que a idade avançada não é um fator determinante para a capacidade de memorização de senhas, mas sim a experiência prévia com o uso de senhas. Concluímos que é necessário desenvolver soluções de autenticação que levem em consideração as particularidades da população idosa, como a dificuldade de memorização de senhas complexas. O estudo contribui para a área de segurança digital e pode ser utilizado como base para o desenvolvimento de políticas públicas e soluções tecnológicas que garantam a segurança e a privacidade dos idosos na era digital.

Palavras-chave: Autenticação; Idoso; Memória em idosos; Senhas visuais; Senhas verbais.

Abstract

In this dissertation we present research on electronic authentication of older adults. The main objective of the study is to evaluate the ability of older adults to memorize passwords, making a direct comparison between passwords based on images and those based on characters. The work begins with an introduction that highlights the importance of authenticating older adults in the digital era and justifies the need for a specific level of authentication guarantee for this population. Next, we present the methodology used, which consists of a narrative review of the literature pertinent to remembering passwords in the elderly population. Subsequently, an experiment was carried out with a group of 22 older adults, in which they were subjected to a questionnaire to understand their usual practices and past experiences with the use of passwords. From this initial group, 10 participants, all women aged between 61 and 83, demonstrated interest and commitment to participating in a more in-depth test on remembering passwords. The research results indicate that image-based passwords are easier for older people to memorize than character-based passwords. Furthermore, the study points out that advanced age is not a determining factor for the ability to remember passwords, but rather previous experience with using passwords. We conclude that it is necessary to develop authentication solutions that take into account the particularities of the elderly population, such as the difficulty in memorizing complex passwords. The study contributes to the area of digital security and can be used as a basis for the development of public policies and technological solutions that guarantee the security and privacy of older adults in the digital age.

Keywords: Authentication; Older adults; Memory in the elderly; Visual passwords; Passwords verbal.

Lista de ilustrações

Figura 1 – Quadrado de Políbio. 30
Figura 2 – Revisão de Literatura. 53
Figura 3 – Faixa Etária. 78
Figura 4 – Nível Educacional. 78
Figura 5 – Frequência de Uso de Senhas. 79
Figura 6 – Forma de Escolha de Senhas. 79
Figura 7 – Dificuldade de Memorizar. 80
Figura 8 – Estratégias na memorização de senhas. 80
Figura 9 – Problemas com Memorização das Senhas. 81
Figura 10 – Recuperação de Senhas. 81
Figura 11 – Número de acertos imagens x Número de acertos palavras. . . . 82
Figura 12 – Etapas do modelo proposto 90
Figura 13 – Card com caracteres 113
Figura 14 – Card com imagens 114
Figura 15 – Card com imagens 115

Lista de tabelas

Tabela 1 – Resumo dos efeitos do envelhecimento para diferentes modalidades biométricas, adaptado de Lanitis; Tsapatsoulis 37
Tabela 2 – Diferenças entre IAL e AAL 44
Tabela 3 – Comparação entre Gov.br, eIDAS e NIST 46
Tabela 4 – Tabela de categorização da revisão de artigos 74
Tabela 5 – Continuação da Tabela 4 75
Tabela 6 – NIST - modelo atual x modelo proposto 94
Tabela 7 – eIDAS - modelo atual x modelo proposto 95
Tabela 8 – Gov.br - modelo atual x modelo proposto 96

Lista de abreviaturas e siglas

2FA: Autenticação de dois fatores

AAL: Authenticator Assurance Level

CBS: Cognitive Burden Scale

CEPSH: Comitê de Ética em Pesquisa com Seres Humanos

CNH: Carteira Nacional de Habilitação

CSF: Cybersecurity Framework

CTSS: Compatible Time-Sharing System

eIDAS: electronic IDentification, Authentication and trust Services

EUA: Estados Unidos da América

GDPR: General Data Protection Regulation

HIT: Health Information Technology

IAL: Identity Assurance Level

IBGE: Instituto Brasileiro de Geografia e Estatística

ICP-Brasil: Infraestrutura de Chaves Públicas Brasileira

IOT: Internet of Things

ISO: International Organization for Standardization

MIT: Massachusetts Institute of Technology

NA: Não Aplicável

NGA: Nível de Garantia de Autenticação

NGI: Nível de Garantia de Identidade

NIST: National Institute of Standards and Technology

ONU: Organização das Nações Unidas

PIN: Personal Identification Number

SMS: Short Message Service

TAM: Technology Acceptance Model

TIC: Tecnologia da Informação e Comunicação

TSE: Tribunal Superior Eleitoral

UE: União Européia

UFSC: Universidade Federal de Santa Catarina

UX: User Experience

Sumário

1 INTRODUÇÃO . . . 18
1.1 OBJETIVOS . . . 21
1.1.1 Objetivo Geral . . . 21
1.1.2 Objetivos Específicos . . . 21
1.2 JUSTIFICATIVA . . . 22
1.3 ESTRUTURA DA DISSERTAÇÃO . . . 22

2 METODOLOGIA DA PESQUISA . . . 24
2.1 Revisão sistemática da literatura . . . 24
2.2 Experimento com um grupo de idosos . . . 24
2.2.1 Considerações Éticas . . . 25
2.2.2 Limitações . . . 25

3 REFERENCIAL TEÓRICO SOBRE AUTENTICAÇÃO . . . 26
3.1 Introdução . . . 26
3.2 Autenticação em sistemas de saúde . . . 26
3.3 Fatores de autenticação . . . 27
3.3.1 Senhas . . . 28
3.3.1.1 Retomada Histórica . . . 29
3.3.1.2 O Desafio das Senhas . . . 32
3.3.1.3 A Importância das Senhas no Mundo Moderno . . . 33
3.3.2 Biometria . . . 34
3.3.2.1 Ataques à biometria . . . 35
3.3.2.2 Biometria e envelhecimento . . . 36
3.3.3 Outros Fatores de Autenticação . . . 38
3.4 Autenticação de Dois Fatores (2FA) . . . 39
3.5 Nível de Garantia de Identidade . . . 39
3.5.1 NIST . . . 40
3.5.2 eIDAS . . . 40

3.5.3 Gov.br . . . 41
3.6 Nível de Garantia de Autenticação . . . 41
3.6.1 NIST . . . 42
3.6.2 eIDAS . . . 42
3.6.3 Gov.br . . . 43
3.6.4 Discussão . . . 43
3.7 Conclusão . . . 47

4 REVISÃO DA LITERATURA: MEMORIZAÇÃO DE SENHAS POR PESSOAS IDOSAS . . . 48
4.1 Introdução . . . 48
4.2 Relação entre Senhas e a Terceira Idade . . . 49
4.3 Método . . . 51
4.4 Resultados e Discussão . . . 53
4.4.1 Estudo de Caso . . . 54
4.4.1.1 Envelhecimento . . . 54
4.4.1.2 Tecnologia da Saúde . . . 55
4.4.1.3 Segurança Cibernética . . . 56
4.4.1.4 Autenticação . . . 57
4.4.1.5 Senhas . . . 58
4.4.2 Experimento . . . 64
4.4.2.1 Senhas . . . 64
4.4.3 Revisão de Literatura . . . 67
4.4.3.1 Envelhecimento . . . 67
4.4.3.2 Tecnologia da saúde . . . 68
4.4.3.3 Acessibilidade . . . 69
4.4.3.4 Segurança cibernética . . . 70
4.4.3.5 Senhas . . . 70
4.5 Conclusão . . . 72

5 EXPERIMENTO . . . 76
5.1 Método . . . 76
5.1.1 Recrutamento dos Participantes . . . 76

5.1.2 Local das Atividades 76
5.1.3 Descrição das Atividades do Estudo 76
5.1.4 Critérios de Inclusão e Exclusão 77
5.2 Resultados 77
5.3 Discussão 82
5.3.1 Características Demográficas e Educacionais 82
5.3.2 Uso e Escolha de Senhas 83
5.3.3 Dificuldade e Estratégias de Memorização 83
5.3.4 Problemas com Senhas 84
5.3.5 Análise dos Dados de Senhas Baseadas em Imagens e Palavras . . . 84
5.3.6 Preferência por Imagens 84
5.3.7 Performance Variada 85
5.3.8 Implicações 85
5.3.9 Limitações 85
5.4 Conclusão 86

6 AUTENTICAÇÃO DAS PESSOAS IDOSAS 88
6.1 Fatores de Autenticação 88
6.1.1 Senhas Baseadas em Imagens 89
6.1.2 Biometria Senil 91
6.2 Nível de Garantia de Autenticação 92
6.2.1 NIST 93
6.2.2 eIDAS 93
6.2.3 Gov.br 94
6.2.4 Limitações 95
6.2.5 Contribuições 97

7 CONSIDERAÇÕES FINAIS 98

REFERÊNCIAS 100

GLOSSÁRIO 110

APÊNDICE A – QUESTIONÁRIO SOBRE MEMORIZAÇÃO DE SENHAS POR IDOSOS 111

APÊNDICE B – CARDS DE MEMORIZAÇÃO 113

ANEXO A – PARECER FINAL DO CEPSH-UFSC 117

1 Introdução

O envelhecimento da população é uma tendência global que tem se acelerado nas últimas décadas. Isto representa um crescimento mais elevado da população idosa com relação aos demais grupos etários. A transição demográfica no Brasil resultou em uma transformação de uma nação predominantemente jovem na década de 1980 para uma nação com uma população cada vez mais envelhecida, trazendo consigo uma maior consciência social sobre o envelhecimento (Oliveira; Salvador; Lima, 2023). É importante salientar que, de acordo com a legislação brasileira, uma pessoa é considerada idosa ao atingir a idade de 60 anos ou mais (Ministério da Saúde, 2023).

Segundo dados do último Censo 2022, do IBGE, a população idosa chegou a 32.113.490 (15,6%), um aumento de 56,0% em relação a 2010, quando era de 20.590.597 (10,8%). O índice de envelhecimento considerando-se a população com 60 anos ou mais chegou a 80,0 em 2022, com 80 pessoas idosas para cada 100 crianças de 0 a 14 anos. Em 2010, o índice de envelhecimento correspondia a 44,8. No Brasil, a expectativa de vida atingiu 77,3 anos e estima-se que a população idosa representará 26,8% do total até 2060 (Estatística, 2022).

A discussão sobre o envelhecimento da população tem como marco o Plano Internacional para o Envelhecimento, promovido pela ONU em 2002 (ONU, 2002). Este plano visa garantir um envelhecimento seguro e digno, assegurando que todos os idosos tenham seu lugar na sociedade e seus direitos de cidadania preservados. Assim como o artigo 3º do Estatuto do Idoso (Brasil, 2003) que garante absoluta prioridade aos idosos no acesso aos direitos, considerando a proteção do envelhecimento como um direito social.

Em dezembro de 2020, a Assembleia Geral da ONU promulgou uma resolução crucial, instituindo a Década do Envelhecimento Saudável de 2021 a 2030. Essa decisão representa uma abordagem vanguardista para forjar uma sociedade inclusiva e progressista, reconhecendo e valorizando todas as etapas da vida (ONU, 2020).

O perfil de saúde da população idosa é marcado por três principais tipos de

problemas: doenças crônicas, condições agudas decorrentes de causas externas e agravamento de condições crônicas, sendo as doenças crônicas uma característica marcante desta população (Saúde, 2023). Além disso, também podem ser acometidos por doenças infecciosas, doenças renais e cardiovasculares, complicações metabólicas, baixa qualidade de dieta, obesidade, declínio cognitivo, problemas odontológicos, lesões por quedas ou serem vítimas de uso inapropriado de medicamentos. Essas condições exigem uma atenção especializada e contínua, o que pode ser um desafio para os sistemas de saúde (Minayo; Gualhano, 2017).

É relevante destacar que, embora muitos idosos enfrentem doenças crônicas ou limitações físicas, essas acabam por lançar sombras sobre suas atividades diárias e a capacidade de usufruir plenamente dos serviços, muitas vezes projetados com um olhar voltado para os mais jovens.

No contexto da era digital, a saúde está se tornando cada vez mais integrada à tecnologia. Diariamente, novas tecnologias são incorporadas, incluindo inteligência artificial, *big data*, dispositivos móveis e vestíveis, além de processos que permitem a conexão à distância - todos contribuindo para um tratamento de dados abrangente e contínuo. Além disso, a saúde digital promove a inovação de processos e estruturas institucionais que organizam e coordenam a prestação de cuidados em vários níveis, abrangendo ações de vigilância, promoção e prevenção, bem como ações regulatórias e de gestão nos sistemas de saúde nacionais (Rachid et al., 2023).

Nesse cenário de constante evolução e inovação, os sistemas de informação desempenham um papel fundamental como facilitadores da saúde digital. Eles atuam como a espinha dorsal que suporta a integração de novas tecnologias e a coordenação de cuidados em vários níveis. Ao coletar, processar e distribuir dados de maneira eficiente, esses sistemas permitem que as instituições de saúde aproveitem ao máximo as oportunidades oferecidas pela era digital, melhorando a qualidade do atendimento e a eficiência dos processos (Rachid et al., 2023; Bonten et al., 2020; Laudon; Laudon, 2014).

Assim, surge uma questão primordial: a segurança do usuário e da informação. A autenticação do usuário, uma etapa importante de defesa, trabalha para proteger dados e sistemas contra ameaças cibernéticas. A autenticação, em sua

essência, avalia que o portador de uma identidade é quem ele descreve ser, através de uma combinação de fatores, sejam eles conhecidos, possuídos ou intrínsecos ao usuário (Tanenbaum, 2009).

A autenticação através do uso de senhas é o método mais utilizado. Neste método, o usuário fornece uma senha, que é uma sequência de caracteres secreta conhecida apenas por ele. O sistema de autenticação verifica a senha fornecida com a senha armazenada no banco de dados. Se as senhas forem iguais, o usuário é autenticado e autorizado a acessar o sistema ou recurso. A autenticação por senha oferece diversas propriedades desejáveis como por exemplo o baixo custo, a alta disponibilidade, ser fácil de implementar e ser reutilizável (Tran et al., 2022).

Entretanto, a segurança das senhas é um outro desafio crítico, pois os seres humanos têm dificuldade em lembrar sequências complexas. Os usuários geralmente optam por senhas simples, que são mais fáceis de lembrar, mas que também são mais fáceis de adivinhar (Tran et al., 2022). Além disso, o crescente número de serviços do nosso dia a dia que exigem senhas torna mais difícil lembrar senhas únicas para cada um deles (Pilar et al., 2012).

Assim, o processo de autenticação, embora essencial, pode se tornar mais uma barreira para os idosos, exacerbando a já preocupante exclusão digital que essa população enfrenta, um fenômeno conhecido como "exclusão digital cinzenta". Este termo refere-se à dificuldade que os idosos têm em acessar ou usar serviços digitais devido a diversas barreiras como falta de familiaridade com a tecnologia, dificuldades de aprendizado ou problemas de acessibilidade (Mubarak; Suomi, 2022).

Diante do cenário de envelhecimento populacional e sua interseção com a tecnologia digital, torna-se claro que é fundamental investigar de maneira mais aprofundada os desafios enfrentados pelos idosos em relação à autenticação e segurança digital. Dado que os sistemas de informação e computacionais desempenham um papel crucial na prestação de serviços de saúde e na gestão de informações pessoais, é imperativo assegurar que os processos de autenticação sejam acessíveis e adequados para todas as faixas etárias, incluindo os idosos.

Portanto, nosso ponto central de pesquisa emerge da seguinte questão:

Como aprimorar o processo de autenticação para a população idosa em diversos sistemas informatizados, a fim de torná-lo mais seguro, eficiente e inclusivo?

Compreendemos que a dificuldade dos idosos em acessar sistemas eletrônicos resulta em uma privação de acesso à informação, o que não favorece a equidade. Assim, é crucial que os sistemas sejam projetados considerando as necessidades e habilidades dos idosos, assegurando que eles não sejam marginalizados na era digital.

Neste contexto, nossa proposta é contribuir para a ciência por meio de um experimento que compara a capacidade de memorização de senhas baseadas em caracteres e senhas baseadas em imagens em um grupo de idosos. Além disso, sugerimos alterações nos níveis de garantia de autenticação para os idosos e introduzimos o conceito de biometria senil, que leva em conta as características únicas dessa população.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O objetivo geral deste estudo é propor alterações nos níveis de garantia de autenticação para a pessoa idosa e sugerir o uso de uma biometria que considera os processos de envelhecimento, a biometria senil.

1.1.2 Objetivos Específicos

Considerando o desenvolvimento do trabalho e o objetivo geral apresentado, destacam-se os seguintes objetivos específicos:

a) Elaborar uma revisão sistemática sobre a memorização de senhas na população idosa;

b) Comparar a capacidade de memorização de senhas baseadas em caracteres e senhas baseadas em imagens em um grupo de idosos;

c) Propor modificações nos níveis de garantia de autenticação;

d) Introduzir o conceito de biometria senil.

1.2 JUSTIFICATIVA

O envelhecimento da população é um marcador global em ascensão. Este fenômeno, presente em praticamente todas as regiões do mundo, tem implicações significativas e duradouras para todos os aspectos da sociedade.

Com o crescimento da população idosa, a compreensão e o enfrentamento das questões relacionadas à identidade desses indivíduos se tornam cada vez mais relevantes. A identidade de uma pessoa é um componente essencial de sua existência, e isso permanece inalterado com o avanço da idade.

Assegurar a inclusão dos idosos nos sistemas eletrônicos assume um papel de extrema relevância na sociedade contemporânea. Conforme a tecnologia avança, uma crescente parcela das nossas atividades cotidianas é convertida para o formato digital, abrangendo setores cruciais como assistência médica, finanças e interações sociais. A ausência de acesso adequado a esses sistemas eletrônicos por parte dos idosos pode resultar em sua exclusão de serviços essenciais. Além disso, o uso de tecnologia pode ajudar a melhorar a qualidade de vida dos idosos, permitindo-lhes manter a independência e o contato com a comunidade.

Entretanto, é fundamental que o acesso dos idosos aos sistemas eletrônicos seja não apenas garantido, mas também seguro e personalizado, o que evidencia a necessidade de maiores estudos sobre níveis de garantia de autenticação para a pessoa idosa e propostas que viabilizem a inclusão digital.

1.3 ESTRUTURA DA DISSERTAÇÃO

O presente trabalho está estruturado da seguinte maneira: no Capítulo 2, abordamos o método adotado no estudo. No Capítulo 3, fornecemos um panorama abrangente do referencial teórico relacionado à autenticação, explorando temas como fatores de autenticação, senhas, nível de garantia de identidade e nível de garantia de autenticação. O Capítulo 4 dedica-se à revisão de literatura sobre a memorização de senhas por pessoas idosas. O experimento conduzido nesta

dissertação é detalhado no Capítulo 5. No Capítulo 6, apresentamos uma proposta de modificação dos níveis de garantia para idosos. Por fim, as considerações finais do trabalho são apresentadas no Capítulo 7.

2 Metodologia da Pesquisa

Normalmente, as investigações no campo tecnológico são categorizadas como pesquisas aplicadas, com o objetivo de solucionar problemas específicos de um tema particular. O objetivo principal dessa categoria é gerar um novo conhecimento tecnológico ou aprofundar um existente, às vezes por meio da criação de um artefato. Um artefato pode ser um objeto físico, mas também pode ser uma ideia, uma proposta ou um *framework* (JUNIOR et al., 2017).

O projeto da pesquisa incluiu duas principais abordagens: a revisão sistemática da literatura sobre a memorização de senhas em idosos e um experimento controlado em que há a comparação da memorização de senhas baseadas em caracteres e senhas baseadas em imagens.

2.1 Revisão sistemática da literatura

A revisão sistemática de literatura foi conduzida para estabelecer uma base teórica sólida sobre senhas e suas formas, bem como identificar as melhores práticas em termos de segurança e usabilidade. O processo de revisão incluiu:

Identificação de fontes relevantes em bases de dados acadêmicas, revistas especializadas e livros; seleção de artigos, livros e estudos que abordam senhas, autenticação e o uso de senhas por idosos e análise crítica dos estudos selecionados para resumir os principais achados e tendências na literatura.

2.2 Experimento com um grupo de idosos

O experimento foi projetado para investigar como os idosos interagem com senhas baseadas em caracteres e senhas baseadas em imagens. Os participantes foram recrutados para o experimento e submetidos a um procedimento controlado.

2.2.1 Considerações Éticas

A pesquisa foi conduzida em conformidade com os princípios éticos, após autorização do Comitê de Ética em Pesquisa com Seres Humanos (CEPSH) da Universidade Federal de Santa Catarina (UFSC), incluindo o consentimento informado dos participantes, a garantia de sua privacidade e o tratamento ético dos dados.

2.2.2 Limitações

Este estudo apresenta algumas limitações que devem ser consideradas ao interpretar os resultados. Primeiramente, a pesquisa foi conduzida com um grupo pequeno de idosos, o que pode limitar a generalização dos resultados para a população idosa em geral.

Além disso, observou-se que alguns participantes ficaram nervosos com a tarefa de memorização, o que pode ter afetado seu desempenho e, consequentemente, os resultados do estudo. É possível que a pressão ou a ansiedade tenham interferido na capacidade dos participantes de memorizar as senhas.

Por fim, algumas respostas dos participantes são questionáveis, pois suspeitamos que eles podem não ter desejado demonstrar dificuldades em memorizar as senhas. Isso pode indicar um viés de resposta socialmente desejável, onde os participantes podem ter alterado suas respostas para evitar parecerem frágeis ou incapazes.

Essas limitações destacam a necessidade de estudos futuros com amostras maiores e estratégias para minimizar a ansiedade dos participantes e o viés de resposta. Além disso, pode ser útil explorar métodos alternativos de avaliação da memória que sejam menos dependentes do auto-relato dos participantes.

3 Referencial Teórico sobre Autenticação

3.1 Introdução

A autenticação em sistemas eletrônicos é um componente crucial da segurança da informação e da privacidade do usuário. Ela serve como a primeira linha de defesa contra acessos não autorizados, protegendo os dados e as informações dos usuários contra possíveis ameaças (Conti; Militello; Vitabile, 2017).

A autenticação envolve dois aspectos fundamentais: a garantia de identidade e a garantia de autenticação. A garantia de identidade refere-se à verificação da identidade de um usuário (Conti; Militello; Vitabile, 2017).

Por outro lado, a garantia de autenticação é o processo de confirmar que o usuário é quem ele afirma ser. Isso é frequentemente alcançado através do uso de senhas, PINs (do inglês *Personal Identification Number*), *tokens* de segurança ou métodos biométricos, como impressões digitais ou reconhecimento facial (Nenadic et al., 2007).

Ambas as garantias são essenciais para manter a integridade dos sistemas eletrônicos e a confidencialidade das informações do usuário. À medida que a tecnologia continua a evoluir, também evoluem as técnicas de autenticação, tornando-se cada vez mais sofisticadas para combater as crescentes ameaças à segurança cibernética.

3.2 Autenticação em sistemas de saúde

Nos sistemas de saúde, a segurança das informações é de suma importância, dada a sensibilidade dos dados armazenados. Em um mundo cada vez mais digitalizado, onde os registros médicos são mantidos eletronicamente e os tratamentos podem ser administrados remotamente, o nível de autenticação exigido precisa ser alto pois esses registros contêm detalhes íntimos da saúde de um paciente, seu histórico médico, informações de contato e, por vezes, detalhes financeiros (Kahani;

Elgazzar; Cordy, 2016).

Para proteger esses dados, sistemas de saúde implementam rigorosas camadas de verificação, assegurando que apenas indivíduos autorizados, como médicos, enfermeiros e profissionais administrativos, possam acessá-los. Uma única camada de proteção não é suficiente. Assim, para fortalecer a autenticação, métodos como senhas complexas, tokens físicos que geram códigos de acesso temporários e sistemas biométricos, como reconhecimento facial ou de impressão digital, são adotados (LEITÃO JÚNIOR et al., 2016).

3.3 Fatores de autenticação

Já é notório que a autenticação é um procedimento fundamental para assegurar a proteção das informações digitais, servindo para verificar a identidade de um usuário antes de permitir o acesso a sistemas e dados. Diversos fatores de autenticação estão disponíveis, cada um apresentando suas próprias características, benefícios e limitações. As três categorias de autenticação são (Velásquez; Caro; Rodríguez, 2018):

1. O que você sabe: Autenticação baseada em conhecimento, que exige que o usuário forneça uma credencial que ele conhece, como uma senha ou PIN.

2. O que você tem: Autenticação baseada em posse, que exige que o usuário forneça uma credencial que ele possui, como um cartão de identificação ou token de segurança.

3. O que você é: Autenticação baseada em característica, que exige que o usuário forneça uma credencial que é única para ele, como uma impressão digital ou um padrão facial.

Cada categoria de autenticação tem seus próprios pontos fortes e fracos. A autenticação baseada em conhecimento é a mais comum, pois é relativamente fácil de implementar e usar. No entanto, é também a mais vulnerável a ataques, pois as senhas podem ser facilmente adivinhadas ou roubadas. A autenticação baseada em posse é mais segura do que a autenticação baseada em conhecimento, pois as credenciais são mais difíceis de roubar. No entanto, ela pode ser inconveniente, pois

os usuários precisam carregar as credenciais com eles. A autenticação baseada em característica é a mais segura das três categorias, pois as credenciais são únicas para o usuário. No entanto, ela também é a mais cara e difícil de implementar (Velásquez; Caro; Rodríguez, 2018).

A escolha da categoria de autenticação adequada para uma determinada situação depende de uma série de fatores, incluindo o nível de risco aceitável, o custo e a facilidade de implementação.

Os esquemas de autenticação podem ser classificados com base no número de fatores aplicados no processo de autenticação (AlQahtani; El-Awadi; Min, 2021):

1. Autenticação de Fator Único (SFA): Neste esquema, a autenticação é realizada usando apenas um fator.

2. Autenticação de Dois Fatores (2FA): Este esquema de autenticação utiliza dois fatores diferentes. Por exemplo, a combinação de uma senha e um código temporário enviado por SMS.

3. Autenticação Multifator (MFA): Neste esquema, a autenticação é realizada com base em vários fatores diferentes. Por exemplo, além de códigos temporários e senhas, podem ser incluídos biometrias faciais.

3.3.1 Senhas

A senha, no contexto da segurança da informação, é uma sequência de caracteres, geralmente uma combinação de letras, números e símbolos, que serve como um mecanismo de autenticação para verificar a identidade de um usuário em um sistema ou serviço digital. É uma medida fundamental para garantir a privacidade e a proteção de informações sensíveis. Ela é um dos métodos de autenticação mais comuns, sendo usada em uma variedade de contextos, incluindo sistemas de login, redes Wi-Fi, aplicações móveis e sites.

A definição de senha varia de acordo com a fonte. O Instituto Nacional de Padrões e Tecnologia (NIST) define senha como "uma combinação de caracteres que um usuário usa para autenticar sua identidade" (Tecnologia, 2017). O Conselho Internacional de Padrões (ISO) define senha como "uma sequência de caracteres

usada para autenticar um usuário ou entidade" (Padrões, 2016).

Independentemente da sua definição, as senhas constituem um elemento crucial para a segurança da informação, contribuindo para a proteção de dados e sistemas contra acessos não autorizados.

3.3.1.1 Retomada Histórica

A origem das senhas remonta aos tempos antigos, quando eram usadas principalmente em contextos militares e cerimoniais. Na Antiguidade, era comum para guardas ou sentinelas desafiar aqueles que se aproximavam de postos avançados ou entradas de fortificações com algum tipo de sinal ou palavra-chave. Isso era usado para distinguir amigos de possíveis inimigos, especialmente em situações de pouca luz ou confusão.

Por exemplo, na Bíblia, no Livro dos Juízes (12:5-6), há uma história sobre os efraimitas e os gileaditas. Os gileaditas usaram a palavra "Sibolete" como uma espécie de senha para identificar efraimitas, que pronunciavam a palavra de maneira diferente. Aqueles que não puderam pronunciar a palavra corretamente foram identificados como inimigos.

Políbio, que teve sua vida transcorrida entre os anos 264-146 a.C., foi um historiador grego que é famoso por seus relatos sobre as guerras púnicas e da ascensão de Roma. Ele descreveu um método usado para comunicação a distância e para codificação de mensagens secretas, particularmente por meio de tochas ou tambores, usando uma grade 5x5 para representar letras do alfabeto, conforme ilustra a Figura 1. O quadrado era uma maneira de traduzir letras em uma combinação de dois números, que poderiam ser comunicados por uma variedade de métodos, como o número de batidas em um tambor ou o acendimento de tochas. A tabela se tornou uma ferramenta básica no estudo da criptografia (Arroyo; Dumdumaya; Delima, 2020).

À medida que a sociedade avançou, a necessidade de proteger informações e recursos também cresceu. Com a invenção da escrita, as pessoas começaram a registrar informações que desejavam manter em segredo. Surgiram então as primeiras formas de cifras e codificações, utilizadas para proteger mensagens e

Figura 1 – Quadrado de Políbio.

A	B	Γ	Δ	E
Z	H	Θ	I	K
Λ	M	N	Ξ	O
Π	P	Σ	T	Υ
Φ	X	Ψ	Ω	

Fonte: Adaptado de (Arroyo; Dumdumaya; Delima, 2020).

informações sensíveis (Naser, 2021).

Interessante que na turbulenta década de 1920, os Estados Unidos enfrentaram uma fase emblemática de sua história: a implementação da Lei Seca. Esta legislação, concebida com a intenção de combater os problemas relacionados ao consumo excessivo de álcool, teve consequências não intencionais e levou à proliferação de estabelecimentos clandestinos, os famosos "*speakeasy*". Nestes locais, bebidas alcoólicas eram comercializadas à margem da lei e, muitas vezes, a preços inferiores ao mercado regular. Para acessar tais ambientes, não bastava simplesmente querer entrar. Era essencial ser iniciado no segredo, o que geralmente envolvia a apresentação de um cartão especial, a menção de uma frase de código ou, em algumas situações, a declaração de uma senha específica. Estas precauções eram necessárias para garantir a segurança dos frequentadores e dos proprietários, mantendo a discrição e evitando a intervenção das autoridades (McClellan, 2012).

O século XX viu o nascimento da era digital. Com os primeiros computadores e, mais tarde, a internet, a proteção de dados tornou-se crucial. Senhas, agora em forma digital, eram o meio mais comum de proteger informações pessoais, bancárias e corporativas.

A Máquina Enigma, uma invenção notável desenvolvida na Alemanha na década de 1920, desempenhou um papel significativo durante a Segunda Guerra Mundial como um dispositivo de cifragem utilizado pelas forças armadas alemãs.

Criada originalmente para proteger comunicações comerciais e militares, a Enigma tornou-se conhecida por sua complexidade e eficácia na codificação de mensagens. Operando por meio de rotores intercambiáveis e um painel de entrada alfabética, a máquina oferecia milhões de combinações possíveis, tornando as mensagens aparentemente indecifráveis. A quebra do código da Enigma tornou-se um dos feitos mais notáveis da inteligência aliada, com a equipe liderada por Alan Turing desempenhando um papel crucial no desenvolvimento da primeira máquina capaz de decifrar as mensagens codificadas, contribuindo significativamente para a vitória dos Aliados na guerra. A Máquina Enigma, embora tenha sido uma ferramenta formidável de segurança para os alemães, acabou sendo decifrada, marcando um ponto de virada na história da criptografia e da guerra cibernética (Fiarresga et al., 2010).

Em 1961, durante os primórdios da era da computação, o professor de ciência da computação do MIT, Fernando Corbató, fez uma contribuição significativa ao mundo da segurança digital. Corbató estava trabalhando no desenvolvimento do Compatible Time-Sharing System (CTSS), uma das primeiras tentativas de criar um sistema de compartilhamento de tempo, que permitia que vários usuários utilizassem um computador simultaneamente (Corbató; Merwin-Daggett; Daley, 1962). Diante do desafio de garantir que cada usuário tivesse acesso seguro e individualizado ao sistema, ele introduziu o conceito de senha digital.

Essa abordagem era revolucionária na época e se tornou a fundação das práticas modernas de segurança cibernética. Ao atribuir uma senha única a cada usuário, Corbató não só resolveu um problema de projeto, mas também estabeleceu as bases para a autenticação digital, protegendo a privacidade e a integridade dos dados dos usuários em um ambiente compartilhado (Messerschmidt; Pleva, 2019).

A popularização da internet, que até então era um domínio de instituições acadêmicas e militares, tornou-se acessível a um público global. Ao entrar nos anos 2000, a onda digital cresceu exponencialmente. E-mails, fóruns online, redes sociais e uma variedade de plataformas digitais emergiram, cada uma requerendo que seus usuários criassem contas e, consequentemente, senhas.

Nesse cenário inovador, a necessidade de segurança digital não era tão

amplamente compreendida. Para muitos usuários da época, a internet era uma novidade e a ideia de ameaças cibernéticas parecia algo distante. A prática simplificada de usar a mesma senha em várias plataformas tornou-se comum, muitas vezes por pura conveniência ou por falta de conscientização sobre a importância de práticas seguras de gerenciamento de senhas.

Este comportamento inadvertidamente abriu as portas para adversários cibernéticos. A reutilização de senhas, combinada com métodos inseguros de armazenamento de dados por algumas empresas, resultou em um aumento significativo de violações de dados. Essas violações não apenas expuseram informações pessoais, mas também causaram perdas financeiras substanciais para indivíduos e empresas. Além das perdas monetárias, o impacto na privacidade dos usuários foi incalculável, com dados pessoais, históricos de navegação e outros detalhes sensíveis caindo nas mãos erradas (Siqueira et al., 2021).

O resultado foi um ambiente cibernético transformado em um verdadeiro campo de batalha. De um lado, hackers, equipados com ferramentas sofisticadas e motivados por ganhos financeiros, espionagem ou simplesmente pelo desafio. Do outro, profissionais de segurança, armados com as mais recentes tecnologias de proteção, trabalhando incansavelmente para defender sistemas e redes.

A luta entre esses dois lados tornou-se uma corrida armamentista tecnológica, com cada grupo tentando superar o outro em uma dança contínua de ataques e defesas. Essa corrida ainda ressoa hoje, enfatizando a necessidade vital de práticas robustas de segurança cibernética em nossa era digital interconectada.

3.3.1.2 O Desafio das Senhas

Senhas desempenham um papel fundamental no mundo digital contemporâneo, atuando como a primeira linha de defesa na proteção de informações pessoais e dados valiosos. Desde os primórdios da computação até a era da cibersegurança em que vivemos, elas evoluíram de simples palavras-chave a complexos algoritmos de autenticação (Stallings, 2010; Schneier, 2015).

A complexidade na criação de senhas não reside apenas na introdução de uma série de caracteres aleatórios, mas sim em um delicado equilíbrio. Este

equilíbrio é uma balança entre construir uma fortaleza digital e garantir que a senha possa ser facilmente lembrada pelo usuário. Senhas com uma combinação de letras maiúsculas e minúsculas, números e símbolos certamente oferecem um alto grau de segurança. No entanto, sua complexidade também pode torná-las difíceis de lembrar, levando a frequentes solicitações de redefinição e anotações inseguras.

Daí surge a relevância das "senhas mnemônicas". Estas são frases ou sequências de palavras construídas de forma que tenham significado pessoal e, portanto, sejam mais fáceis de recordar. A ideia é que, ao serem embasadas em memórias ou experiências pessoais, tais senhas se tornam intrinsecamente desafiadoras para invasores externos deduzirem (Dix, 2008).

Por exemplo, uma memória de infância ou uma citação favorita podem ser transformadas em uma senha forte e memorável. Assim, ao equilibrar sagazmente significado pessoal e complexidade, usuários podem fortalecer sua segurança digital sem sacrificar a facilidade de acesso.

3.3.1.3 A Importância das Senhas no Mundo Moderno

A era digital transformou radicalmente a maneira como vivemos, trabalhamos e nos comunicamos. Em meio a essa revolução tecnológica, a crescente dependência da internet se entrelaçou de forma inseparável com nosso cotidiano. Desde a verificação de e-mails matinais, passando pela interação em redes sociais e até mesmo ao acessar nossas contas bancárias, estamos constantemente navegando por um labirinto digital que exige autenticação a cada virada. Nesse cenário, as senhas emergem não apenas como chaves, mas como guardiãs de nossa identidade digital e privacidade.

O escopo do desafio das senhas vai além de plataformas digitais convencionais. Com a revolução da Internet das Coisas (IoT), objetos outrora simples de nosso dia a dia ganharam "inteligência" e conectividade. Geladeiras, fechaduras, câmeras de segurança e até mesmo termostatos estão agora interligados em redes, muitas vezes protegidos apenas por senhas. Assustadoramente, uma senha fraca em um desses dispositivos pode ser a porta de entrada para um invasor, ameaçando não apenas a segurança de nossos dados, mas também a integridade de nossos lares e

bem-estar físico (Alves, 2021).

A importância de uma senha forte e única não deve ser subestimada. Aqui estão algumas melhores práticas, de acordo com Federal Trade Commision Consumer Advice (Commission, 2023):

Complexidade: As senhas devem conter uma mistura de letras maiúsculas e minúsculas, números e símbolos.

Tamanho: Senhas curtas são facilmente decifráveis. Recomenda-se que uma senha tenha pelo menos 12 caracteres.

Evitar informações pessoais: Nunca use detalhes facilmente acessíveis, como aniversário ou nome de animais de estimação.

Atualização regular: Mesmo as senhas mais fortes devem ser alteradas regularmente.

Gerenciadores de senha: Estas ferramentas criam e armazenam senhas fortes para cada serviço que você usa, garantindo que cada senha seja única.

3.3.2 Biometria

A biometria é a técnica de identificar indivíduos com base em características físicas ou comportamentais distintas, como impressões digitais, reconhecimento facial ou de voz. Embora a biometria tenha origens antigas, com impressões digitais sendo usadas em documentos na China antiga, a tecnologia atual ampliou sua aplicação em diversas áreas, desde o desbloqueio de smartphones até o acesso a instalações de alta segurança. Um dos principais benefícios da biometria é sua segurança inerente, pois as características biométricas são únicas para cada indivíduo e, diferentemente das senhas, não podem ser esquecidas ou perdidas (Sarkar; Singh, 2020).

No entanto, a biometria também apresenta implicações éticas. A coleta e armazenamento de dados biométricos geram questões sobre sua guarda, acesso e uso, trazendo à tona preocupações de privacidade. Além disso, uma vez que os

dados biométricos são irrevogáveis e não podem ser alterados como uma senha, se forem comprometidos, podem representar um risco ao longo da vida do indivíduo.

Legalmente, muitas jurisdições exigem consentimento explícito para coletar e armazenar esses dados, e regulamentações, como o *General Data Protection Regulation* (GDPR) na Europa, impõem normas rigorosas para sua manipulação (Regulation, 2018). Socialmente, embora a biometria seja vista como um meio conveniente de autenticação, ela traz consigo preocupações relativas à privacidade e segurança.

Para abordar alguns desses desafios, estão surgindo soluções que focam no armazenamento seguro de dados biométricos, como mantê-los localmente no dispositivo do usuário, em vez de em servidores centralizados (Tanwar et al., 2019).

3.3.2.1 Ataques à biometria

Os métodos biométricos mais comuns incluem impressões digitais, reconhecimento facial, íris, voz e padrões de veias. Cada um desses métodos se baseia na singularidade das características biológicas de um indivíduo, tornando-os aparentemente seguros. Contudo, a complexidade dos sistemas biométricos não está imune a tentativas de manipulação.

Um dos ataques à biometria mais conhecidos é a falsificação de impressões digitais. Utilizando técnicas avançadas, hackers conseguem criar réplicas das impressões digitais de uma pessoa. Isso pode ser feito por meio da impressão 3D ou até mesmo utilizando materiais flexíveis para reproduzir a textura e características únicas da pele. Além disso, ataques de impressões digitais falsas também podem ocorrer através da obtenção de impressões digitais deixadas em superfícies, como copos ou telas sensíveis ao toque, e sua posterior reprodução (Sharif et al., 2019).

O reconhecimento facial, apesar de sua popularidade, também enfrenta desafios significativos. Ataques utilizando máscaras 3D têm sido bem-sucedidos em enganar sistemas de segurança baseados em reconhecimento facial. Estes ataques exploram as limitações dos algoritmos de detecção, que podem não distinguir adequadamente entre uma face real e uma representação tridimensional bem elaborada (Neto et al., 2022).

Outro ponto de vulnerabilidade é o chamado "ataque de apresentação", em que uma imagem ou vídeo é usado para simular a presença física do indivíduo diante do sistema biométrico. Tecnologias de detecção de vida, como o reconhecimento de piscar de olhos, são implementadas para mitigar esse tipo de ataque, mas ainda assim, há desafios para tornar esses sistemas à prova de fraudes (Sharif et al., 2019).

É importante mencionar que a biometria não é invulnerável e, como qualquer tecnologia, requer constante aprimoramento para lidar com as ameaças emergentes. A evolução constante dos métodos de ataque destaca a necessidade de abordagens multifacetadas na segurança biométrica. Isso inclui a implementação de técnicas antifraude, como o reconhecimento de padrões anômalos de comportamento, o uso de autenticação multifatorial e a integração de inteligência artificial para detecção de tentativas de manipulação.

3.3.2.2 Biometria e envelhecimento

O desempenho dos sistemas de autenticação biométrica é impactado por disparidades entre os dados armazenados nos modelos biométricos e os dados correspondentes derivados dos reais detentores desses modelos. Tais disparidades são principalmente atribuídas às variações intra-individuais das características biométricas. Dentro de todas as formas de variações intra-individuais, destaca-se a variação relacionada ao envelhecimento, a qual apresenta características únicas que tornam a gestão do envelhecimento uma tarefa desafiadora (Lanitis, 2010).

O trabalho de Scheidat et al. sugere uma nova abordagem para comparar resultados de diversas avaliações biométricas no contexto do envelhecimento biológico dos usuários. Para as três modalidades biométricas (Impressão digital, face e íris) foi demonstrado que o desempenho do sistema e a usabilidade são dependentes do envelhecimento. Na maioria dos casos, os problemas são descritos principalmente em grupos etários muito jovens e muito idosos.

A variação do envelhecimento causa modificações nas características biométricas que afetam a correspondência entre modelos biométricos armazenados e capturados, causando, assim, deterioração no desempenho dos sistemas de autenticação biométrica, conforme demonstrado na tabela 1 (Lanitis; Tsapatsoulis,

2011).

Tabela 1 – Resumo dos efeitos do envelhecimento para diferentes modalidades biométricas, adaptado de Lanitis; Tsapatsoulis

Modalidade biométrica	**Efeitos diretos do envelhecimento**	**Efeitos indiretos do envelhecimento**
Face	Crescimento ósseo Redução da elasticidade da pele	Doenças (diabetes, doenças cardíacas) Estilo de vida
Íris	Modificações nos padrões da íris	Doenças (catarata, glaucoma)
Impressões digitais	Redução da elasticidade da pele Desgaste	Lesões
Palma	Crescimento ósseo Desgaste	Doenças (artrite)
Voz	Redução da capacidade pulmonar Atrofia muscular vocal	Doenças (laringite, câncer de pescoço)
Comportamental	Redução da força muscular Redução da visão e audição	Doenças (parkinson, acidente vascular cerebral)

Ainda, de acordo com o artigo "Review of Ageing with respect to Biometrics and Diverse Modalities", podemos afirmar que o envelhecimento afeta os modelos biométricos. Os autores do artigo realizaram uma revisão sistemática da literatura sobre os efeitos do envelhecimento em diferentes modalidades e concluíram que o envelhecimento pode causar uma série de mudanças nas características biométricas, incluindo: redução da elasticidade da pele; crescimento ósseo; modificações nos padrões da íris; alterações na voz e alterações no comportamento. Essas mudanças podem dificultar a correspondência entre modelos biométricos armazenados e capturados, o que pode levar a um aumento na taxa de falsa rejeição. Além disso, o envelhecimento pode causar uma diminuição no desempenho a longo prazo de um sistema biométrico, pois as características biométricas continuam a mudar com o tempo (Lanitis; Tsapatsoulis; Maronidis, 2013).

3.3.3 Outros Fatores de Autenticação

Em resposta às crescentes ameaças cibernéticas e à necessidade de garantir uma segurança mais robusta para sistemas e dados sensíveis, foram desenvolvidos métodos mais avançados de autenticação. Um desses métodos é a Autenticação Baseada em Comportamento, que analisa o comportamento do usuário durante o uso do sistema, levando em consideração a maneira como o usuário digita, sua localização geográfica, a velocidade com que ele interage com o sistema e outros padrões de uso para determinar se a autenticação é legítima (Shahzad; Liu; Samuel, 2017).

Outro método é a Autenticação por Reconhecimento de Íris, uma técnica de autenticação biométrica baseada na análise da íris dos olhos de um usuário. Este método é altamente preciso e oferece uma camada adicional de segurança, pois a íris de cada pessoa é única (Singh et al., 2020).

A Autenticação por Reconhecimento de Voz também é um método eficaz, pois a voz de uma pessoa é única. Este método envolve a análise das características vocais para confirmar a identidade do usuário (Abozaid et al., 2019).

Além do reconhecimento facial 2D, o reconhecimento facial 3D é outro método de autenticação que utiliza sensores 3D para criar uma imagem tridimensional do rosto do usuário, tornando a autenticação mais segura e resistente a falsificações (Zhang et al., 2006).

Por fim, a Autenticação por Biometria Comportamental é uma técnica que considera o comportamento do usuário, como a maneira como ele segura o dispositivo, a pressão exercida na tela e outros padrões comportamentais para verificar a identidade (Liang et al., 2020).

A escolha do método de autenticação mais adequado depende dos requisitos de segurança, do nível de risco e das necessidades específicas de uma aplicação ou sistema.

3.4 Autenticação de Dois Fatores (2FA)

A Autenticação de Dois Fatores (2FA) é um método que confirma a identidade do usuário usando duas formas diferentes de verificação. Isso geralmente envolve a combinação de algo que o usuário sabe, como uma senha, com algo que o usuário tem, como um token ou um código enviado ao telefone.

O conceito de usar múltiplos fatores para autenticação tem uma longa história, mas, com o aumento dos ataques cibernéticos e a facilidade de comprometimento de senhas, a 2FA tornou-se uma norma essencial para a segurança online. Ela oferece uma camada adicional de segurança, pois mesmo que um invasor consiga a senha de um usuário, ele ainda precisará do segundo fator de autenticação para acessar a conta (Ometov et al., 2018).

No entanto, há implicações éticas associadas ao uso da 2FA. Por exemplo, usar dispositivos pessoais para receber códigos ou notificações de autenticação pode invadir a privacidade do usuário, especialmente se a plataforma compartilhar mais dados do que o necessário.

Além disso, nem todos têm acesso a dispositivos móveis ou à tecnologia necessária para a 2FA, levantando preocupações sobre a exclusão digital. Legalmente, em algumas jurisdições, as empresas são obrigadas a fornecer opções de segurança robustas, como a 2FA, particularmente em setores como finanças e saúde.

Do ponto de vista social, apesar dos benefícios de segurança da 2FA, ela pode ser vista como um incômodo por alguns, o que pode afetar sua adoção. Em resposta a esses desafios, empresas estão explorando soluções emergentes como métodos de autenticação que não dependem de senhas, incluindo aquelas baseadas em biometria ou tokens físicos (Gilsenan et al., 2023).

3.5 Nível de Garantia de Identidade

A identidade se refere ao conjunto de características que definem um indivíduo ou entidade, destacando-o como único entre os diversos agentes da sociedade (Faria; Souza, 2011).

O Nível de Garantia de Identidade (NGI) ou Identity Assurance Level (IAL) refere-se à confiança na validação da identidade do usuário. Ele está preocupado com a coleta e verificação de informações sobre uma pessoa durante o processo de registro. Isso pode incluir a verificação de documentos de identidade, dados biométricos ou outras informações pessoais (Standards; Technology, 2017).

3.5.1 NIST

O National Institute of Standards and Technology (NIST), é uma agência governamental dos Estados Unidos que desenvolve padrões, diretrizes, melhores práticas e outros recursos para atender às necessidades de indústrias, agências federais e do público em geral. O NIST define três níveis de garantia de identidade (Standards; Technology, 2017):

IAL1: No IAL1, os atributos, se houver, são autodeclarados ou devem ser tratados como autodeclarados.

IAL2: No IAL2, é necessária a comprovação de identidade remota ou presencial. O IAL2 exige que os atributos de identificação sejam verificados pessoalmente ou remotamente.

IAL3: No IAL3, é necessária a comprovação de identidade presencial. Os atributos de identificação devem ser verificados por um representante autorizado.

3.5.2 eIDAS

O electronic IDentification, Authentication and trust Services (eIDAS) é um regulamento da União Europeia (UE) que estabeleceu um sistema unificado para identificação eletrônica e serviços de confiança, simplificando a oferta de serviços em toda a União Europeia (Parliament; Union,).

O eIDAS promoveu a interoperabilidade entre os 27 Estados-Membros da UE, assegurando que esses países reconheçam reciprocamente os sistemas de identificação eletrônica notificados uns pelos outros (Parliament; Union,).

De acordo com o eIDAS, existem três níveis de garantia de identidade:

Baixo: por exemplo, a inscrição é realizada por auto-registro em uma página web, sem qualquer verificação de identidade ;

Substancial: por exemplo, a inscrição é realizada fornecendo e verificando informações de identidade, e a autenticação usando um nome de usuário e uma senha e uma senha de uso único enviada para o seu celular;

Alta: por exemplo, a inscrição é realizada mediante registro presencial em um escritório e a autenticação por meio de cartão inteligente, como a Carteira de Identidade Nacional.

3.5.3 Gov.br

No Brasil, a conta gov.br é a iniciativa do Governo Federal para facilitar a identificação e autenticação do cidadão no ambiente digital. Ela proporciona um meio seguro para o indivíduo acessar os serviços públicos digitais usando dispositivos tecnológicos modernos como smartphones, computadores, laptops e tablets. O Gov.br oferece três níveis de garantia de identidade (Brasil, 2023):

Nível Bronze: Auto-registro com conferência de dados em bases do governo.

Nível Prata: Validação dados via autenticação em banco credenciado, reconhecimento facial CNH.

Nível Ouro: Validação dos dados com certificado ICP-Brasil, reconhecimento facial TSE.

3.6 Nível de Garantia de Autenticação

O Nível de Garantia de Autenticação (NGA) ou Authenticator Assurance Level (AAL) refere-se à confiança na autenticação de um usuário quando ele tenta acessar um sistema. Ele está preocupado com a forma como um usuário é autenticado no momento do acesso, como a utilização de senhas, tokens de hardware, biometria ou outros métodos de autenticação (Tecnologia, 2017).

Os níveis de garantia de autenticação variam de acordo com a aplicação e o contexto, sendo mais rigorosos em cenários que envolvem informações sensíveis,

transações financeiras ou serviços críticos.

3.6.1 NIST

O NIST, já mencionado anteriormente, é uma autoridade mundial em segurança da informação e seus padrões são amplamente adotados por organizações de todos os tamanhos e setores. O NIST estabele três níveis de garantia de autenticação (Tecnologia, 2017):

AAL1: O AAL1 fornece alguma garantia de que o usuário controla um autenticador registrado para o assinante. O AAL1 requer autenticação de fator único usando uma ampla gama de tecnologias de autenticação disponíveis. A autenticação bem-sucedida requer que o usuário comprove a posse e o controle do(s) autenticador(es) por meio de um protocolo de autenticação seguro.

AAL2: O AAL2 fornece alta confiança de que o usuário controla um(s) autenticador(es) registrado(s) para o assinante. É necessária a prova de posse e controle de dois fatores de autenticação diferentes por meio de um protocolo de autenticação seguro. Técnicas criptográficas aprovadas são necessárias no AAL2 e acima.

AAL3: O AAL3 fornece uma confiança muito alta de que o usuário controla um(s) autenticador(es) registrado(s) para o assinante. A autenticação no AAL3 é baseada na prova de posse de uma chave por meio de um protocolo criptográfico. O AAL3 é semelhante ao AAL2, mas também requer um autenticador criptográfico "rígido"que fornece resistência à personificação do verificador.

3.6.2 eIDAS

O eIDAS, também já mencionado anteriormente, estabelece um quadro para a autenticação eletrônica transfronteiriça e propõe três níveis de garantia (Parliament; Union,):

Baixa: A autenticação é baseada em um fator, como uma senha ou uma pergunta de segurança;

Substancial: A autenticação é baseada em dois fatores, como uma senha e um *token* ou uma senha e uma prova de vida;

Alta: A autenticação é baseada em três fatores, como uma senha, um *token* e uma prova de vida.

3.6.3 Gov.br

O nível de garantia de autenticação do gov.br é um conceito usado pelo governo brasileiro para estabelecer um padrão de segurança para a autenticação em serviços públicos online. O Gov.br oferece três níveis de garantia de autenticação (Brasil, 2023):

Nível Bronze: Requisito mínimo de garantia, fornecido por uma senha ou outro fator de conhecimento.

Nível Prata: Garantia moderada, fornecido por uma combinação de fatores de conhecimento e posse, como uma senha e um token de segurança.

Nível Ouro: Garantia alta, fornecido por uma combinação de fatores de conhecimento, posse, inerência e contexto, como uma senha, um token de segurança, uma impressão digital e um reconhecimento de localização.

3.6.4 Discussão

O Nível de Garantia de Identidade (IAL) e o Nível de Garantia de Autenticação (AAL) são dois conceitos importantes na segurança da informação, especialmente quando se trata de autenticação de usuários. Enquanto o IAL refere-se à confiabilidade e certeza associadas à atribuição de identidade a uma entidade (como um usuário, dispositivo ou serviço) em um sistema, o AAL refere-se ao grau de confiabilidade associado ao processo de autenticação, que é o ato de verificar que a entidade é realmente quem ela afirma ser, de acordo com o exemplificado na tabela 2.

Em relação às comparações específicas dos níveis de garantia de autenticação, elaboramos a tabela 3 para visualização.

Tabela 2 – Diferenças entre IAL e AAL

	Nível de Garantia de Identidade (IAL)	**Nível de Garantia de Autenticação (AAL)**
Definição	Refere-se à confiança na validação da identidade do usuário.	Refere-se à confiança na autenticação de um usuário quando ele tenta acessar um sistema.
Foco	Coleta e verificação de informações sobre uma pessoa durante o processo de registro.	A forma como um usuário é autenticado no momento do acesso.
Exemplos	Verificação de documentos de identidade, dados biométricos ou outras informações pessoais.	Utilização de senhas, tokens de hardware, biometria ou outros métodos de autenticação.

Objetivo: Gov.br e eIDAS têm objetivos semelhantes, que são facilitar o acesso a serviços públicos digitais e promover a identificação eletrônica. Já o NIST não tem um objetivo específico, mas fornece orientações e recomendações para a autenticação de usuários.

Alcance: Gov.br e o NIST tem um alcance nacional, enquanto eIDAS tem um alcance europeu.

Abrangência: Gov.br abrange apenas serviços públicos digitais do governo federal brasileiro. eIDAS abrange governos e empresas da União Europeia. O NIST abrange o governo americano.

Níveis de garantia: Gov.br, NIST e eIDAS oferecem três níveis de garantia.

Métodos de autenticação: Gov.br suporta uma variedade de métodos de autenticação, incluindo senhas, tokens de segurança, biometria e reconhecimento facial. O eIDAS também suporta uma variedade de métodos de autenticação, incluindo cartões de cidadão, certificados digitais, biometria e reconhecimento facial. O NIST não especifica métodos de autenticação específicos, mas recomenda o uso de uma combinação de fatores de conhecimento, posse e intrínsecas.

Regulação: Gov.br é regulamentado pela Lei nº 14.063, de 24 de setembro de 2020. O eIDAS é regulamentado pelo Regulamento (UE) nº 910/2014 do Parlamento

Europeu e do Conselho de 23 de julho de 2014. O NIST é regulamentado por várias leis federais dos EUA. No entanto, o NIST Cybersecurity Framework (CSF), um conjunto de padrões, diretrizes e práticas recomendadas para gerenciar riscos relacionados à segurança cibernética, é uma estrutura voluntária.

Tabela 3 – Comparação entre Gov.br, eIDAS e NIST

Característica	**Gov.br**	**eIDAS**	**NIST**
Objetivo	Facilitar o acesso a serviços públicos digitais do governo federal brasileiro	Facilitar a identificação eletrónica e a prestação de serviços transfronteiriços na União Europeia	Fornecer orientações e recomendações para a autenticação de usuários
Alcance	Brasil	União Europeia	EUA
Abrangência	Governo federal brasileiro	Governos e empresas da União Europeia	Governo americano
Níveis de garantia	Bronze, prata e ouro	Baixo, substancial e alto	AAL1, AAL2 e AAL3
Métodos de autenticação	Senhas, tokens de segurança, biometria e reconhecimento facial	Cartões de cidadão, certificados digitais, biometria e reconhecimento facial	Senhas, tokens de segurança, biometria e outros fatores de conhecimento, posse e inerência
Regulação	Lei nº 14.063, de 24 de setembro de 2020	Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014	Publicação Especial 800-63-3 do NIST

3.7 Conclusão

A importância dos níveis de garantia de identidade e níveis de garantia de autenticação no contexto da segurança digital é inegável. Esses parâmetros desempenham um papel crítico na construção de sistemas digitais seguros e confiáveis, essenciais na proteção de informações sensíveis e na prevenção de fraudes cibernéticas. O NIST estabeleceu diretrizes rigorosas para a autenticação e identificação, fornecendo um quadro de referência sólido para garantir a confiabilidade dos sistemas digitais. Da mesma forma, a União Europeia, por meio do eIDAS, promove a interoperabilidade e a segurança dos sistemas de identificação eletrônica em toda a UE. No Brasil, o programa Gov.br busca aprimorar a segurança e a conveniência na interação dos cidadãos com o governo, estabelecendo níveis de garantia que protegem a privacidade e a confiabilidade dos dados.

Após uma análise sobre autenticação de usuários em sistemas eletrônicos, onde exploramos os conceitos de garantia de identidade, garantia de autenticação e os diversos fatores de autenticação, é importante considerar como esses métodos se aplicam a diferentes grupos demográficos. Em particular, a população idosa pode enfrentar desafios únicos na interação com esses sistemas. Portanto, vamos agora fazer uma transição para uma revisão sistemática sobre a memorização de senhas na população idosa. Esta revisão irá lançar luz sobre como os idosos lidam com a tarefa de memorizar senhas, um componente crucial da autenticação do usuário, e como os sistemas podem ser projetados para melhor atender às suas necessidades.

4 Revisão da Literatura: Memorização de Senhas por Pessoas Idosas

4.1 Introdução

No cenário contemporâneo, não se pode negar a profundidade e abrangência da revolução digital. Cada vez mais, estar conectado se tornou um sinônimo de participação ativa na sociedade moderna, e a inclusão digital agora serve como um pilar para a inclusão social plena (Sayago; Blat, 2009). Esta realidade é especialmente palpável quando refletimos sobre a população idosa. Embora muitos sejam rápidos em celebrar os benefícios da digitalização, para a terceira idade, o ambiente digital pode ser uma paisagem repleta de desafios e incertezas.

As senhas, os portões silenciosos que guardam nossos segredos mais valiosos, surgem como um ponto crucial nesse contexto. Historicamente, os seres humanos sempre adotaram mecanismos para proteger suas informações. Desde as antigas civilizações, como a Mesopotâmia e o Egito, a humanidade tem empregado palavras-chave para garantir acesso a locais e informações sagrados. No campo de batalha, as senhas eram um sinal de confiança, garantindo que mensageiros eram genuínos e suas mensagens permaneciam intactas (Florencio; Herley, 2007).

Com a invenção dos computadores e a ascensão da era da informação no século XX, a senha foi elevada de um mero código falado para um mecanismo digital de proteção. A explosão da internet nos anos 90 catapultou a senha para a linha de frente da segurança cibernética, exigindo novos e mais complexos formatos de autenticação. No entanto, o que ganhamos em segurança, muitas vezes perdemos em facilidade de memorização, levando a uma busca contínua por equilíbrio entre segurança e praticidade.

O envelhecimento populacional é uma realidade incontestável que se estende por diversas partes do mundo. Em um panorama global, observa-se uma reconfiguração demográfica marcada pelo crescimento expressivo do número de

indivíduos idosos. Esta tendência não é somente evidente em nações desenvolvidas, mas também em países em desenvolvimento, como o Brasil.

No contexto brasileiro, o processo de envelhecimento apresenta características e desafios peculiares, influenciados por aspectos históricos, sociais e de saúde pública. Entre os determinantes deste fenômeno, podemos citar o aumento da expectativa de vida e as significativas transformações nas condições de saúde ao longo das últimas décadas.

O número de brasileiros idosos de 60 anos ou mais era de 2,6 milhões em 1950, passou para 29,9 milhões em 2020 e deve alcançar 72,4 milhões em 2100. O crescimento absoluto foi de 27,6 vezes. Em termos relativos, a população idosa de 60 anos ou mais representava 4,9% do total de habitantes de 1950, passou para 14% em 2020 e deve atingir o impressionante percentual de 40,1% em 2100 (um aumento de 8,2 vezes no peso relativo entre 1950 e 2100) (Alves, 2019).

Além disso, vale ressaltar que a população idosa contemporânea está imersa em um período de intensas mudanças tecnológicas, sendo parte integrante da revolução digital. Nesse cenário, a capacidade de memorizar senhas complexas não se restringe a uma necessidade de segurança. Mais do que isso, representa um instrumento que confere independência e autonomia a esses indivíduos na era digital, permitindo-lhes acesso e participação ativa no mundo cibernético.

Portanto, ao longo desta revisão, exploraremos a relação entre a população idosa e os desafios associados à memorização de senhas, buscando compreender como a tecnologia e a demografia se entrelaçam no século XXI.

4.2 Relação entre Senhas e a Terceira Idade

Em nossa era de avanços digitais constantes, uma população frequentemente relegada à periferia da revolução digital emerge com necessidades únicas e desafios distintos: nossos idosos. À medida que a população mundial envelhece, torna-se cada vez mais evidente que as soluções tecnológicas amplamente adotadas não estão satisfazendo todos os segmentos da sociedade de maneira equitativa (Hülür; Macdonald, 2020).

O aumento no número de pessoas idosas não é apenas um testemunho das conquistas da medicina moderna e de estilos de vida mais saudáveis, mas também representa uma mudança demográfica que traz consigo um conjunto de desafios e oportunidades. Uma dessas dificuldades, embora possa parecer trivial para os nativos digitais, é a interação com a tecnologia através do ritual quase universal de inserir senhas (Alves, 2019).

O ato de lembrar e inserir senhas tornou-se uma ação tão corriqueira que muitos de nós nem sequer percebem o processo. No entanto, para a população idosa, que pode enfrentar declínios naturais na memória e na cognição, este processo é tudo menos simples. Imagine por um momento que cada visita a um site, cada tentativa de fazer uma compra online, ou cada acesso a uma plataforma social se tornasse um quebra-cabeça mental. Não só isso, mas um quebra-cabeça que, se resolvido incorretamente várias vezes, pode bloquear o acesso ou causar outros problemas.

Ao observarmos de perto, percebemos que esse desafio está enraizado em dois dilemas principais. O primeiro é a necessidade de ter senhas robustas para proteger as informações e a privacidade. Em um mundo onde os cibercriminosos estão constantemente aprimorando suas habilidades, senhas como "123456" ou "senha" são convites abertos para problemas. Assim, as diretrizes de segurança cibernética têm insistido em senhas mais complexas, muitas vezes combinando letras, números e símbolos, além de encorajar a mudança regular destas.

O segundo dilema é a capacidade cognitiva. Com o envelhecimento, é natural que ocorram mudanças na memória e na capacidade de processar informações. Para muitos idosos, a tarefa de criar, lembrar e atualizar constantemente uma série de senhas complicadas para diferentes plataformas torna-se não apenas desafiadora, mas também angustiante (Melo et al., 2017).

Isso nos leva ao risco real da exclusão digital. A incapacidade de gerenciar senhas pode levar a uma relutância em interagir com plataformas digitais. Em uma era em que serviços essenciais, comunicações e até entretenimento estão se movendo para o domínio online, não poder acessar ou sentir-se confortável no espaço digital é equivalente a um tipo de isolamento.

Mas, onde há desafios, também há oportunidades para inovação e crescimento. A situação atual é um apelo para os designers de Experiência do Usuário (ou User Experience - UX), desenvolvedores e especialistas em cibersegurança reimaginar a forma como abordamos a autenticação. Está na hora de conceber soluções que sejam seguras, mas também acessíveis e amigáveis para aqueles que não cresceram na era digital.

Algumas soluções emergentes incluem autenticação biométrica, como reconhecimento facial ou de impressões digitais, e sistemas de autenticação de dois fatores que enviam códigos para dispositivos confiáveis. Estas opções, embora promissoras, ainda precisam ser otimizadas para a população idosa, garantindo que sejam intuitivas e fáceis de usar.

Em última análise, à medida que a sociedade avança e adota tecnologias, é essencial que não deixemos ninguém para trás. O dilema das senhas e da população idosa é apenas um exemplo de como precisamos pensar de forma mais inclusiva em nosso mundo digital. Afinal, a tecnologia deve servir à humanidade em toda a sua diversidade e complexidade. E isso inclui garantir que nossos idosos tenham acesso seguro e sem estresse ao mundo digital que muitos de nós damos como certo.

4.3 Método

O presente capítulo consiste em uma revisão sistemática da literatura pertinente a memorização de senhas na população idosa. Conforme descrito por Grant e Booth, em 2009, essas revisões representam uma abordagem sistemática e abrangente que visa capturar, descrever e discutir o desenvolvimento ou o "estado da arte" de um tópico particular, seja através de uma lente teórica ou contextual (Grant; Booth, 2009).

Tal método se baseia em uma extensa investigação de fontes diversificadas como livros, artigos de periódicos impressos e eletrônicos, proporcionando uma síntese coerente das informações disponíveis. Durante este processo, a interpretação e avaliação crítica do autor tornam-se essenciais para discernir e destacar os aspectos mais relevantes da literatura.

O valor intrínseco de tal abordagem reside em sua capacidade de oferecer uma visão consolidada e aprofundada sobre o tema, servindo como ferramenta vital para a educação contínua. Ela age como um veículo que permite ao leitor assimilar e se atualizar rapidamente sobre avanços recentes e principais debates em torno de um tópico específico.

Para a realização desta revisão, foi conduzida uma pesquisa sistemática nas bases de dados acadêmicas PubMed (NLM, 2023), Scientific Eletronic Library Online (SCIELO) (Fapesp, 2023), Google Scholar (Google, 2023) e Semantic Scholar (Allen Institute, 2023). Foram adotadas as seguintes combinações de palavras-chave para otimizar a identificação de estudos relevantes: ((“Password") AND ("Older Adults”) OR ("Password") AND ("Memory") AND ("Older Adults") OR ("Authentication") AND ("Older Adults") OR ("Multi-Factor Authentication") AND ("Older Adults"))

Essas chaves de busca foram empregadas com o objetivo de abranger uma variedade de estudos relacionados ao tema principal, que é a memorização e uso de senhas entre a população idosa.

Foram incluídos artigos disponibilizados na íntegra, sem marco temporal, no idioma inglês e que tratassem da temática. O critério utilizado para inclusão das publicações era ter as expressões utilizadas nas buscas no título ou palavras-chave, ou ter explícito no resumo que o texto se relaciona à memorização e uso de senhas na população idosa. Os artigos excluídos não apresentavam o critério de inclusão estabelecido e/ou apresentavam duplicidade, ou seja, publicações recuperadas em mais de uma das bases de dados.

Foram selecionados 46 artigos de fontes confiáveis e reconhecidas. A análise dos documentos selecionados incluiu uma avaliação do conteúdo, focando nas metodologias utilizadas, resultados, e conclusões, assim como na interpretação crítica em relação ao objetivo desta revisão, conforme exemplificado na Figura 2.

Figura 2 – Revisão de Literatura.

Fonte: Autor.

4.4 Resultados e Discussão

O mundo digital, em sua constante e vertiginosa expansão, vem criando uma teia complexa de plataformas, aplicativos e serviços online. Com essa evolução, há uma exigência crescente para que seus usuários estejam sempre atualizados e preparados para interagir de maneira segura e eficaz. Uma das demandas mais marcantes dessa realidade é a necessidade de memorizar uma miríade de senhas, uma para cada serviço ou aplicativo utilizado.

Cada senha representa um ponto de acesso e, frequentemente, informações pessoais e valiosas. Assim, proteger essa chave torna-se imperativo. Infelizmente, a crescente quantidade de senhas pode tornar difícil a gestão e recordação das mesmas.

Por isso, a memorização não é apenas um mero requisito, mas uma habilidade essencial para aqueles que desejam navegar com segurança e confiança no vasto mundo digital. Ao mesmo tempo, esse desafio ilustra a importância de encontrarmos soluções mais práticas e intuitivas para a autenticação no futuro, principalmente para populações marginalizadas à era tecnológica.

Nesta revisão categorizamos os artigos de acordo com o tipo de estudo e após subcategorizamos de acordo com o tema central de cada um, como mostram as tabelas 4 e 5.

4.4.1 Estudo de Caso

Nesta seção apresentaremos os artigos de estudo de caso, que foram subdivididos de acordo com a temática central, sendo elas: Envelhecimento; Tecnologia da Saúde; Segurança Cibernética; Autenticação e Senhas.

4.4.1.1 Envelhecimento

O artigo "Narrowing the age-based digital divide: Developing digital capability through social activities" (Zhao et al., 2023) investiga como as atividades sociais podem ajudar a desenvolver as capacidades digitais dos adultos mais velhos. Os autores argumentam que a capacidade digital não é apenas uma habilidade técnica, mas também uma habilidade social, e que as atividades sociais podem proporcionar aos idosos oportunidades de aprender e praticar novas habilidades digitais em um ambiente de apoio. O estudo foi realizado com 33 participantes, incluindo pacientes chineses e seus familiares. Os autores entrevistaram os participantes sobre suas experiências com as tecnologias da informação e comunicação (TICs) e suas atividades sociais. A partir das entrevistas, os autores desenvolveram um modelo teórico para entender o processo pelo qual as atividades sociais podem moldar as capacidades digitais dos adultos mais velhos. O modelo sugere que as atividades sociais podem influenciar as capacidades digitais dos adultos mais velhos de duas maneiras principais:

1. Oportunidades de aprendizado: As atividades sociais podem proporcionar aos adultos mais velhos oportunidades de aprender sobre novas tecnologias e como usá-las. Por exemplo, um adulto mais velho pode aprender a usar um smartphone participando de um clube de informática para idosos ou conversando com um neto sobre as últimas tendências tecnológicas.

2. Motivação para aprender: As atividades sociais podem motivar os adultos mais velhos a aprender sobre novas tecnologias. Por exemplo, um adulto mais velho pode se sentir mais motivado a aprender a usar um computador se ele puder usar o computador para se comunicar com amigos e familiares que vivem longe.

O estudo também encontrou evidências de que o apoio social, através de familiares ou amigos, desempenha um papel importante no desenvolvimento das

capacidades digitais dos adultos mais velhos. Além disso, o artigo discute os benefícios potenciais das TICs para os idosos, como o acesso a informações de saúde, a possibilidade de monitoramento à distância e a melhoria na comunicação com os profissionais de saúde.

Esses benefícios das atividades sociais para os adultos mais velhos são ainda mais importantes quando se considera a relação entre isolamento social e solidão e a perda da função cognitiva. Um estudo de Cacioppo e Cacioppo (Cacioppo; Cacioppo, 2013), envolvendo um total de 8.688 voluntários, descobriu que o isolamento social e a solidão podem levar a uma perda da função cognitiva ao longo do tempo, destacando a importância da atenção da comunidade de saúde ao ambiente social desta população.

4.4.1.2 Tecnologia da Saúde

O artigo "Design Considerations for Patient Portal Adoption by Low-Income, Older Adults" de Latulipe et al. (Latulipe et al., 2015) investiga os fatores que influenciam a adoção de portais de pacientes por adultos mais velhos de baixa renda. Os autores realizaram uma entrevista com 36 pacientes e cuidadores de baixa renda com idades entre 50 e 80 anos para entender suas experiências com portais de pacientes. Os resultados do estudo revelaram que há uma série de barreiras à adoção de portais de pacientes, incluindo falta de acesso à tecnologia; habilidades digitais limitadas e condições socioeconômicas que limitam a disponibilidade de tempo ao uso de portais. Os autores então sugerem uma série de considerações de design para portais de pacientes que visam atender às necessidades desta população, que incluem: acessibilidade; simplicidade; relevância e apoio para configuração e uso.

Latulipe et al., em 2018, realizaram entrevistas com 10 pacientes com idades entre 65 e 92 anos para entender suas preocupações sobre o acesso de seus cuidadores às informações de saúde disponíveis nos portais de pacientes. Os resultados do estudo revelaram que os pacientes mais velhos têm uma série de preocupações sobre o uso de portais de pacientes por proxy por seus cuidadores, incluindo:

Privacidade: Os pacientes estão preocupados com a privacidade de suas

informações de saúde e com a possibilidade de seus cuidadores acessarem essas informações sem o seu consentimento.

Confiança: Os pacientes precisam confiar em seus cuidadores para usar as informações de saúde de forma responsável.

Competência: Os pacientes estão preocupados com a possibilidade de seus cuidadores não terem as habilidades necessárias para usar os portais de pacientes de forma eficaz.

4.4.1.3 Segurança Cibernética

O artigo "I'm Doing the Best I Can: Understanding Technology Literate Older Adults' Account Management Strategies"explora as abordagens de gerenciamento de contas adotadas por idosos proficientes em tecnologia, ou seja, que utilizavam regularmente dispositivos eletrônicos e tinham bom entendimento da tecnologia. O estudo, baseado em entrevistas com 20 participantes de 60 a 86 anos, revela que esses adultos utilizam diversas estratégias, incluindo o uso de senhas fortes e exclusivas, atualização regular de senhas, ativação da autenticação multifatorial, organização cuidadosa de contas e monitoramento constante para detectar atividades suspeitas. Apesar dessas estratégias, eles enfrentam desafios como dificuldade em lembrar senhas e falta de tempo para monitorar todas as contas regularmente (Abraham; Crabb; Radomirovic, 2021).

Já o trabalho de Grimes et al., publicado em 2010, comparou o conhecimento de segurança na internet entre adultos mais velhos e adultos mais jovens. Os resultados mostraram que os idosos têm um conhecimento menor sobre segurança na internet do que os adultos mais jovens. Isso ocorre porque os idosos têm menos conhecimento e experiência com computadores. Como resultado, os idosos estão em maior risco de sofrer problemas de segurança e privacidade online. O estudo também investigou o impacto do gênero, mas não encontrou diferenças significativas entre homens e mulheres (Grimes et al., 2010).

Quan-Haase e Ho, em 2020, reforçam essa discussão ao analisar as preocupações dos idosos em relação à privacidade online e as estratégias de proteção de privacidade entre os idosos em East York, Toronto, Canadá. A pesquisa foi

realizada através de entrevistas com 40 idosos acima de 65 anos e descobriu que a maioria deles está principalmente preocupada com questões de privacidade de segurança, seguidas por preocupações de privacidade institucional. As maiores preocupações incluíam o uso indevido de informações por desconhecidos e o acesso não autorizado às suas informações pessoais. Foi observado que, para alguns idosos, suas altas preocupações com a privacidade os impediam de aproveitar plenamente os benefícios potenciais da mídia digital1. Além disso, os idosos de East York variaram consideravelmente no uso de estratégias de proteção de privacidade; alguns idosos não usaram estratégias, enquanto outros estavam ansiosos para proteger sua privacidade usando todas as estratégias à sua disposição.

Seguindo o mesmo raciocínio, no trabalho de Frik et al., de 2019, também foram realizadas entrevistas com 46 idosos para identificar suas preocupações com segurança e privacidade. O estudo revelou que os idosos enfrentam dificuldades devido à opacidade dos fluxos de dados, dificuldades de compreensão das configurações de privacidade e segurança e tendem a confiar mais em fontes familiares ou amigos. O artigo apresenta várias recomendações para aliviar essas ameaças, incluindo o desenvolvimento de materiais de segurança e privacidade voltados especificamente para idosos (Frik et al., 2019).

4.4.1.4 Autenticação

Em 2020, Das et al. analisaram a experiência dos idosos com a autenticação de dois fatores (2FA) e como isso afeta sua segurança online. A pesquisa foi realizada através de um estudo qualitativo com dez idosos (60 anos ou mais) sobre o uso (ou não uso) sustentado de 2FA por trinta dias. Foi observado que a adoção e a usabilidade do 2FA continuam sendo um desafio. Os participantes adotaram pouco as chaves de segurança devido ao design não inclusivo das chaves, à falta de benefícios tangíveis, às instruções inconsistentes e às dependências do dispositivo. O estudo propõe assistência adequada, comunicação de riscos, mudanças no processo de registro e alinhamento de requisitos focados em segurança para incentivar a adoção de 2FA entre os idosos e as instituições confiadas com seus dados. O estudo também introduz o conceito de 'Cuidadores de Segurança', que podem garantir a segurança e a independência digital para a população idosa (Das et al., 2020).

4.4.1.5 Senhas

O padrão de comportamento humano muitas vezes inclina-se para soluções mais simples e facilmente memorizáveis, principalmente quando se trata de criar e lembrar senhas para diferentes plataformas. As dificuldades inerentes em memorizar múltiplas combinações complexas levam os usuários a reutilizar senhas ou a escolher sequências mais óbvias. No entanto, essa tendência pode entrar em conflito com a necessidade de manter a qualidade e a confidencialidade das senhas em sistemas de informação. Senhas robustas são importantes para garantir a proteção de dados e evitar acessos não autorizados, tornando essencial encontrar um equilíbrio entre a inclinação natural das pessoas para a simplicidade e a demanda por segurança na era digital.

O estudo de Šolić, Očevčić e Blažević, de 2015, apresenta resultados de uma pesquisa empírica sobre a autoavaliação da qualidade das senhas e várias questões de privacidade relacionadas à manipulação de senhas entre os usuários de sistemas de informação. Os dados foram coletados por meio de um questionário com 627 usuários de e-mail que eram adultos, de nacionalidade croata e usavam o sistema de e-mail regularmente. Os usuários foram agrupados em categorias considerando idade, gênero, conhecimento técnico, nível de educação e experiência de uso para realizar uma análise comparativa. Os resultados mostraram que a maioria dos usuários avalia a qualidade de suas senhas como média, enquanto 13,8% de todos os usuários classificaram sua senha como ruim. Em relação à manipulação de senhas, 53,4% de todos os usuários disseram que usam as mesmas senhas para a maioria dos sistemas de informação que usam. No total, 20,7% de todos os usuários às vezes emprestam sua senha e 17,1% deles a anotam para lembrar (Šolić; Očevčić; Blažević, 2015).

Em "Age and gender impact on password hygiene" há o interesse em analisar o impacto da idade e do gênero na força das senhas usando um grande conjunto de dados de senhas. Os pesquisadores recuperaram senhas previamente criptografadas de 102.120 usuários de um banco de dados de clientes vazado de uma empresa de compartilhamento de carros. Embora o tamanho do efeito medido fosse pequeno, os homens tinham senhas significativamente mais fortes do que as mulheres para todos os grupos etários. Os homens de 26 a 45 anos também eram significativamente

diferentes de todos os outros grupos, e a complexidade da senha diminuía com a idade para ambos os gêneros igualmente. No geral, foi observada uma higiene de senha muito fraca, 72% dos usuários basearam sua senha em uma palavra ou usaram uma sequência simples de dígitos, e as senhas de mais de 39% dos usuários foram encontradas em listas de palavras de vazamentos anteriores (Juozapavičius et al., 2022).

Do ponto de vista psicológico, a escolha de senhas reflete uma luta entre a necessidade de segurança e o desejo inerente de facilidade e conveniência. A partir desta perspectiva, Loos e Crosby (2018) analisaram a seleção de senhas para melhorar a interação humano-computador e discutiram como a escala interna e externa do locus de controle, bem como as associações de memória e fatores cognitivos podem afetar a escolha de senhas. A escala interna e externa de locus do controle é um questionário utilizado para avaliar a tendência de uma pessoa em acreditar que eventos em sua vida são controlados por fatores internos ou externos, amplamente utilizado na pesquisa psicológica. Uma pessoa com um locus de controle interno pode escolher senhas mais complexas e difíceis de adivinhar, enquanto uma pessoa com locus de controle externo tende a escolher senhas mais simples e fáceis de lembrar. Também notaram que uma pessoa pode escolher uma senha que seja facilmente lembrada por causa de uma associação com um evento importante em sua vida ou com uma palavra significativa. A pesquisa sugere que a capacidade de memória de curto prazo pode afetar a complexidade da senha escolhida, sendo que aqueles com pior capacidade de memória podem preferir senhas mais simples e fáceis. O artigo destaca que o gerenciamento de senhas é um processo problemático e que compreender como os usuários armazenam e recuperam informações na memória pode ajudar os designers de sistema a criar interfaces mais intuitivas e eficazes (Loos; Crosby, 2018).

O cérebro humano é orientado para reconhecer padrões e simplificar tarefas repetitivas, levando muitos a escolher senhas que tenham um significado pessoal ou que sigam padrões facilmente lembrados.

Luna, em 2019, também discutiu a psicologia do usuário, explorando como crenças metacognitivas podem influenciar a seleção de senhas. Seu estudo sugere que crenças equivocadas podem levar a escolha de senhas menos seguras, acreditando

que a facilidade de memorização está inversamente relacionada à segurança (Luna, 2019).

A memorabilidade é um aspecto crucial no design de sistemas de autenticação, pois senhas que são difíceis de lembrar podem levar os usuários a adotar práticas inseguras, como anotar senhas em post-its ou usar a mesma senha em várias contas.

Idealmente, uma senha deve ser tanto memorável quanto segura, embora encontrar o equilíbrio entre esses dois aspectos possa ser um desafio. A memorabilidade é frequentemente contrastada com a força da senha, que se refere à resistência de uma senha contra tentativas de adivinhação ou ataque.

No estudo de Woods e Siponen, de 2018, fica claro que a capacidade de recordar senhas não se relaciona diretamente com as habilidades de memória de um indivíduo. De forma alternativa, a percepção que cada pessoa tem acerca de suas habilidades de memória - sob a luz de sua capacidade de memorizar senhas, controle percebido sobre a própria memória, motivação para lembrar e entendimento de como sua memória funciona - esclarecem o porquê de muitos usuários não conseguirem se recordar de suas senhas. Além disso, o estudo aponta fatores relacionados à metacognição no contexto de senhas que preveem a correta recordação delas. Entre eles, incluem-se a facilidade em lembrar senhas, a confiança na recordação de senhas, e a percepção de que as senhas são importantes. A partir desses resultados, os autores sugerem estratégias práticas para aprimorar a memorização de senhas, como criar senhas mais facilmente memorizáveis e adotar métodos eficazes de recordação (Woods; Siponen, 2018).

Em sua tese de doutorado, Imran, em 2015, comparou o desempenho e as preferências de adultos e crianças ao usar esquemas de senha gráfica PassTiles. Surpreendentemente, as crianças se saíram melhor com o esquema Object PassTiles, enquanto não houve diferença significativa entre as idades para os outros dois esquemas de senha gráfica (Imran, 2015).

Já Mahesh et al., em 2018, vai além ao estudar os hábitos de senha de indivíduos com conhecimento em segurança de rede e computador. Descobriu que alguns hábitos comuns incluem o uso de senhas suficientemente longas, o uso de

caracteres em maiúsculas, números e caracteres especiais, a escolha completamente aleatória (sem palavras do dicionário ou informações pessoais identificáveis) e evitar armazenar senhas em locais fáceis de descobrir. Entretanto, mesmo que com conhecimento sobre os riscos associados à escolha de senhas fracas, muitos indivíduos ainda praticam hábitos inseguros, como o uso de senhas fracas e a reutilização de senhas em várias contas. A tese destaca que a falta de memória é um dos principais motivos pelos quais as pessoas adotam práticas inseguras e sugere que a conscientização sobre os riscos pode ajudar a incentivar práticas mais seguras (Mahesh et al., 2018).

Abbott, Calarco e Camp realizaram, em 2018, uma pesquisa através do estudo das políticas de senha de vinte e duas universidades dos Estados Unidos e da análise de 1,3 bilhão de endereços de e-mail e senhas obtidos das listas de combinação Exploit.in e Anti-Public com o objetivo de limitar a reutilização de senhas implementando políticas adaptativas que permitem a proteção contra roubo de dados em qualquer rede de instituição educacional, . Os pesquisadores analisaram a reutilização potencial das credenciais dos estudantes, funcionários, professores e outros usuários associados para cada um dos domínios das universidades e verificaram se elas atendiam aos requisitos específicos de cada política de senha. Concluiram que várias decisões de política adotadas por instituições educacionais podem diminuir a segurança relacionada às credenciais de conta. Assim, as políticas de senha atuais podem não ser suficientes para prevenir a reutilização de senhas, o que pode levar a violações de segurança (Abbott; Calarco; Camp, 2018).

O artigo “Did You Forget Your Password?” de Abbas Moallem, analisa o comportamento do usuário em relação à segurança ao visualizar uma aplicação web, a maneira como lidam com várias senhas e a recuperação da senha esquecida usando a pergunta de segurança. A pesquisa foi realizada através de um estudo quantitativo com 390 pessoas com diferentes níveis de experiência no uso de computadores. Os resultados mostram que a maioria das pessoas seria capaz de responder a uma variedade de perguntas de segurança para outras pessoas em seu entorno (Moallem, 2011).

A necessidade de gerenciar adequadamente as senhas também foi reforçada por um estudo realizado por Alshahrani e Alghamdi, em 2022, que investigou os

fatores que influenciam o uso real de gerenciadores de senhas. O estudo integra alguns fatores do Modelo de Aceitação de Tecnologia (percebido como facilidade de uso, utilidade percebida e atitude) com outros fatores da revisão de literatura (prontidão do usuário, conscientização e motivação). Os pesquisadores descobriram que a facilidade percebida de uso, a utilidade percebida e a prontidão do usuário têm um impacto positivo no uso dessas ferramentas (Alshahrani; Alghamdi, 2022).

A usabilidade desses gerenciadores de senhas também é fundamental para sua adoção. Um estudo forneceu insights úteis para desenvolvedores e designers, abordando desafios de usabilidade como desconfiança do usuário, complexidade da interface do usuário, dificuldade em lembrar senhas mestras, falta de feedback sobre a força das senhas e falta de suporte para dispositivos móveis. Para melhorar a usabilidade, o estudo sugeriu simplificação da interface do usuário, diminuição do número de etapas para realizar uma tarefa, melhoria da consistência visual, uso de assistentes de configuração, o uso de ícones claros e intuitivos e implementação de um sistema de feedback sobre a força das senhas (Carreira; Ferreira; Mendes, 2021).

Chung et al. (Chung et al., 2010) delineia os contrastes de usabilidade entre diferentes grupos etários e diferentes tipos de teclado, focando especificamente na entrada de números. Embora o teclado sensível ao toque tenha se mostrado popular entre os participantes do estudo, tanto jovens quanto idosos, foi o teclado físico que apresentou maior precisão de entrada, provavelmente devido ao feedback tátil. A idade também afetou o tempo de conclusão das tarefas, com os idosos necessitando de mais tempo, salientando a importância de considerar o design de teclado para otimizar a usabilidade para diferentes públicos, especialmente os mais idosos.

A dissertação de mestrado de Nedvěd, de 2021, apresenta uma contribuição significativa, iluminando a problemática do gerenciamento inadequado de senhas e suas implicações na segurança dos usuários. Esta pesquisa evidenciou que práticas como a similaridade entre nome de usuário e senha, bem como a reutilização de senhas, são exemplos de má gestão de senhas que podem comprometer a segurança dos usuários (Nedvěd, 2021).

Adicionalmente, foi investigada as considerações dos usuários idosos em

relação ao uso de gerenciadores de senhas, identificando as motivações e barreiras para a adoção desses sistemas. Curiosamente, a preocupação em admitir a capacidade diminuída de lembrar informações foi apontada pelos idosos como uma das barreiras para a adoção de gerenciadores de senhas (Ray et al., 2020).

O artigo "Biometrics: Password replacement for elderly?" investigou como a biometria pode ser usada como uma alternativa para senhas, especialmente para a população idosa. O estudo foi realizado com idosos de centros geriátricos e avaliou como eles atualmente gerenciam as várias senhas que criam para suas contas, como se sentem sobre seus métodos de gerenciamento atuais e métodos que eles sentem que podem melhorar sua experiência. A maioria dos idosos achava difícil usar teclados e preferia opções de digitalização biométrica. Mesmo que 83,33% dos idosos achassem os métodos tradicionais mais difíceis, apenas 61,11% preferiam a opção biométrica, demonstrando a resistência em adotar novas tecnologias. Entretanto, os pesquisadores concluíram que a biometria é a forma mais segura de autenticação até o momento, independentemente da idade (Ahmed et al., 2017).

Hämäläinen em sua pesquisa com 25 idosos entre 50 e 90 anos, avaliou suas opiniões sobre o uso da biometria para armazenar informações de usuário e senhas em comparação com métodos tradicionais. Embora a resposta geral tenha sido positiva, surgiram preocupações com a privacidade e a segurança dos dados biométricos. Apesar dessas preocupações, a pesquisa sugere que os idosos estão dispostos a adotar tecnologias mais avançadas, se apresentadas de maneira acessível e fácil de usar (Hämäläinen, 2015).

O estudo de Hämäläinen discute os mecanismos de autenticação em geral e, em seguida, examina a biometria e apresenta algumas aplicações. O processo de envelhecimento resulta em muitas mudanças físicas e cognitivas, algumas das quais podem precisar ser consideradas ao avaliar a usabilidade da biometria. Em sua pesquisa com 25 idosos entre 50 e 90 anos, avaliou suas opiniões sobre o uso da biometria para armazenar informações de usuário e senhas em comparação com métodos tradicionais. Embora a resposta geral tenha sido positiva, surgiram preocupações com a privacidade e a segurança dos dados biométricos. Apesar dessas preocupações, a pesquisa sugere que os idosos estão dispostos a adotar tecnologias mais avançadas, se apresentadas de maneira acessível e fácil de usar (Hämäläinen,

2015).

4.4.2 Experimento

Nesta seção apresentaremos os artigos de experimentos e eles se concentraram na temática de senhas.

4.4.2.1 Senhas

A segurança de senhas é uma área de grande relevância na autenticação online, com vários estudiosos, como Blanchard, propondo estruturas alternativas para aumentar a tolerância a erros de digitação e a segurança do hashing de senhas (Blanchard, 2022; Blanchard, 2020). Um dos métodos propostos envolve um algoritmo de programação dinâmica que calcula a distância de edição entre duas strings sem ter acesso direto a elas, permitindo a correção de erros comuns de digitação (Blanchard, 2019).

Além disso, outro estudo de Blanchard, Malaingre e Selker, de 2018, introduziu um método de matriz bidimensional para criar senhas memoráveis e seguras, mostrando que essa estratégia levou a senhas com alta entropia teórica, menos erros de memória e mais memorabilidade (Blanchard; Malaingre; Selker, 2018).

A usabilidade refere-se à medida em que um produto pode ser utilizado por usuários específicos para alcançar objetivos específicos com eficácia, eficiência e satisfação em um contexto de uso específico. Em outras palavras, é sobre o quão fácil e intuitivo um produto, seja ele um software, hardware ou qualquer outro tipo de interface, é para o usuário.

A usabilidade e a segurança das senhas como método de autenticação foram discutidas por Yan et al., em 2004, destacando práticas recomendadas para a criação de senhas fortes e a utilidade dos gerenciadores de senhas na geração e armazenamento seguro de senhas. Os autores realizaram um ensaio controlado para determinar como ajudar os usuários a escolher boas senhas, fornecendo diferentes tipos de conselhos. Os resultados do estudo desafiam a sabedoria estabelecida. Os usuários raramente escolhem senhas que são ao mesmo tempo difíceis de adivinhar e fáceis de lembrar. O estudo sugere que as senhas baseadas em frases mnemônicas são

tão difíceis de decifrar quanto as senhas aleatórias, mas tão fáceis de lembrar quanto as seleções de usuários ingênuos. Além disso, o estudo discute métodos alternativos de autenticação, como reconhecimento facial ou por voz, ou autenticação baseada em certificado (Yan et al., 2004).

Greene e Tamborello (Greene; Tamborello, 2015) apresentam um modelo cognitivo computacional de ensaio de senha e uma extensão de digitação para a arquitetura cognitiva ACT-R destinada a estudar questões de interação humano-computador no domínio de segurança utilizável, para melhorar a segurança e usabilidade de senhas, considerando como as pessoas criam, lembram e digitam suas senhas, permitindo o desenvolvimento de políticas de senha mais eficientes e sistemas de autenticação mais seguros, assim como Khan e Chefranov, em 2020, propõem um modelo inovador para fortalecer a segurança de senhas, em que aliam o conceito de reconhecimento com esquemas baseados em recuperação e recuperação com dicas para oferecer segurança superior em comparação com os esquemas existentes. Eles combinam Símbolos de Clique (CS) Alfabético em uma entidade: símbolos Alfanuméricos (A) e Visuais (V) (CS-AV) é um esquema de senha baseado em Captcha. Eles integram isso com pontos de grade baseados em recuperação n $\times$ n, onde um usuário pode desenhar a forma ou padrão pela interseção dos pontos de grade como uma maneira de inserir uma senha gráfica. O próximo esquema, a combinação de CS-AV com células de grade, permite um espaço de senha muito grande (2,4 $\times$ 10$\hat{4}$ bits de entropia) e fornece resultados de usabilidade razoáveis, determinando um estudo empírico do espaço de senha memorável. Estes trabalhos ressaltam a necessidade de equilibrar a usabilidade e a segurança, um tema que é consistentemente abordado em toda a literatura (Greene; Tamborello, 2015; Khan; Chefranov, 2020).

Al-Slais e El-Medany, em 2022, propõem um framework que cria políticas de senha sob medida para usuários com diferentes limiares cognitivos sem sacrificar a força e a entropia de senha. O framework inclui testes PassPAST, que consiste numa série de cinco testes breves para medir a força inicial da senha, o limiar de lembrança da senha e o limiar de escrita da senha; uma escala de carga cognitiva para perfilar o usuário, a Cognitive Burden Scale (CBS) que classifica o usuário em crítico, típico ou especialista; e um gerador de senha PassGEN, que gera

senhas fortes com alta entropia utilizando a CBS e os resultados dos testes de PassPAST. A metodologia inclui uma série de testes para avaliar a força e a lembrança da senha, classificando o usuário em categorias que vão desde crítico até especialista. Os resultados preliminares indicaram que o framework gera senhas fortes para todos os níveis de usuários, sendo as senhas mnemônicas potencialmente as mais favoráveis. Ainda, o artigo discute a importância de políticas de senhas adaptativas centradas no usuário na luta contra a fadiga de senhas e na melhoria da cibersegurança (Al-Slais; El-Medany, 2022).

O estudo "The influence of password restrictions and mnemonics on the memory for passwords of older adults" investiga a influência das restrições de senhas e das técnicas mnemônicas na memória das senhas entre adultos mais velhos. Para isso, foram utilizadas variáveis dentro de um design misto, com variações entre e dentro dos sujeitos do estudo. Um programa Java foi utilizado em um laptop para conduzir o experimento com os participantes, que foi realizado em duas sessões com uma semana de intervalo entre elas. Na primeira sessão, os participantes receberam instruções sobre a técnica de geração de senhas que estariam utilizando e foram orientados a gerar senhas que se adequassem aos critérios estabelecidos. O programa registrou as senhas geradas e o tempo necessário para os participantes se lembrarem de suas senhas após 10 minutos e 1 semana. O experimento ocorreu em uma sala tranquila e bem iluminada, onde cada participante foi testado individualmente. No total, 18 participantes mais velhos foram aleatoriamente designados para o grupo de mnemônicos baseados em imagens e 19 para o grupo de mnemônicos baseados em texto. Para o grupo de adultos mais jovens, 20 participantes foram designados aleatoriamente para o grupo de mnemônicos baseados em imagens e 20 para o grupo de mnemônicos baseados em texto. Os resultados indicaram que não houve diferença significativa na segurança das senhas geradas pelos adultos mais velhos em comparação com os mais jovens. Além disso, não foi encontrada diferença significativa na segurança das senhas geradas pelas técnicas mnemônicas baseadas em imagens e em texto. O software Cain and Abel (Montoro; Babcock, 2014) não conseguiu decifrar nenhuma das senhas geradas pelos participantes, indicando que as senhas foram consideradas seguras. Contudo, o estudo apontou que o programa Java utilizado pode ter sido confuso para alguns dos participantes mais velhos, e que

um programa com uma interface mais gráfica poderia ter otimizado o desempenho deles (Vu; Hills, 2013).

Nesse contexto, é relevante destacar que um estudo envolvendo 20 idosos, com idades entre 60 e 75 anos, investigou a eficácia das senhas gráficas utilizando o Passface. Os resultados indicaram um desempenho superior dos participantes ao lidar com imagens faciais particionadas em comparação com imagens faciais completas. Vale ressaltar que ambas as formas de apresentação de imagem mostraram eficácia na prevenção do "shoulder-surfing", uma técnica de engenharia social que envolve a obtenção de informações, como números de identificação pessoal (PINs), senhas e outros dados confidenciais, observando o que alguém está fazendo olhando por cima do ombro da pessoa (Jittibumrungrak; Hongwarittorrn, 2019).

4.4.3 Revisão de Literatura

Nesta seção apresentaremos os artigos de revisão de literatura, que exploraram os temas de Envelhecimento; Tecnologia da Saúde; Acessibilidade; Segurança Cibernética e Senhas.

4.4.3.1 Envelhecimento

O artigo “The Role of Information and Communication Technology (ICT) for Older Adults’ Decision-Making Related to Health, and Health and Social Care Services in Daily Life—A Scoping Review” de Susanna Nordin et al. (Nordin et al., 2021), explora o papel da Tecnologia da Informação e Comunicação (TIC) na tomada de decisões de adultos mais velhos em relação à saúde e aos serviços de saúde e assistência social. Os autores realizaram uma revisão sistemática de artigos publicados entre 2010 e 2020, identificando 12 artigos que atendiam aos seus critérios de inclusão. Os resultados da revisão foram divididos em três categorias:

1. Forma e função da TIC para a tomada de decisão: a TIC pode ser usada para apoiar a tomada de decisão de adultos mais velhos de várias maneiras, através do fornecimento de acesso a informações sobre saúde e serviços de saúde e sociais; facilitando a comunicação com profissionais de saúde e familiares e oferecendo suporte para a autogestão da saúde.

2. Valor percebido e efeito da TIC para a tomada de decisão: a TIC é geralmente percebida pelos adultos mais velhos como uma ferramenta valiosa para a tomada de decisão relacionada à saúde. No entanto, eles observam que os efeitos na tomada de decisão ainda precisam ser mais investigados.

3. Fatores que influenciam o uso da TIC para a tomada de decisão: identificaram vários fatores que influenciam o uso da TIC para a tomada de decisão, incluindo: Acesso a dispositivos e serviços de TIC; habilidades digitais; apoio social e motivação para usar a TIC.

Considerando a alfabetização digital como um aspecto crucial para o uso efetivo da tecnologia, o artigo "Measurement of Digital Literacy Among Older Adults: Systematic Review" concluiu que é necessário desenvolver intervenções específicas para melhorar a alfabetização digital entre os adultos mais velhos e reduzir as desigualdades na sociedade. O objetivo do estudo foi identificar as medidas utilizadas para avaliar a alfabetização digital e examinar as diferenças nos níveis entre adultos mais velhos com base em fatores como idade, gênero e nível de educação. Os resultados mostraram que a alfabetização digital é um fator importante para o bem-estar dos adultos mais velhos e que existem diferenças significativas nos níveis de alfabetização com base em fatores socioeconômicos (Oh et al., 2020).

4.4.3.2 Tecnologia da saúde

Wilson et al. (2021) conduziram uma revisão abrangente dos obstáculos e facilitadores para o uso de serviços de saúde eletrônicos (e-health) por adultos mais velhos. A revisão seguiu as diretrizes do PRISMA-ScR e utilizou uma metodologia de revisão de escopo para mapear a amplitude da literatura disponível sobre o tema, fornecer uma visão geral dos conceitos associados e identificar lacunas na literatura. A escolha por uma revisão de escopo, em vez de uma revisão sistemática, foi motivada pela escassez de literatura que explora as barreiras e facilitadores para o uso de e-health por adultos mais velhos. Os dados foram extraídos de 14 estudos de acordo com critérios específicos, como design do estudo, foco do estudo, descrição da população, tipo de tecnologia, serviços ou intervenções, e barreiras e facilitadores de acesso. Os resultados da revisão foram sintetizados em cinco

categorias temáticas: 1. características do usuário; 2. características da tecnologia; 3. características do contexto; 4. características do provedor; 5. características do sistema.

A revisão revelou que os adultos mais velhos são mais propensos a usar serviços de e-health que são sensíveis às suas necessidades físicas e funcionais, fornecem educação e treinamento adequados para o engajamento com a tecnologia, abordam experiências negativas anteriores e conceitos errôneos sobre tecnologias de saúde digital e empregam estratégias para melhorar a confiabilidade e a credibilidade percebida do e-health. Além disso, a participação ativa dos adultos mais velhos no design e entrega de programas de e health pode ser benéfica, e estratégias para melhorar a autoeficácia e abordar preocupações com a privacidade devem ser implementadas (Wilson et al., 2021).

4.4.3.3 Acessibilidade

O estudo de Andrew et al., em 2020, trouxe uma perspectiva inclusiva ao abordar a autenticação para pessoas com deficiência. Na seção de pesquisa sobre autenticação de pessoas com deficiência visual observaram que leitores de tela e lupa são muito utilizados por estes usuários, o que os faz ficar vulneráveis a ataques de espionagem e observadores; o método de escaneamento de impressão digital é o mais acessível e que PIN e escaneamento de íris são os menos acessíveis. Identificaram também novos métodos como senhas em braile, interfaces cérebro-computador e autenticação baseada em gestos, assim como interação tátil e áudio. A revisão teve dificuldade em encontrar artigos que relataram métodos de autenticação para usuários com deficiência auditiva, mas enfatizaram que esta população tem dificuldades em inserir pressionamentos de teclas dados por orientação auditiva. Já com usuários com deficiência cognitiva, que envolve dificuldade para lembrar, raciocinar, pensar e prestar atenção, foi visto que é possível conceber soluções tecnológicas como gerenciadores de senhas e senhas musicais para apoiar e diminuir a carga cognitiva de lembrar senhas nesta população. Na população com deficiência motora alguns progressos foram feitos, como a autenticação baseada em fala e toque e deslocamento inteligentes. O estudo, portanto, encontrou uma série de técnicas diferenciadas, como senhas em braille, interfaces cérebro-computador e autenticação

baseada em gestos para pessoas com deficiência visual, além de gerenciadores de senhas e senhas musicais para pessoas com deficiências cognitivas (Andrew et al., 2020).

4.4.3.4 Segurança cibernética

O artigo "User, Usage and Usability: Redefining Human Centric Cyber Security" explora a crescente complexidade da segurança cibernética com uma perspectiva mais ampla, definindo usuário, uso e usabilidade (3U's) como três componentes essenciais para consideração de segurança cibernética. O estudo classifica os esforços de desenvolvimento por meio de trabalhos de pesquisa existentes com base no design de segurança centrado no humano, implementação e implantação desses componentes. O foco está em estudos que especificamente ilustram a mudança de paradigma da segurança cibernética centrada em funcional e uso, para a segurança cibernética centrada no usuário, considerando os aspectos humanos dos usuários. O objetivo desta pesquisa é fornecer aos usuários e projetistas de sistemas insights sobre o funcionamento e as aplicações da segurança cibernética centrada no humano. O estudo argumenta que, apesar de muitos avanços na concepção e implementação de sistemas de segurança cibernética, os fatores humanos muitas vezes ainda levam ao seu fracasso completo (Grobler; Gaire; Nepal, 2021).

A população idosa também é particularmente vulnerável, especialmente em relação aos crimes cibernéticos financeiros. Burton et al., em 2021, identificaram vários fatores que contribuem para a vulnerabilidade dessa população, incluindo declínio cognitivo, isolamento social, falta de familiaridade com a tecnologia, percepção de maior riqueza e uma predisposição para confiar em autoridades. A fim de reduzir esses riscos, o estudo sugere estratégias como educação e conscientização, apoio social, melhor acessibilidade tecnológica para os idosos, e a criação de senhas seguras e implementação de autenticação de dois fatores (Burton et al., 2021).

4.4.3.5 Senhas

A memorabilidade de senhas é mais explorada no artigo de Lennartsson, que conduziu uma revisão sistemática da literatura para identificar até que ponto diferentes estratégias de criação de senhas facilitam a geração de senhas memoráveis.

Vários termos de pesquisa foram usados para sondar quatro bancos de dados científicos em busca de artigos revisados por pares que satisfizessem critérios de seleção distintos. No final, 61 artigos aceitos passaram por uma análise de dados qualitativa por meio da teoria fundamentada. A análise mostrou que diferentes estratégias de composição resultaram em diferenças substanciais na memorabilidade. As senhas que infundiam um significado mais profundo para o usuário eram consideradas fáceis de lembrar, enquanto a falta de infusão de significado dificultava a recordação. No geral, as senhas geradas pelo usuário mostraram ser mais memoráveis do que as geradas pelo sistema. Contudo, ele também destaca a necessidade de equilibrar a memorabilidade e a segurança, pois senhas fáceis de lembrar podem ser mais vulneráveis a ataques (Lennartsson, 2019).

Considerando a importância da usabilidade, segurança e confiança em gerenciadores de senhas, Chaudhary et al., em 2019,tinham como objetivo identificar os principais desafios enfrentados pelos usuários ao utilizar essas ferramentas e propor melhorias para aprimorar sua usabilidade e segurança. Os autores realizaram uma revisão sistemática da literatura, selecionando trinta e dois artigos com resultados coerentes associados à usabilidade e segurança. Os desafios encontrados pelos usuários ao utilizar gerenciadores de senhas podem incluir problemas de usabilidade, como dificuldade na criação e gerenciamento de senhas complexas, problemas de integração com diferentes dispositivos e plataformas, e questões de segurança, como vulnerabilidades na proteção de dados e riscos de violação de privacidade. A partir desses resultados, eles deduziram e apresentaram sugestões significativas para a realização de um gerenciador de senhas utilizável, seguro e confiável (Chaudhary et al., 2019).

Em linha com esses achados, a obra de Simmons et al., de 2021, investigou a usabilidade e design dos gerenciadores de senhas, identificando oportunidades para melhorar esses sistemas e potencializar as pesquisas na área. A partir de uma minuciosa análise, constatou-se que grande parte dos casos de uso não haviam sido anteriormente contemplados em estudos de usabilidade. Adicionalmente, constatou-se uma ausência de pesquisas que comparassem os paradigmas de design ou as abordagens de implementação, deixando em aberto as vantagens e desvantagens dos designs existentes e suas melhores práticas de implementação. Apoiando-se nesta

revisão sistemática, testes de usabilidade foram realizados em oito gerenciadores de senhas, cobrindo os principais e recomendados casos de uso. Dentre as observações feitas, notaram-se dificuldades significativas ao digitar credenciais quando o preenchimento automático não estava disponível, designs de interfaces que causavam confusão e problemas ao vincular credenciais a múltiplos sites (Simmons et al., 2021).

Em uma investigação sobre a intersecção entre idade, educação e memória, o estudo conduzido por Pilar et al., em 2012, descortinou os desafios enfrentados pelos idosos no mundo digital. A pesquisa revelou que a era digital pode não ser tão amigável para todos. Foram entrevistados um total de 263 participantes, com idades variando de 18 a 93 anos, e nível de educação variando do ensino fundamental ao ensino superior. Os resultados sugeriram que o número de usos de senha foi o fator mais influente no desempenho da memória. Ou seja, à medida que o número de circunstâncias em que os indivíduos utilizavam senhas aumentava, a incidência de senhas esquecidas e misturadas também aumentava. Enquanto jovens adultos e aqueles com um nível educacional mais elevado apresentaram um desempenho melhor em lembrar e utilizar senhas, os idosos e indivíduos com menos escolaridade se encontravam em um labirinto de esquecimentos. Estes insights não apenas destacam a complexidade da mente humana, mas também ressaltam a necessidade de soluções mais intuitivas e inclusivas no cenário tecnológico atual (Pilar et al., 2012).

4.5 Conclusão

Em conclusão, esta revisão destaca a importância de considerar a perspectiva do usuário, especialmente dos usuários mais velhos, ao projetar e implementar tecnologias de saúde digital. As barreiras para o uso da tecnologia podem ser superadas através de estratégias eficazes de treinamento e suporte, bem como através de melhorias na usabilidade e segurança da tecnologia.

Além disso, é importante que se crie um ambiente seguro e de confiança para que os usuários se sintam confortáveis ao utilizar essas tecnologias. Finalmente, a participação ativa dos usuários na fase de design pode garantir que as tecnologias

sejam adequadas às suas necessidades e capacidades.

Essa abordagem centrada no usuário pode ser um fator-chave para a adoção bem-sucedida e a utilização eficaz das tecnologias de saúde digital.

Tabela 4 – Tabela de categorização da revisão de artigos

Referência	**Ano**	**Tipo de Estudo**	**Tema central da pesquisa**
Abbot et. al (Abbott; Calarco; Camp, 2018)	2018	Estudo de caso	Senhas
Solic et. al (Šolić; Očevčić; Blažević, 2015)	2015	Estudo de caso	Senhas
Juozapavicius et. al (Juozapavičius et al., 2022)	2022	Estudo de caso	Senhas
Loos et. al (Loos; Crosby, 2018)	2018	Estudo de caso	Senhas
Luna K. (Luna, 2019)	2019	Estudo de caso	Senhas
Woods et. al (Woods; Siponen, 2018).	2018	Estudo de caso	Senhas
Imran A. (Imran, 2015)	2015	Estudo de caso	Senhas
Mahesh et. al (Mahesh et al., 2018)	2018	Estudo de caso	Senhas
Moallem A. (Moallem, 2011)	2011	Estudo de caso	Senhas
Alshahrani et. al (Alshahrani; Alghamdi, 2022)	2022	Estudo de caso	Senhas
Chung et. al (Chung et al., 2010)	2010	Estudo de caso	Senhas
Nedved V. (Nedvěd, 2021)	2021	Estudo de caso	Senhas
Carreira et. al (Carreira; Ferreira; Mendes, 2021)	2021	Estudo de caso	Senhas
Ray et. al (Ray et al., 2020)	2020	Estudo de caso	Senhas
Ahmed et. al (Ahmed et al., 2017)	2017	Estudo de caso	Senhas
Hamalainen N. (Hämäläinen, 2015)	2015	Estudo de caso	Senhas
Latulipe et. al (Latulipe et al., 2015)	2015	Estudo de caso	Tecnologia da saúde
Latulipe et. al (Latulipe et al., 2018)	2018	Estudo de caso	Tecnologia da saúde
Das et. al (Das et al., 2020)	2020	Estudo de caso	Autenticação
Frik et. al (Frik et al., 2019)	2019	Estudo de caso	Segurança cibernética
Grimes et. al (Grimes et al., 2010)	2010	Estudo de caso	Segurança cibernética
Abraham et. al (Abraham; Crabb; Radomirovic, 2021)	2021	Estudo de caso	Segurança cibernética

Tabela 5 – Continuação da Tabela 4

Referência	**Ano**	**Tipo de Estudo**	**Tema central da pesquisa**
Quan-Haase et. al (Quan-Haase; Ho, 2020)	2020	Estudo de caso	Segurança cibernética
Cacioppo et. al (Cacioppo; Cacioppo, 2013)	2013	Estudo de caso	Envelhecimento
Zhao et. al (Zhao et al., 2023)	2023	Estudo de caso	Envelhecimento
Blanchard E. (Blanchard, 2022)	2022	Experimento	Senhas
Blanchard E. (Blanchard, 2020)	2020	Experimento	Senhas
Blanchard N K. (Blanchard, 2019)	2019	Experimento	Senhas
Blachard et. al (Blanchard; Malaingre; Selker, 2018)	2018	Experimento	Senhas
Yan et. al (Yan et al., 2004)	2004	Experimento	Senhas
Al-Slais et. al (Al-Slais; El-Medany, 2022)	2022	Experimento	Senhas
Jittibumrungrak et. al (Jittibumrungrak; Hongwarittorrn, 2019)	2019	Experimento	Senhas
Vu et. al (Vu; Hills, 2013)	2013	Experimento	Senhas
Greene et. al (Greene; Tamborello, 2015)	2015	Experimento	Senhas
Khan et. al (Khan; Chefranov, 2020)	2020	Experimento	Senhas
Burton et. al (Burton et al., 2021)	2021	Revisão de literatura	Segurança cibernética
Grobler et. al (Grobler; Gaire; Nepal, 2021)	2021	Revisão de literatura	Segurança cibernética
Andrew et. al (Andrew et al., 2020)	2020	Revisão de literatura	Acessibilidade
Nordin et. al (Nordin et al., 2021)	2021	Revisão de literatura	Envelhecimento
Oh et. al (Oh et al., 2020)	2020	Revisão de literatura	Envelhecimento
Wilson et. al (Wilson et al., 2021)	2021	Revisão de literatura	Tecnologia da saúde
Lennartsson M. (Lennartsson, 2019)	2019	Revisão de literatura	Senhas
Chaudhary et. al (Chaudhary et al., 2019)	2019	Revisão de literatura	Senhas
Simmons et. al (Simmons et al., 2021)	2021	Revisão de literatura	Senhas
Pilar et. al (Pilar et al., 2012)	2012	Revisão de literatura	Senhas

5 Experimento

O estudo foi conduzido em colaboração com o grupo Mente Ativa, do SESC SC, localizado no bairro Estreito - Florianópolis (Sesc, 2023). O grupo reúne idosos de 60 a 80 anos semanalmente às terças-feiras, após aprovação do Comitê de Ética em Pesquisa com Seres Humanos - UFSC, CAAE: 69431423.3.0000.0121, conforme Anexo **??**.

5.1 Método

5.1.1 Recrutamento dos Participantes

Os participantes do estudo foram recrutados entre os membros do grupo Mente Ativa, do SESC- SC. Foi feito um convite aos idosos presentes nas reuniões semanais, após aprovação do CEPSH-UFSC, explicando os objetivos da pesquisa e solicitando voluntários interessados em participar. A coleta de dados ocorreu durante uma reunião regular do grupo, nos dias 27/06/2023 e 15/08/2023, a fim de minimizar o impacto na rotina dos participantes.

5.1.2 Local das Atividades

As atividades do estudo foram realizadas nas dependências do SESC-SC, onde ocorrem as reuniões do grupo Mente Ativa. Foi reservado um espaço adequado, com privacidade e conforto, para a aplicação dos questionários e tarefas relacionadas à pesquisa.

5.1.3 Descrição das Atividades do Estudo

A pesquisa, estruturada no formato não-supervisionado, englobou 9 questões. Estas questões, predominantemente de respostas simples e de múltiplas escolhas, foram projetadas para serem claras e diretas, minimizando possíveis dúvidas por parte dos participantes. Essa abordagem não-supervisionada oferece a liberdade

para o usuário preencher o questionário sem a necessidade de um monitoramento contínuo.

Os participantes receberam um questionário básico que abordou a frequência do uso de senhas em diferentes contextos e os métodos que utilizam para memorizá-las. O questionário foi aplicado individualmente, em um ambiente tranquilo, durante a reunião do grupo Mente Ativa.

Cada participante foi solicitado a escolher uma senha de 3 itens a partir de um card com vários objetos e outra senha de 3 itens a partir de um card com várias palavras. Eles tiveram um tempo máximo de 5 minutos para cada escolha. Essa tarefa foi realizada de forma individual, em um ambiente propício à concentração.

Após a conclusão da tarefa de memorização de senhas, foi oferecido um intervalo de 40 minutos para os participantes. Durante esse período, eles realizaram as atividades recreativas já corriqueiras pelo grupo ou descansar. Essas atividades foram importantes para minimizar a fadiga mental e proporcionar um momento de descontração aos participantes.

Após o intervalo, os participantes foram solicitados a escrever as senhas que escolheram anteriormente. A pontuação foi baseada no número de itens corretos presentes em cada senha. Essa avaliação foi realizada de forma individual, garantindo a privacidade e a concentração necessárias para a tarefa.

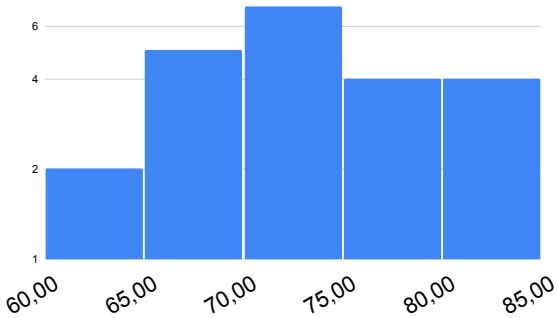
5.1.4 Critérios de Inclusão e Exclusão

O critérios de inclusão foram idosos com idade entre 60 e 90 anos e que concordaram em participar da pesquisa. Foram excluídos do experimento os idosos que utilizavam a assistência de terceiros para a escolha de senhas e idosos que não concordaram em participar da pesquisa.

5.2 Resultados

Foram entrevistados ao total 22 idosos para o questionário, sendo 20 do sexo feminino e 2 do sexo masculino. A faixa etária variou entre 61 anos até 83 anos, conforme mostra a Figura 3.

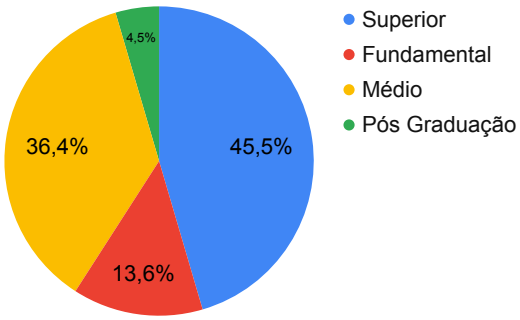
Figura 3 – Faixa Etária.



Fonte: Autor.

Quando perguntados sobre o nível educacional, 3 participantes fizeram até o ensino fundamental, 8 até o ensino médio, 10 respoderam ter feito até ensino superior e 1 fez até pós graduação. A Figura 4 mostra o nível educacional dos entrevistados.

Figura 4 – Nível Educacional.

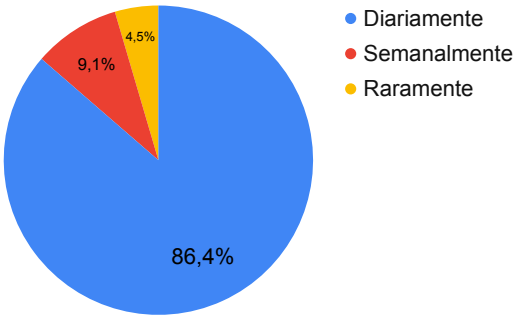


Fonte: Autor.

Sobre a frequência no uso de senhas, 19 responderam que utilizam senhas diariamente, 2 semanalmente e apenas 1 afirmou que utiliza senhas raramente. A Figura 5 mostra que a maioria dos entrevistados usa, todos os dias, senhas para se autenticar em serviços eletrônicos.

Sobre a forma que utilizam para escolher suas senhas, 11 idosos responderam que escolhem senhas com base em informações pessoais, 7 com base em palavras aleatórias, 2 com base em palavras comuns como "senha", "123456"e 2 afirmaram utilizar outras formas de escolha mas não especificaram. A Figura 6 mostra que

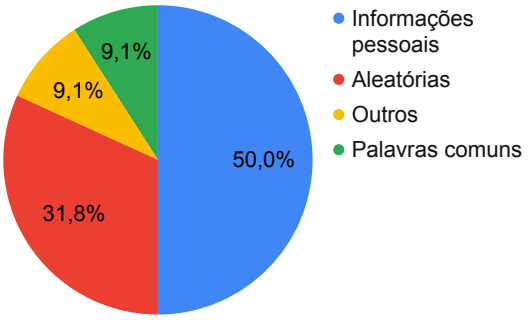
Figura 5 – Frequência de Uso de Senhas.



Fonte: Autor.

quase 50% dos entrevistados utiliza informações de cunho pessoal ou palavras comuns como senha.

Figura 6 – Forma de Escolha de Senhas.

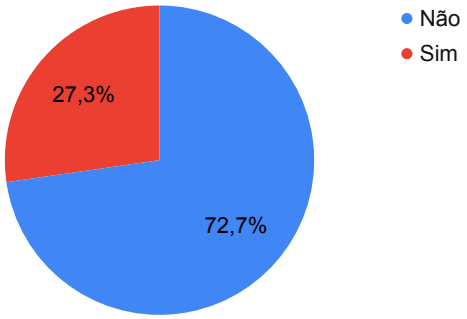


Fonte: Autor.

Conforme ilustra a Figura 7, quando questionados sobre a dificuldade em memorizar senhas, a maioria (72,7% - 16 idosos) afirmou não possuir dificuldade e apenas 6 participantes (27,3%) afirmaram possuir dificuldade em memorizá-las.

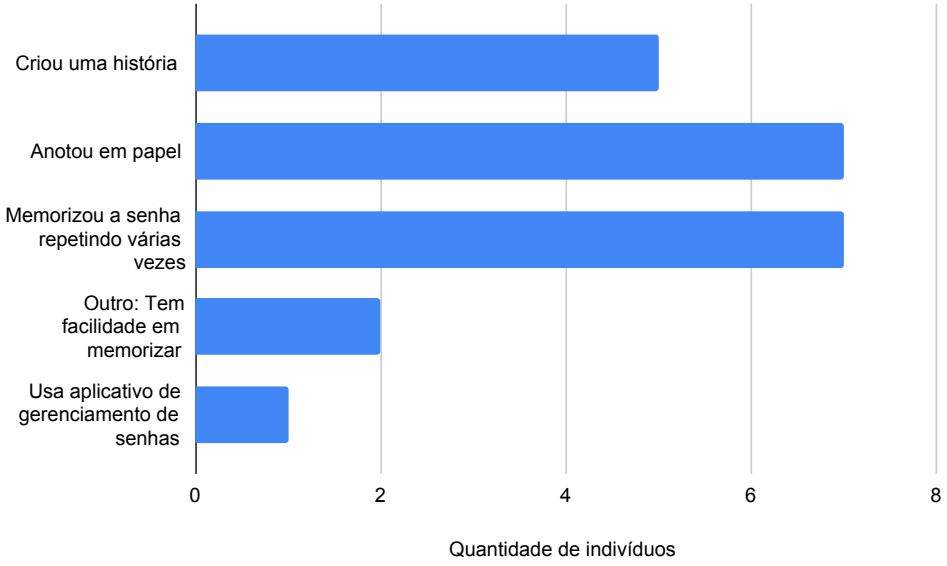
Ao falarem sobre suas estratégias para a memorização de senhas, 7 idosos afirmaram anotá-las em um papel, 7 idosos memorizam a senha repetindo-a diversas vezes, 5 idosos criam história para facilitar a memorização, 2 idosos disseram ter facilidade em memorizar e apenas 1 idoso faz uso de gerenciadores de senhas. A Figura 8 ilustra as estratégias adotadas pelos entrevistados para memorizar as senhas.

Figura 7 – Dificuldade de Memorizar.



Fonte: Autor.

Figura 8 – Estratégias na memorização de senhas.



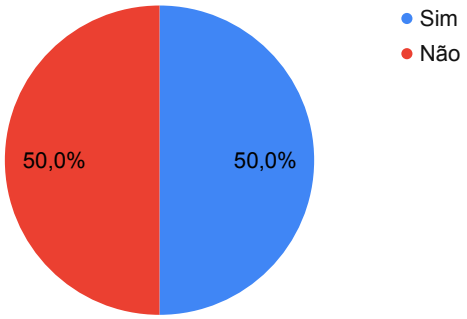
Fonte: Autor.

Conforme ilustra a Figura 9, quando questionados se já haviam tido problemas na memorização de senhas, 50% dos participantes afirmaram que sim e 50% afirmaram que não.

Na questão livre, sobre como fizeram para resolver o problema na memorização de senhas, tivemos as seguintes respostas:

- 6 idosos optaram por trocar a senha;

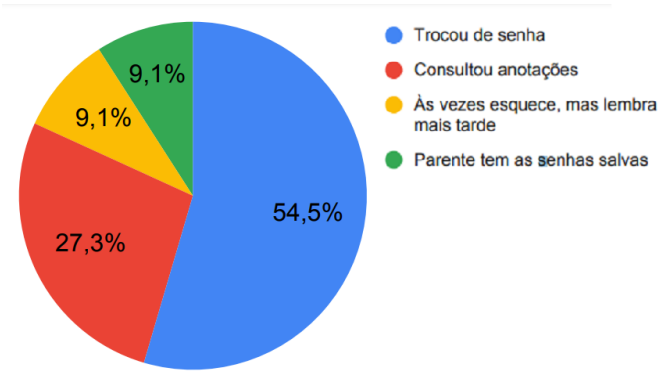
Figura 9 – Problemas com Memorização das Senhas.



Fonte: Autor.

- 3 idosos consultaram anotações em papel;
- 1 idoso afirmou que se lembrou da senha num período mais tarde;
- 1 idoso afirmou que tinha um parente que sabia sua senha.

Figura 10 – Recuperação de Senhas.



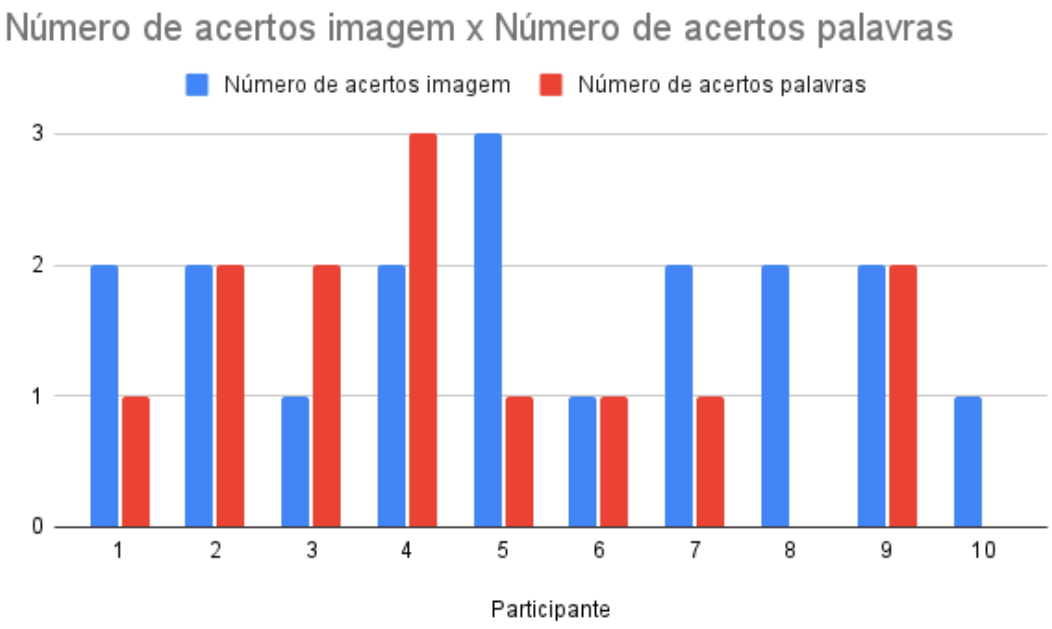
Fonte: Autor.

A Figura 10 ilustra o percentual dos métodos que os entrevistados usavam para recuperação de suas senhas.

Apenas 10 participantes aceitaram participar da coleta de senhas baseadas em imagens ou senhas baseadas em palavras, sendo 100% do sexo feminino. Todas as participantes acertaram pelo menos uma imagem, duas participantes não se

recordaram de nenhuma palavra. Nenhuma participante se recordou de todas as imagens e todas as palavras. Nenhuma participante não se recordou de nenhuma imagem, conforme mostra a Figura 11

Figura 11 – Número de acertos imagens x Número de acertos palavras.



Fonte: Autor.

5.3 Discussão

A análise das respostas oferecidas pelos 22 idosos que participaram deste estudo permite um aprofundamento nas questões relativas à memorização de senhas entre esse grupo etário. Os dados fornecidos nos oferecem uma visão clara das escolhas, desafios e estratégias desses indivíduos, permitindo uma discussão relevante.

5.3.1 Características Demográficas e Educacionais

Primeiramente, é essencial reconhecer o desequilíbrio de gênero dos entrevistados, com uma predominância marcante de mulheres (90,9%). Essa disparidade

poderia ter uma influência nas respostas, especialmente se houvesse diferenças significativas de comportamento entre os sexos.

A faixa etária variada entre 61 e 83 anos sugere uma representação diversificada do grupo idoso, desde aqueles em início de envelhecimento até aqueles mais avançados em idade. O nível educacional também se mostrou variado, com uma representação ligeiramente superior daqueles que completaram o ensino superior (45,5%). Essa variação educacional poderia ser um fator influenciador na escolha e memorização de senhas.

5.3.2 Uso e Escolha de Senhas

Um fato interessante é que uma vasta maioria dos idosos entrevistados usa senhas diariamente (86,4%). Isso desmistifica a ideia de que os idosos não são usuários ativos de tecnologias que exigem senhas.

A escolha da senha com base em informações pessoais, utilizada por 50% dos entrevistados, é uma prática comum, mas potencialmente arriscada. Senhas derivadas de informações pessoais são mais fáceis de serem adivinhadas ou descobertas, especialmente em um mundo onde muitos detalhes de nossas vidas estão disponíveis online.

5.3.3 Dificuldade e Estratégias de Memorização

Mesmo entre o grupo idoso, 72,7% afirmaram não ter dificuldade em memorizar senhas, embora 50% dos participantes já tiveram problemas em memorizá-las. Isso sugere que reconhecer as vulnerabilidades em pesquisa ainda é essencial, pois há uma complexidade inerente na forma como os idosos percebem e lidam com suas habilidades cognitivas, que pode não ser diretamente refletida nas respostas imediatas que eles fornecem.

As estratégias usadas para memorização são variadas, com destaque para anotações em papel e repetição. Ambas as práticas mostram um viés mais tradicional de aprendizado. Entretanto, vale ressaltar que o uso de gerenciadores de senhas, uma solução tecnológica e moderna, foi mencionado por apenas 1 idoso.

5.3.4 Problemas com Senhas

O fato de que 50% dos participantes já tiveram problemas com memorização em algum momento não é surpreendente e é algo que poderia ser observado em outros grupos etários também. As soluções adotadas, como trocar a senha ou consultar anotações, mostram práticas comuns e práticas um tanto arriscadas, como depender de parentes para lembrar a senha.

5.3.5 Análise dos Dados de Senhas Baseadas em Imagens e Palavras

A inclusão de um experimento sobre a memorização de senhas baseadas em imagens versus senhas baseadas em palavras adiciona uma nova dimensão à nossa discussão. Considerando que apenas 10 participantes aceitaram participar dessa fase do estudo, e todos sendo do sexo feminino, temos uma amostra seletiva, o que pode afetar a generalização dos resultados.

Realizar pesquisa de memorização com idosos apresenta desafios específicos que vão além dos aspectos cognitivos. A capacidade de memória tende a declinar com a idade, tornando mais difícil para alguns idosos lembrar-se de informações ou processar novos dados rapidamente. Essa dificuldade pode, em muitos casos, levar ao nervosismo e à frustração. O idoso, ao perceber suas limitações durante as sessões de pesquisa, pode se sentir inseguro ou envergonhado. Essas emoções negativas, por sua vez, podem criar uma barreira adicional à capacidade de retenção e recuperação de informações.

5.3.6 Preferência por Imagens

Os resultados indicam uma tendência clara de que as participantes se lembraram pelo menos de uma imagem, enquanto duas delas não se recordaram de nenhuma palavra. Esta observação corrobora a teoria de que imagens podem ser mais fáceis de recordar do que palavras, especialmente no grupo idoso. Estudos anteriores já sugeriam que o cérebro humano tem uma capacidade notável de reconhecimento visual, o que pode explicar a facilidade observada em lembrar imagens.

5.3.7 Performance Variada

A variação na capacidade de memorização, tanto para imagens quanto para palavras, é notável entre as participantes. Enquanto algumas participantes tiveram uma performance equilibrada entre os dois tipos de senhas, outras tiveram dificuldades notáveis, especialmente com senhas baseadas em palavras. Esta variação sugere que não há uma "abordagem única" para todos os idosos, e as capacidades cognitivas podem variar amplamente dentro deste grupo.

Nenhuma participante foi capaz de se lembrar de todas as imagens e palavras, indicando que, independentemente do método, há um limite na capacidade de memorização. Isto é uma lembrança importante de que, enquanto as soluções de senhas baseadas em imagens podem ser mais eficazes em determinados cenários, elas ainda não são infalíveis.

5.3.8 Implicações

A tendência observada na maior facilidade de lembrar senhas baseadas em imagens sugere que sistemas de autenticação baseados em imagens poderiam ser uma alternativa viável para idosos, pelo menos para aquelas que têm dificuldade em memorizar senhas baseadas em palavras. Além disso, poderia ser útil considerar treinamentos ou sistemas de apoio que combinem ambos os métodos, oferecendo uma abordagem multimodal para a memorização.

5.3.9 Limitações

Este estudo apresenta algumas limitações que devem ser levadas em consideração ao interpretar os resultados. Em primeiro lugar, a pesquisa foi realizada com um grupo pequeno de idosos, o que pode limitar a generalização dos resultados para a população idosa em geral. Além disso, o grupo de idosos não era homogêneo, talvez fosse mais apropriado subdividir o grupo em faixas etárias para uma análise mais precisa.

Foi observado que alguns participantes ficaram nervosos com a tarefa de memorização, o que pode ter afetado seu desempenho e, consequentemente, os

resultados do estudo. A pressão ou a ansiedade podem ter interferido na capacidade dos participantes de memorizar as senhas.

Além disso, algumas respostas dos participantes são questionáveis, pois suspeitamos que eles podem não ter querido demonstrar dificuldades em memorizar as senhas. Isso pode indicar um viés de resposta socialmente desejável, onde os participantes podem ter alterado suas respostas para evitar parecerem frágeis ou incapazes.

Essas limitações destacam a necessidade de estudos futuros com amostras maiores e estratégias para minimizar a ansiedade dos participantes e o viés de resposta. Além disso, pode ser útil explorar métodos alternativos de avaliação da memória que sejam menos dependentes do auto-relato dos participantes. Também seria interessante considerar a subdivisão dos participantes em faixas etárias para uma análise mais detalhada.

5.4 Conclusão

Este experimento reforça a ideia de que a memorização de senhas é uma questão multifacetada para os idosos, com vários fatores em jogo, incluindo o tipo de senha e as habilidades cognitivas individuais. Ao desenvolver sistemas de autenticação ou ao fornecer treinamento sobre segurança digital para idosos, essas nuances devem ser cuidadosamente consideradas para garantir uma experiência de usuário eficaz e segura.

A acessibilidade deve ser considerada uma terceira dimensão essencial do domínio do design de segurança cibernética, além da segurança técnica e da usabilidade. É primordial que se assegure a segurança mesmo com os esforços de aprimoramento da usabilidade e da acessibilidade (Renaud; Coles-Kemp, 2022).

No universo da segurança cibernética, frequentemente imaginamos um usuário padrão: ágil, totalmente equipado e com plena capacidade cognitiva para navegar por intrincados sistemas de segurança. Contudo, essa visão muitas vezes obscurece uma realidade: uma parcela significativa de indivíduos, que busca seu espaço no cenário digital, encontra-se à margem, enfrentando desafios e buscando

inclusão em um mundo cada vez mais conectado.

6 Autenticação das Pessoas Idosas

À medida que a digitalização permeia cada vez mais todos os aspectos da sociedade, a demanda por soluções de segurança personalizadas se torna cada vez mais urgente. Uma dessas necessidades emergentes é o desenvolvimento de sistemas de autenticação que levem em consideração os processos de envelhecimento, que podem diferir significativamente dos sistemas projetados para a população mais jovem.

A população idosa enfrenta desafios únicos na autenticação digital. Isso inclui dificuldades em lembrar senhas e outros fatores de conhecimento, desafios no uso de dispositivos e tecnologias digitais, e uma maior vulnerabilidade a ataques cibernéticos. Esses desafios foram observados em vários estudos e pesquisas anteriores, como visto da revisão sistemática desta dissertação.

Portanto, é crucial que as soluções de autenticação sejam projetadas com esses desafios em mente, oferecendo métodos de autenticação que sejam acessíveis e fáceis de usar para a população idosa, ao mesmo tempo que mantêm um alto nível de segurança para proteger contra ameaças cibernéticas.

6.1 Fatores de Autenticação

Os fatores de autenticação são categorizados em três tipos principais: o que você sabe, o que você tem e o que você é. "O que você sabe" refere-se a informações que o usuário conhece, como senhas ou PINs. "O que você tem" refere-se a algo que o usuário possui, como um cartão de identificação ou um *token* de segurança. "O que você é" refere-se a características biológicas do usuário, como impressões digitais ou padrões de íris (Velásquez; Caro; Rodríguez, 2018).

A população idosa pode enfrentar desafios significativos ao usar fatores de autenticação de posse e conhecimento. O uso de dispositivos físicos ou *tokens* para autenticação pode ser difícil para alguns idosos, especialmente aqueles com limitações físicas ou falta de familiaridade com a tecnologia. Da mesma forma, os

fatores de autenticação baseados em conhecimento, como senhas ou PINs, podem ser difíceis de lembrar para aqueles com dificuldades de memória. No entanto, um tipo de fator de conhecimento que tem se mostrado promissor para a população idosa é a autenticação baseada em imagens. As imagens são muitas vezes mais fáceis de lembrar do que palavras ou números, e podem ser uma forma eficaz de autenticação para aqueles que lutam para lembrar senhas tradicionais (Jittibumrungrak; Hongwarittorrn, 2019).

O experimento realizado neste estudo revelou uma tendência notável entre os idosos do grupo: a maioria conseguiu se lembrar de pelo menos uma imagem, enquanto duas pessoas não conseguiram se lembrar de nenhuma palavra. Essa observação reforça a teoria de que as imagens podem ser mais fáceis de recordar do que as palavras, especialmente para o grupo de idosos. Pesquisas anteriores já indicavam que o cérebro humano possui uma capacidade notável de reconhecimento visual, o que pode explicar a facilidade observada em lembrar imagens.

6.1.1 Senhas Baseadas em Imagens

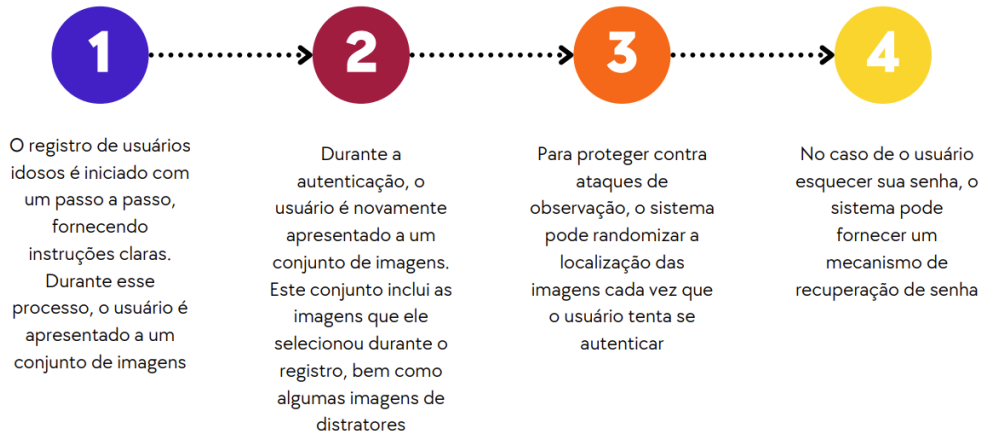
As senhas baseadas em imagens são uma alternativa promissora para as senhas baseadas em texto, especialmente para a população idosa. Estudos mostraram que as pessoas, especialmente os idosos, tendem a lembrar imagens melhor do que palavras ou números. Portanto, usar imagens como senhas pode facilitar a memorização e, consequentemente, a autenticação. Além disso, as senhas baseadas em imagens podem ser mais resistentes a ataques comuns, como ataques de força bruta ou de dicionário (Komanduri; Hutchings, 2008).

Os estudos oferecem percepções valiosas sobre a memorabilidade de imagens para idosos. Tomaszczyk e Fernandes (Tomaszczyk; Fernandes, 2013) observaram que os idosos tendem a selecionar imagens positivas como memoráveis e esse viés está sob controle cognitivo. Charles, Mather e Carstensen (Charles; Mather; Carstensen, 2003) também constataram que os idosos têm uma memória diminuída para imagens negativas em comparação com imagens positivas e neutras. Palladino e Beni (Palladino; Beni, 2003) descobriram que os idosos geram um maior número de imagens mentais gerais e autorreferidas, mas um menor número de imagens específicas. O pré-treinamento de imagens melhorou a lembrança do nome do rosto

em idosos, conforme observou Yesavage (Yesavage, 1983).

Com base no exposto até agora, propomos um *framework* de um sistema de autenticação com senha baseada em imagens, conforme mostra a Figura 12:

Figura 12 – Etapas do modelo proposto



Fonte: Autor.

1. Registro do Usuário: O registro de usuários idosos é iniciado com um passo a passo, fornecendo instruções claras. Durante esse processo, o usuário é apresentado a um conjunto de imagens. Este conjunto pode ser personalizado para o usuário, com base em seus interesses e preferências, para facilitar a memorização. O usuário seleciona uma sequência específica de imagens para formar sua "senha". Esta sequência é então armazenada no sistema para futura autenticação. É importante que o sistema armazene a sequência de imagens de forma segura, possivelmente usando técnicas de hash ou criptografia.

2. Autenticação: Durante a autenticação, o usuário é novamente apresentado a um conjunto de imagens. Este conjunto inclui as imagens que ele selecionou durante o registro, bem como algumas imagens de distratores. As imagens de distratores são imagens que o usuário não selecionou durante o registro e servem para aumentar a segurança do sistema. O usuário deve selecionar as imagens na sequência correta para ser autenticado.

3. Proteção contra ataques de observação (shoulder surfing): Para proteger contra ataques de observação, o sistema pode randomizar a localização das

imagens cada vez que o usuário tenta se autenticar. Isso significa que um atacante que observa o usuário selecionar as imagens não será capaz de replicar a sequência correta, pois a localização das imagens muda a cada tentativa.

4. Recuperação de Senha: No caso de o usuário esquecer sua senha, o sistema pode fornecer um mecanismo de recuperação de senha. Este mecanismo pode ser baseado em perguntas de segurança, onde o usuário deve responder a algumas perguntas que ele selecionou durante o registro. Alternativamente, o sistema pode enviar um link de redefinição de senha para o e-mail do usuário.

6.1.2 Biometria Senil

A biometria é outra forma eficaz de autenticação que pode ser particularmente útil para a população idosa. A biometria se refere à medição de características físicas ou comportamentais únicas, como impressões digitais, reconhecimento facial ou de voz. Esses métodos de autenticação são fáceis de usar e não requerem que o usuário lembre de qualquer informação, tornando-os ideais para a população idosa.

A Biometria Senil vai além do simples reconhecimento de características físicas. Ela é uma abordagem integral que considera a totalidade da experiência de envelhecimento. Por exemplo, com a idade, a pele passa por várias transformações, tornando-se mais fina, perdendo elasticidade e apresentando manchas e outras variações. Essas mudanças, embora naturais, podem afetar a capacidade dos sistemas biométricos tradicionais de ler com precisão as impressões digitais (Bonte et al., 2019).

Além disso, a coordenação motora fina pode ser comprometida à medida que envelhecemos, afetando a capacidade de realizar tarefas delicadas, como posicionar um dedo exatamente sobre um sensor (Curreri et al., 2018).

Outra proposta da dissertação é a Biometria Senil, que poderia ser estruturado da seguinte maneira:

1. Adaptação às Alterações Cutâneas: Os sistemas biométricos devem ser projetados para reconhecer e se adaptar às mudanças na pele que ocorrem com o envelhecimento. Isso pode envolver o uso de sensores mais sensíveis ou algoritmos de processamento de imagem mais avançados que podem levar em consideração a

textura, a elasticidade e as variações de cor da pele.

2. Tolerância à Motricidade Fina: Os sistemas biométricos devem ser tolerantes a pequenos desvios de posicionamento que podem ocorrer devido à diminuição da coordenação motora fina. Isso pode envolver o uso de sensores maiores, a implementação de algoritmos de correção de erro ou a inclusão de feedback ao usuário para ajudar no posicionamento correto.

3. Incorporação de Outras Características Biológicas: Os sistemas biométricos devem ser capazes de incorporar outras características biológicas que podem ser afetadas pelo envelhecimento, como a visão e a audição. Isso pode envolver o uso de reconhecimento de voz adaptado para tonalidades de voz mais frágeis ou sistemas de reconhecimento facial que levam em consideração características como catarata ou degeneração macular.

4. Facilidade de Uso: Os sistemas biométricos devem ser fáceis de usar para a população idosa. Isso pode envolver a simplificação do processo de autenticação, a inclusão de instruções claras e a implementação de interfaces de usuário intuitivas.

5. Segurança: Apesar das adaptações para acomodar a população idosa, os sistemas biométricos devem manter um alto nível de segurança para proteger contra ameaças cibernéticas. Isso pode envolver o uso de criptografia, a implementação de medidas de segurança física e a realização de auditorias de segurança regulares.

6.2 Nível de Garantia de Autenticação

À medida que a população mundial envelhece, torna-se cada vez mais importante adaptar nossos sistemas de segurança para atender às necessidades únicas desse grupo demográfico. Os idosos podem enfrentar desafios únicos ao interagir com a tecnologia, incluindo alterações físicas e cognitivas associadas ao envelhecimento. Portanto, é crucial que revisitemos e ajustemos os níveis de garantia em nossos sistemas de segurança para garantir que eles sejam acessíveis e eficazes para a população idosa. Isso pode envolver a implementação de novas tecnologias, como a biometria senil, e a adaptação de nossos processos de autenticação para

serem mais inclusivos e compreensíveis para os usuários idosos. Diante desse contexto, propõe-se a modificação nos Níveis de Garantia de Autenticação, no âmbito do NIST, do eIDAS e do Gov.br.

6.2.1 NIST

AAL1 (Nível de Garantia de Autenticação 1): Este nível permite a autenticação de um único fator, como uma senha memorizada ou um dispositivo físico. Para a população idosa, poderíamos considerar o uso de autenticação biométrica, como reconhecimento facial ou de voz, que pode ser mais fácil de usar do que senhas tradicionais.

AAL2 (Nível de Garantia de Autenticação 2): Este nível requer o uso de dois fatores de autenticação. Para a população idosa, poderíamos considerar a combinação de uma senha baseada em imagem e um fator biométrico, como o reconhecimento facial. Isso poderia proporcionar um nível mais alto de segurança sem a necessidade de lembrar senhas complexas.

AAL3 (Nível de Garantia de Autenticação 3): Este é o nível mais alto de segurança e normalmente requer autenticação de vários fatores. Para a população idosa, poderíamos considerar a combinação de vários fatores biométricos, como reconhecimento facial e de voz, juntamente com uma senha baseada em imagem. Isso proporcionaria o mais alto nível de segurança, enquanto ainda seria fácil de usar para a população idosa.

A tabela 6 sintetiza as modificações propostas:

6.2.2 eIDAS

Baixo: Este nível permite a autenticação de um único fator, como uma senha memorizada ou um dispositivo físico, como um token. Para a população idosa, poderíamos considerar o uso de autenticação biométrica, como reconhecimento facial ou de voz, que pode ser mais fácil de usar do que senhas tradicionais.

Substancial: Este nível requer o uso de dois fatores de autenticação. Para a população idosa, poderíamos considerar a combinação de uma senha baseada

Tabela 6 – NIST - modelo atual x modelo proposto

Nível de Garantia	**Modelo Atual do NIST**	**Proposta para a População Idosa**
AAL1	Um fator de autenticação (senha ou dispositivo físico).	Autenticação biométrica (facial ou voz)
AAL2	Dois fatores de autenticação.	Senha baseada em imagem + um fator biométrico, como o reconhecimento facial.
AAL3	Prova de possessão de chave criptográfica.	Combinação de vários fatores biométricos (reconhecimento facial e de voz) + uma senha baseada em imagem.

em imagem e um fator biométrico, como o reconhecimento facial. Isso poderia proporcionar um nível mais alto de segurança sem a necessidade de lembrar senhas complexas.

Alto: Este é o nível mais alto de segurança e normalmente requer autenticação de vários fatores. Para a população idosa, poderíamos considerar a combinação de vários fatores biométricos, como reconhecimento facial e de voz, juntamente com uma senha baseada em imagem. Isso proporcionaria o mais alto nível de segurança, enquanto ainda seria fácil de usar para a população idosa.

A tabela 7 sintetiza as modificações propostas:

6.2.3 Gov.br

Nível de Garantia Bronze: Este nível permite a autenticação de um único fator, como uma senha memorizada ou um dispositivo físico, como um token. Para a população idosa, poderíamos considerar o uso de autenticação biométrica, como reconhecimento facial ou de voz, que pode ser mais fácil de usar do que senhas tradicionais.

Nível de Garantia Prata: Este nível requer o uso de dois fatores de autenticação. Para a população idosa, poderíamos considerar a combinação de um dispositivo físico, como um token, e um fator biométrico, como o reconhecimento facial. Isso poderia proporcionar um nível mais alto de segurança sem a necessidade

Tabela 7 – eIDAS - modelo atual x modelo proposto

Nível de Garantia	**Modelo Atual do eIDAS**	**Proposta para a População Idosa**
Baixo	Autenticação de um único fator, como uma senha memorizada ou um dispositivo físico.	Autenticação biométrica (reconhecimento facial ou de voz).
Substancial	Dois fatores de autenticação.	Senha baseada em imagem + um fator biométrico, como o reconhecimento facial.
Alto	Pelo menos duas categorias diferentes de fatores de autenticação.	Combinação de vários fatores biométricos (reconhecimento facial e de voz) + uma senha baseada em imagem.

de lembrar senhas complexas.

Nível de Garantia Ouro: Este é o nível mais alto de segurança e normalmente requer autenticação de vários fatores. Para a população idosa, poderíamos considerar a combinação de vários fatores biométricos, como reconhecimento facial e de voz, juntamente com um dispositivo físico, como um token. Isso proporcionaria o mais alto nível de segurança, enquanto ainda seria fácil de usar para a população idosa.

A tabela 8 sintetiza as modificações propostas:

6.2.4 Limitações

A implementação de qualquer proposta, particularmente aquelas voltadas para públicos específicos como a população idosa, inevitavelmente encontra desafios e limitações. No contexto das adaptações propostas nos Níveis de Garantia para atender às necessidades desse grupo demográfico, algumas limitações merecem atenção.

Primeiramente, a aceitação e adoção dessas mudanças podem depender significativamente da familiaridade e aceitação dos usuários idosos com as tecnologias digitais, que podem ter diferentes níveis de experiência e conforto.

Tabela 8 – Gov.br - modelo atual x modelo proposto

Nível de Garantia	**Modelo Atual do Gov.br**	**Proposta para a População Idosa**
Bronze	Autenticação de um único fator, como senha memorizada ou dispositivo físico (token).	Autenticação biométrica (reconhecimento facial ou de voz).
Prata	Dois fatores de autenticação.	Senha baseada em imagem + um fator biométrico, como o reconhecimento facial.
Ouro	Geralmente exigindo autenticação de vários fatores.	Combinação de vários fatores biométricos (reconhecimento facial e de voz) + uma senha baseada em imagem.

Além disso, a efetiva implementação dessas propostas pode ser influenciada por questões de custo e infraestrutura. A integração de tecnologias biométricas, por exemplo, pode exigir investimentos substanciais em hardware e software, o que pode ser um obstáculo em ambientes com recursos limitados.

Outra limitação potencial é a rápida evolução da tecnologia. À medida que novas soluções e padrões emergem, a proposta inicial pode precisar ser revisada e atualizada para acompanhar as mudanças no cenário tecnológico. Além disso, a segurança é uma preocupação constante, e a implementação de tecnologias inovadoras deve ser cuidadosamente avaliada para garantir que não comprometa a integridade do sistema.

Em última análise, o reconhecimento e a abordagem dessas limitações são cruciais para a eficácia de qualquer iniciativa de adaptação. A colaboração entre especialistas em tecnologia, designers de interface e representantes da população idosa pode ser fundamental para superar esses desafios e desenvolver soluções que sejam não apenas seguras, mas também intuitivas e acessíveis para todos os usuários.

6.2.5 Contribuições

Nosso trabalho trouxe contribuições significativas relacionadas à memorização de senhas e à autenticação de pessoas idosas nos sistemas informatizados. São elas:

1. Revisão sistemática da literatura sobre memorização de senhas por pessoas idosas;

2. Experimento com um grupo de idosos sobre memorização e comparação de senhas baseadas em caracteres e senhas baseadas em imagens;

3. Proposta de modificação dos níveis de garantia de autenticação para pessoas idosas e;

4. Introduzir o conceito de Biometria Senil.

7 Considerações Finais

Estamos vivendo em uma era onde as linhas entre o virtual e o real estão se tornando cada vez mais indistintas. A digitalização, como um trem em alta velocidade, está revolucionando nossas vidas, remodelando a forma como trabalhamos, nos relacionamos e até mesmo como sonhamos. No entanto, será que esse trem está preparado para acomodar todos os passageiros? À medida que avançamos para um futuro cada vez mais digital, é crucial refletir sobre quem estamos incluindo nessa jornada e quem pode estar sendo inadvertidamente deixado para trás.

Neste cenário em rápida evolução, a segurança cibernética se tornou uma prioridade incontestável. De registros médicos a transações bancárias, quase todos os aspectos de nossa existência têm uma contrapartida digital que precisa ser protegida. Assim, os sistemas de autenticação salvaguardam nossas informações e identidades. No entanto, muitas vezes, no ímpeto de fortalecer esses sistemas contra ameaças, esquecemos de torná-los acessíveis a todos os usuários.

Inclusão e segurança, dois conceitos aparentemente em oposição, devem, na realidade, ser vistos como complementares. Um sistema verdadeiramente inclusivo não deixa ninguém para trás, enquanto um sistema seguro protege todos os seus usuários. Mas, como garantir que esses dois ideais coexistam harmoniosamente?

Primeiramente, é fundamental reconhecer que os usuários digitais não são um grupo homogêneo. Cada indivíduo, seja um adolescente hiperconectado ou um idoso tentando enviar seu primeiro e-mail, tem suas próprias habilidades, desafios e necessidades. E aqui entra um componente muitas vezes negligenciado no design de sistemas digitais: a empatia.

Empatia é a capacidade de se colocar no lugar do outro, de entender e sentir suas experiências. Ao desenvolver sistemas de autenticação, essa empatia significa considerar como diferentes pessoas interagem com a tecnologia. Para alguns, lembrar uma senha complexa pode ser fácil. Para outros, especialmente aqueles que enfrentam desafios cognitivos, como os idosos, pode ser uma tarefa hercúlea.

Ao nos movermos em direção ao futuro digital, é importante equilibrar tanto a inclusão quanto a segurança. Ambas devem ser consideradas simultaneamente, orientadas por uma abordagem que seja ao mesmo tempo empática e inovadora. Isso garantirá que todos, independentemente da idade, experiência, habilidade ou nível socioeconômico, possam se beneficiar e participar plenamente da era digital.

Referências

ABBOTT, J.; CALARCO, D.; CAMP, L. J. Factors influencing password reuse: A case study. In: *TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy*. [S.l.: s.n.], 2018.

ABOZAID, A.; HAGGAG, A.; KASBAN, H.; ELTOKHY, M. Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. *Multimedia tools and applications*, Springer, v. 78, p. 16345–16361, 2019.

ABRAHAM, M.; CRABB, M.; RADOMIROVIC, S. "I'm doing the best I can.- understanding technology literate older adults' account management strategies. In: SPRINGER VERLAG. *11th International Workshop on Socio-Technical Aspects in Security and Trust*. 2021. p. 86–107. Disponível em: <https://api.semanticscholar.org/CorpusID:251137745>.

AHMED, E.; DELUCA, B.; HIROWSKI, E.; MAGEE, C.; TANG, I.; COPPOLA, J. Biometrics: Password replacement for elderly? 2017 ieee long island systems. In: *Applications and Technology Conference, LISAT*. [S.l.: s.n.], 2017. v. 10.

AL-SLAIS, Y.; EL-MEDANY, W. M. User-centric adaptive password policies to combat password fatigue. *Int. Arab J. Inf. Technol.*, v. 19, p. 55–62, 2022. Disponível em: <https://api.semanticscholar.org/CorpusID:245508555>.

Allen Institute. *Semantic Scholar*. 2023. Disponível em: <https://www.semanticscholar.org/>.

ALQAHTANI, A. A. S.; EL-AWADI, Z.; MIN, M. A survey on user authentication factors. In: *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. [S.l.: s.n.], 2021. p. 0323–0328.

ALSHAHRANI, H.; ALGHAMDI, A. A. The factors influencing the use of password managers. *Journal of Information Security and Cybercrimes Research*, 2022. Disponível em: <https://api.semanticscholar.org/CorpusID:250197963>.

ALVES, J. E. D. Envelhecimento populacional no Brasil e no mundo. *Revista Longeviver*, São Paulo, 2019.

ALVES, L. V. Análise dos aspectos de segurança aplicada à internet das coisas e usabilidade do usuário. In: MARTINS, E. R. (Ed.). *Tecnolologia da Informação e Comunicação: Pesquisas em Inovações Tecnológicas*. São Paulo: Editora Científica Digital, 2021. cap. 2, p. 24–41.

ANDREW, S.; WATSON, S.; OH, T. H.; TIGWELL, G. W. A review of literature on accessibility and authentication techniques. *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, 2020. Disponível em: <https://api.semanticscholar.org/CorpusID:225962989>.

ARROYO, J. C. T.; DUMDUMAYA, C. E.; DELIMA, A. J. P. Polybius square in cryptography: a brief review of literature. *International Journal*, v. 9, n. 3, 2020.

BLANCHARD, E. Making more extensive and efficient typo-tolerant password checkers. In: IEEE. *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. [S.l.], 2020. p. 1581–1588.

BLANCHARD, E. Client-side hashing for efficient typo-tolerant password checkers. *International Journal of Systems and Software Security and Protection (IJSSSP)*, IGI Global, v. 13, n. 1, p. 1–24, 2022.

BLANCHARD, N. K. Secure and efficient password typo tolerance. In: *ACM Conference*. [S.l.: s.n.], 2019. p. 1–14.

BLANCHARD, N. K.; MALAINGRE, C.; SELKER, T. Improving security and usability of passphrases with guided word choice. In: *Proceedings of the 34th Annual Computer Security Applications Conference*. [S.l.: s.n.], 2018. p. 723–732.

BONTE, F. J.; GIRARD, D.; ARCHAMBAULT, J. C.; DESMOULIÈRE, A. Skin changes during ageing. *Sub-cellular biochemistry*, v. 91, p. 249–280, 2019. Disponível em: <https://api.semanticscholar.org/CorpusID:83463205>.

BONTEN, T. N.; RAUWERDINK, A.; WYATT, J. C.; KASTELEYN, M. J.; WITKAMP, L.; RIPER, H.; GEMERT-PIJNEN, L. J. van; CRESSWELL, K.; SHEIKH, A.; SCHIJVEN, M. P. et al. Online guide for electronic health evaluation approaches: systematic scoping review and concept mapping study. *Journal of medical Internet research*, JMIR Publications Toronto, Canada, v. 22, n. 8, p. e17774, 2020.

BRASIL. lei, *Estatuto do Idoso*. Congresso Nacional, 2003. Art. 3º. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.741.htm>.

BRASIL, G. F. do. *Níveis da conta gov.br*. 2023. Disponível em: <https://www.gov.br/governodigital/pt-br/conta-gov-br/niveis-da-conta-govbr>.

BURTON, A.; COOPER, C.; DAR, A.; MATHEWS, L.; TRIPATHI, K. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, v. 159, 2021. Disponível em: <https://api.semanticscholar.org/CorpusID:243228988>.

CACIOPPO, J. T.; CACIOPPO, S. Older adults reporting social isolation or loneliness show poorer cognitive function 4 years later. *Evidence-Based Nursing*, v. 17, p. 59 – 60, 2013. Disponível em: <https://api.semanticscholar.org/CorpusID:38497953>.

CARREIRA, C.; FERREIRA, J. F.; MENDES, A. Towards improving the usability of password managers. In: . [s.n.], 2021. Disponível em: <https://api.semanticscholar.org/CorpusID:250102811>.

CHARLES, S. T.; MATHER, M.; CARSTENSEN, L. L. Aging and emotional memory: the forgettable nature of negative images for older adults. *Journal of experimental psychology. General*, v. 132 2, p. 310–24, 2003. Disponível em: <https://api.semanticscholar.org/CorpusID:72143>.

CHAUDHARY, S.; SCHAFEITEL-TÄHTINEN, T.; HELENIUS, M.; BERKI, E. Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, Elsevier, v. 33, p. 69–90, 2019.

CHUNG, M. K.; KIM, D.; NA, S.; LEE, D. Usability evaluation of numeric entry tasks on keypad type and age. *International Journal of Industrial Ergonomics*, Elsevier, v. 40, n. 1, p. 97–105, 2010.

COMMISSION, F. T. *Creating Strong Passwords and Other Ways To Protect Your Accounts*. 2023. Disponível em: <https://consumer.ftc.gov/articles/creating-strong-passwords-and-other-ways-protect-your-accounts>.

CONTI, V.; MILITELLO, C.; VITABILE, S. Biometric authentication overview: a fingerprint recognition sensor description. *International Journal of Biosensors Bioelectronics*, v. 2, n. 1, p. 26–31, 2017.

CORBATÓ, F. J.; MERWIN-DAGGETT, M.; DALEY, R. C. An experimental time-sharing system. In: *Proceedings of the May 1-3, 1962, spring joint computer conference*. São Francisco: ACM, 1962. p. 335–344.

CURRERI, C.; TREVISAN, C.; CARRER, P.; FACCHINI, S.; GIANTIN, V.; MAGGI, S.; NOALE, M.; RUI, M. D.; PERISSINOTTO, E.; ZAMBON, S.; CREPALDI, G.; MANZATO, E.; SERGI, G. Difficulties with fine motor skills and cognitive impairment in an elderly population: The progetto veneto anziani. *Journal of the American Geriatrics Society*, v. 66, 2018. Disponível em: <https://api.semanticscholar.org/CorpusID:46820149>.

DAS, S.; JELEN, B.; KIM, A.; HUBER, L. L.; CAMP, L. J. Non-inclusive online security: Older adults' experience with two-factor authentication. *Other Information Systems & eBusiness eJournal*, 2020. Disponível em: <https://api.semanticscholar.org/CorpusID:232412868>.

DIX, A. *Human Computer Interaction*. New York: Pearson Education, 2008. 860 p.

ESTATíSTICA, I. B. de Geografia e. *Censo Demográfico 2022*. 2022. Acesso em: 15 nov. 2023. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/periodicos/93/cd_2022_v1_br.pdf>.

Fapesp. *SciELO*. 2023. Disponível em: <https://www.scielo.br/>.

FARIA, E. d.; SOUZA, V. L. T. d. Sobre o conceito de identidade: apropriações em estudos sobre formação de professores. *Psicologia Escolar e Educacional*, v. 15, n. 1, p. 35–42, 2011. Disponível em: <https://www.scielo.br/j/pee/a/DTxHk78xxwXWq6gcH7RKjQG/?format=pdf>.

FIARRESGA, V. M. C. et al. *Criptografia e matemática*. Tese (Doutorado), 2010.

FLORENCIO, D.; HERLEY, C. A large-scale study of web password habits. In: *Proceedings of the 16th international conference on World Wide Web*. [S.l.: s.n.], 2007. p. 657–666.

FRIK, A.; NURGALIEVA, L.; BERND, J.; LEE, J.; SCHAUB, F.; EGELMAN, S. Privacy and security threat models and mitigation strategies of older adults. In: *SOUPS @ USENIX Security Symposium*. [s.n.], 2019. Disponível em: <https://api.semanticscholar.org/CorpusID:201803798>.

GILSENAN, C.; SHAKIR, F.; ALOMAR, N.; EGELMAN, S. Security and privacy failures in popular 2fa apps. In: *32nd USENIX Security Symposium (USENIX Security 23)*. [S.l.: s.n.], 2023.

Google. *Scholar*. 2023. Disponível em: <https://scholar.google.com/>.

GRANT, M. J.; BOOTH, A. A typology of reviews: an analysis of 14 review types and associated methodologies. *Health information and libraries journal*, v. 26 2, p. 91–108, 2009. Disponível em: <https://api.semanticscholar.org/CorpusID:42356478>.

GREENE, K. K.; TAMBORELLO, F. Password entry errors: Memory or motor? In: *Proceedings of the 2015 International conference on Cognitive Modeling*. [S.l.: s.n.], 2015.

GRIMES, G. A.; HOUGH, M. G.; MAZUR, E.; SIGNORELLA, M. L. Older adults' knowledge of internet hazards. *Educational Gerontology*, v. 36, p. 173 – 192, 2010. Disponível em: <https://api.semanticscholar.org/CorpusID:144434753>.

GROBLER, M.; GAIRE, R. K.; NEPAL, S. User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, v. 4, 2021. Disponível em: <https://api.semanticscholar.org/CorpusID:232162903>.

HÄMÄLÄINEN, N. Biometrics as an alternative to passwords for older users. In: . [s.n.], 2015. Disponível em: <https://api.semanticscholar.org/CorpusID:61265923>.

HÜLÜR, G.; MACDONALD, B. Rethinking social relationships in old age: Digitalization and the social lives of older adults. *American Psychologist*, American Psychological Association, v. 75, n. 4, p. 554, 2020.

IMRAN, A. *A comparison of password authentication between children and adults*. Tese (Doutorado) — Carleton University, 2015.

JITTIBUMRUNGRAK, P.; HONGWARITTORRN, N. A preliminary study to evaluate graphical passwords for older adults. *Proceedings of the 5th International ACM In-Cooperation HCI and UX Conference*, 2019. Disponível em: <https://api.semanticscholar.org/CorpusID:201090541>.

JUNIOR, V. F.; CECI, F.; WOSZEZENKI, C. R.; GONÇALVES, A. Design science research methodology enquanto estratégia metodológica para a pesquisa tecnológica. *Revistas Espacios 38 (6)*, p. 25, 2017.

JUOZAPAVIČIUS, A.; BRILINGAITĖ, A.; BUKAUSKAS, L.; LUGO, R. G. Age and gender impact on password hygiene. *Applied Sciences*, MDPI, v. 12, n. 2, p. 894, 2022.

KAHANI, N.; ELGAZZAR, K.; CORDY, J. R. Authentication and access control in e-health systems in the cloud. In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. [S.l.: s.n.], 2016.

KHAN, A.; CHEFRANOV, A. G. A captcha-based graphical password with strong password space and usability study. In: IEEE. *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*. [S.l.], 2020. p. 1–6.

KOMANDURI, S.; HUTCHINGS, D. R. Order and entropy in picture passwords. In: CITESEER. *Proceedings of graphics interface 2008*. [S.l.], 2008. p. 115–122.

LANITIS, A. A survey of the effects of aging on biometric identity verification. *International Journal of Biometrics*, v. 2, n. 1, p. 34, 2010.

LANITIS, A.; TSAPATSOULIS, N. Quantitative evaluation of the effects of aging on biometric templates. *IET Computer Vision*, IET, v. 5, n. 6, p. 338, 2011.

LANITIS, A.; TSAPATSOULIS, N.; MARONIDIS, A. Review of ageing with respect to biometrics and diverse modalities. In: . [s.n.], 2013. Disponível em: <https://api.semanticscholar.org/CorpusID:130991916>.

LATULIPE, C.; GATTO, A.; NGUYEN, H. T.; MILLER, D. P.; QUANDT, S. A.; BERTONI, A. G.; SMITH, A.; ARCURY, T. A. Design considerations for patient portal adoption by low-income, older adults. In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. [S.l.: s.n.], 2015. p. 3859–3868.

LATULIPE, C.; QUANDT, S. A.; MELIUS, K. A.; BERTONI, A.; JR, D. P. M.; SMITH, D.; ARCURY, T. A. Insights into older adult patient concerns around the caregiver proxy portal use: qualitative interview study. *Journal of medical Internet research*, JMIR Publications Toronto, Canada, v. 20, n. 11, p. e10524, 2018.

LAUDON, K. C.; LAUDON, J. P. *Sistemas de Informações Gerenciais*. São Paulo: Pearson Prentice Hall, 2014. 504 p.

LEITÃO JÚNIOR, P. d. S.; LUCENA, F. N. de; BRAGA, R. D.; NEIRA, R. A. Q. Regulação de segurança da informação eletrônica em saúde: visão geral. *Journal of Health Informatics*, v. 8, n. 4, 2016.

LENNARTSSON, M. *Evaluating the memorability of different password creation strategies: A systematic literature review.* 48 p. Dissertação (Bachelor's Thesis) — University of Skövde, School of Informatics, 2019.

LIANG, Y.; SAMTANI, S.; GUO, B.; YU, Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. *IEEE Internet of Things Journal*, IEEE, v. 7, n. 9, p. 9128–9143, 2020.

LOOS, L. A.; CROSBY, M. E. Cognition and predictors of password selection and usability. In: SPRINGER. *Augmented Cognition: Users and Contexts: 12th International Conference, AC 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part II.* [S.l.], 2018. p. 117–132.

LUNA, K. If it is easy to remember, then it is not secure: Metacognitive beliefs affect password selection. *Applied Cognitive Psychology*, Wiley Online Library, v. 33, n. 5, p. 744–758, 2019.

MAHESH, N.; HASH, L. J.; ADVISOR; MARSH, J.; WHITE, J. S. Password habits of security literate individuals. In: . [s.n.], 2018. Disponível em: <https://api.semanticscholar.org/CorpusID:69289826>.

MCCLELLAN, M. L. America walks into a bar: A spirited history of taverns and saloons, speakeasies, and grog shops. *Journal of American History*, Oxford University Press, v. 99, n. 2, p. 558–559, 09 2012. ISSN 0021-8723. Disponível em: <https://doi.org/10.1093/jahist/jas264>.

MELO, B. R. d. S.; DINIZ, M. A. A.; CASEMIRO, F. G.; FIGUEIREDO, L. C.; SANTOS-ORLANDI, A. A. d.; HAAS, V. J.; ORLANDI, F. d. S.; GRATÃO, A. C. M. Cognitive and functional assessment about elderly people users of health public service. *Escola Anna Nery*, SciELO Brasil, v. 21, p. e20160388, 2017.

MESSERSCHMIDT, M.; PLEVA, M. Biometric systems utilizing neural networks in the authentication for e-learning platforms. In: IEEE. *17th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. [S.l.], 2019. p. 518–523.

MINAYO, M.; GUALHANO, L. *Problemas de saúde e vulnerabilidade da população idosa.* 2017. SciELO em Perspectiva | Press Releases. Disponível em: <https://pressreleases.scielo.org/blog/2017/01/03/problemas-de-saude-e-vulnerabilidade-da-populacao-idosa/>.

Ministério da Saúde. *Saúde da pessoa idosa.* 2023. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/saude-de-a-a-z/s/saude-da-pessoa-idosa>.

MOALLEM, A. Did you forget your password? In: *Interacción*. [s.n.], 2011. Disponível em: <https://api.semanticscholar.org/CorpusID:3066621>.

MONTORO, M.; BABCOCK, S. *Cain and Abel (software)*. 2014. Disponível em: <https://en.wikipedia.org/wiki/Cain_and_Abel_(software)>.

MUBARAK, F.; SUOMI, R. Elderly forgotten? digital exclusion in the information age and the rising grey digital divide. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, v. 59, 2022.

NASER, S. Cryptography: from the ancient history to now, it's applications and a new complete numerical model. *International journal of mathematics and statistics studies*, v. 9, n. 3, p. 11–30, 2021.

NEDVĚD, V. *Careless society: Drivers of (un)secure passwords*. 284 p. Dissertação (Mestrado) — Univerzita Karlova, Fakulta sociálních věd, 2021.

NENADIC, A.; ZHANG, N.; YAO, L.; MORROW, T. Levels of authentication assurance: an investigation. 2007.

NETO, S. V. d. S. et al. Detecção de ataques em biometria facial utilizando redes neurais convolucionais. Universidade Federal da Paraíba, 2022.

NLM. *PubMed*. 2023. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/>.

NORDIN, S.; STURGE, J.; AYOUB, M.; JONES, A.; MCKEE, K. J.; DAHLBERG, L.; MEIJERING, L.; ELF, M. The role of information and communication technology (ict) for older adults' decision-making related to health, and health and social care services in daily life—a scoping review. *International Journal of Environmental Research and Public Health*, v. 19, 2021. Disponível em: <https://api.semanticscholar.org/CorpusID:245470663>.

OH, S. S.; KIM, K. A.; KIM, M.; OH, J.; CHU, S. H.; CHOI, J. Measurement of digital literacy among older adults: Systematic review. *Journal of Medical Internet Research*, v. 23, 2020. Disponível em: <https://api.semanticscholar.org/CorpusID:231788328>.

OLIVEIRA, W. d.; SALVADOR, P. d. O.; LIMA, K. d. Aspectos determinantes para construção social da pessoa idosa a partir das políticas públicas no brasil. *Saude soc*, v. 32, n. 2, p. e210118pt, 2023.

OMETOV, A.; BEZZATEEV, S.; MÄKITALO, N.; ANDREEV, S.; MIKKONEN, T.; KOUCHERYAVY, Y. Multi-factor authentication: A survey. *Cryptography*, MDPI, v. 2, n. 1, p. 1, 2018.

ONU. *Plano de Ação Internacional para o Envelhecimento*. Nova York: Organização das Nações Unidas, 2002. 86 p.

ONU. *Assembleia Geral da ONU declara 2021-2030 como Década do Envelhecimento Saudável*. 2020. Disponível em: <https://brasil.un.org/pt-br/105264-assembleia-geral-da-onu-declara-2021-2030-como-d%C3%A9cada-do-envelhecimento-saud%C3%A1vel>.

PADRõES, C. I. de. *A Segurança da Informação nos Sistemas de Saúde*. Genebra, 2016.

PALLADINO, P.; BENI, R. D. When mental images are very detailed: image generation and memory performance as a function of age. *Acta psychologica*, v. 113 3, p. 297–314, 2003. Disponível em: <https://api.semanticscholar.org/CorpusID:26002789>.

PARLIAMENT, E.; UNION, C. of the E. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. 73-115 p. Disponível em: <https://eur-lex.europa.eu/eli/reg/2014/910/oj>.

PILAR, D.; JAEGER, A.; GOMES, C. F. A.; STEIN, L. M. Passwords usage and human memory limitations: A survey across age and educational background. *PLoS ONE*, v. 7, 2012. Disponível em: <https://api.semanticscholar.org/CorpusID:2595779>.

QUAN-HAASE, A.; HO, D. Online privacy concerns and privacy protection strategies among older adults in east york, canada. *J. Assoc. Inf. Sci. Technol.*, v. 71, p. 1089–1102, 2020. Disponível em: <https://api.semanticscholar.org/CorpusID:218964845>.

RACHID, R.; FORNAZIN, M.; CASTRO, L.; GONçALVES, L.; PENTEADO, B. Saúde digital e a plataformização do estado brasileiro. *Ciênc saúde coletiva*, v. 28, n. 7, p. 2143–2153, Jul 2023.

RAY, H.; WOLF, F.; KUBER, R.; AVIV, A. J. Why older adults (don't) use password managers. *ArXiv*, abs/2010.01973, 2020. Disponível em: <https://api.semanticscholar.org/CorpusID:222133142>.

REGULATION, G. D. P. General data protection regulation (gdpr). *Intersoft Consulting, Accessed in October*, v. 24, n. 1, 2018.

RENAUD, K. V.; COLES-KEMP, L. Accessible and inclusive cyber security: A nuanced and complex challenge. *Sn Computer Science*, v. 3, 2022. Disponível em: <https://api.semanticscholar.org/CorpusID:249954389>.

SARKAR, A.; SINGH, B. K. A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, Springer, v. 79, p. 27721–27776, 2020.

SAYAGO, S.; BLAT, J. About the relevance of accessibility barriers in the everyday interactions of older people with the web. In: *Proceedings of the 2009 International Cross-Disciplinary Conference on Web Accessibililty (W4A)*. [S.l.: s.n.], 2009. p. 104–113.

SAúDE, M. da. *Saúde da pessoa idosa*. 2023. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/saude-de-a-a-z/s/saude-da-pessoa-idosa>.

SCHEIDAT, T.; HEINZE, J.; VIELHAUER, C.; DITTMANN, J.; KRAETZER, C. Comparative review of studies on aging effects in context of biometric authentication. In: *Electronic imaging*. [s.n.], 2011. Disponível em: <https://api.semanticscholar.org/CorpusID:121396725>.

SCHNEIER, B. *Secrets and lies: digital security in a networked world*. Nova Jersey: John Wiley & Sons, 2015. 448 p.

Sesc. *Mente Ativa*. 2023. Disponível em: <https://www.sesc-sc.com.br/servicos/mente-ativa>.

SHAHZAD, M.; LIU, A. X.; SAMUEL, A. Behavior based human authentication on touch screen devices using gestures and signatures. *IEEE Transactions on Mobile Computing*, v. 16, n. 10, p. 2726–2741, 2017.

SHARIF, M.; RAZA, M.; SHAH, J. H.; YASMIN, M.; FERNANDES, S. L. An overview of biometrics methods. *Handbook of multimedia information security: techniques and applications*, Springer, p. 15–35, 2019.

SIMMONS, J.; DIALLO, O.; OESCH, S.; RUOTI, S. Systematization of password manageruse cases and design paradigms. *Annual Computer Security Applications Conference*, 2021. Disponível em: <https://api.semanticscholar.org/CorpusID:238864929>.

SINGH, G.; SINGH, R. K.; SAHA, R.; AGARWAL, N. Iwt based iris recognition for image authentication. *Procedia Computer Science*, Elsevier, v. 171, p. 1868–1876, 2020.

SIQUEIRA, O. N.; CONTIN, A. C.; BARUFI, R. B.; LEHFELD, L. de S. A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. *Revista Eletrônica Pesquiseduca*, v. 13, n. 29, p. 236–255, 2021.

ŠOLIĆ, K.; OČEVČIĆ, H.; BLAŽEVIĆ, D. Survey on password quality and confidentiality. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, KoREMA-Hrvatsko društvo za komunikacije, računarstvo, elektroniku, mjerenja . . . , v. 56, n. 1, p. 69–75, 2015.

STALLINGS, W. *Arquitetura e Organização de Computadores*. 8. ed. São Paulo: Person, 2010. 624 p.

STANDARDS, N. I. of; TECHNOLOGY. *Digital Identity Guidelines*. [S.l.], 2017. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>.

TANENBAUM, A. S. *Sistemas Operacionais Modernos*. 3. ed. São Paulo: Pearson Universidades, 2009. 672 p.

TANWAR, S.; TYAGI, S.; KUMAR, N.; OBAIDAT, M. S. Ethical, legal, and social implications of biometric technologies. *Biometric-based physical and cybersecurity systems*, Springer, p. 535–569, 2019.

TECNOLOGIA, I. N. de Padrões e. *Digital Identity Guidelines: Authentication and Lifecycle Management*. [S.l.], 2017. Disponível em: <https://doi.org/10.6028/NIST.SP.800-63B>.

TOMASZCZYK, J. C.; FERNANDES, M. A. A positivity effect in older adults' memorability judgments of pictures. *Experimental Aging Research*, v. 39, p. 254 – 274, 2013. Disponível em: <https://api.semanticscholar.org/CorpusID:15080234>.

TRAN, L.; NGUYEN, T.; SEO, C.; KIM, H.; CHOI, D. *A Survey on Password Guessing*. 2022.

VELáSQUEZ, I.; CARO, A.; RODRíGUEZ, A. Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, v. 94, p. 30–37, 2018.

VU, K.-P. L.; HILLS, M. M. The influence of password restrictions and mnemonics on the memory for passwords of older adults. In: SPRINGER. *Human Interface and the Management of Information. Information and Interaction Design: 15th International Conference, HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part I 15*. [S.l.], 2013. p. 660–668.

WILSON, J. L.; HEINSCH, M.; BETTS, D.; BOOTH, D.; KAY-LAMBKIN, F. J. Barriers and facilitators to the use of e-health by older adults: a scoping review. *BMC Public Health*, v. 21, 2021. Disponível em: <https://api.semanticscholar.org/CorpusID:237101522>.

WOODS, N.; SIPONEN, M. Too many passwords? how understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, Elsevier, v. 111, p. 36–48, 2018.

YAN, J.; BLACKWELL, A.; ANDERSON, R.; GRANT, A. Password memorability and security: Empirical results. *IEEE Security & privacy*, IEEE, v. 2, n. 5, p. 25–31, 2004.

YESAVAGE, J. A. Imagery pretraining and memory training in the elderly. *Gerontology*, v. 29 4, p. 271–5, 1983. Disponível em: <https://api.semanticscholar.org/CorpusID:20975144>.

ZHANG, L.; RAZDAN, A.; FARIN, G.; FEMIANI, J.; BAE, M.; LOCKWOOD, C. 3d face authentication and recognition based on bilateral symmetry analysis. *The Visual Computer*, Springer, v. 22, p. 43–55, 2006.

ZHAO, Y.; ZHANG, T.; DASGUPTA, R. K.; XIA, R. Narrowing the age-based digital divide: Developing digital capability through social activities. *Information Systems Journal*, v. 33, p. 268 – 298, 2023. Disponível em: <https://api.semanticscholar.org/CorpusID:250576317>.

Glossário

Bares speakeasy É um estabelecimento ilícito que vendia bebidas alcoólicas durante o período da Lei Seca nos EUA.

Braille É um sistema de escrita tátil utilizado por pessoas cegas ou com baixa visão.

Designer de UX O design da experiência do usuário é o processo de definir a experiência pela qual um usuário passaria ao interagir com uma empresa, seus serviços e seus produtos.

Hacking Ato de comprometer dispositivos e redes digitais por meio de acesso não autorizado a uma conta ou sistema de computador

PassPAST Um gerenciador de senha premiado.

Phishing É uma técnica de engenharia social usada para enganar usuários de internet usando fraude eletrônica para obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito.

PIN Número de identificação pessoal.

SQL Structured Query Language, lit. "linguagem de consulta estruturada", é uma linguagem de domínio específico desenvolvida para gerenciar dados relacionais em um sistema de gerenciamento de banco de dados.

Strings São sequências de caracteres alfanuméricos (letras, números e/ou símbolos) amplamente usadas em programação.

Token É um dispositivo físico, que pode ser semelhante a um pen drive, que serve para armazenar um certificado digital

Zero-day É uma vulnerabilidade ainda não conhecida em um aplicativo ou sistema operacional, ou seja, uma lacuna na segurança para a qual não há defesa ou correção porque o fabricante do software não sabe que ela existe.

APÊNDICE A – Questionário sobre Memorização de Senhas por Idosos

Este questionário faz parte de um estudo sobre a memorização de senhas em idosos. As informações coletadas serão confidenciais e não serão compartilhadas com outras pessoas. Se você não quiser responder a alguma pergunta, pode deixá-la em branco.

1. Qual é a sua idade?

2. Qual é o seu gênero?
   ( ) Masculino
   ( ) Feminino
   ( ) Outro (especifique)

3. Até que série você estudou (completo ou não)?
   ( ) Ensino fundamental
   ( ) Ensino médio
   ( ) Ensino superior

4. Com que frequência você usa senhas no seu dia a dia?
   ( ) Diariamente
   ( ) Semanalmente
   ( ) Mensalmente
   ( ) Raramente
   ( ) Nunca

5. Como você costuma escolher suas senhas?
   ( ) Escolho senhas aleatórias
   ( ) Escolho senhas baseadas em informações pessoais (por exemplo, data de nascimento, nome de um parente)
   ( ) Escolho senhas com base em palavras comuns (por exemplo, "senha",

"123456")
( ) Outro (especifique)

6. Você tem dificuldade em memorizar senhas?
   ( ) Sim
   ( ) Não

7. Como você faz para memorizar senhas?
   ( ) Anoto a senha em um papel
   ( ) Memorizo a senha repetindo várias vezes
   ( ) Crio uma história para a senha
   ( ) Uso um aplicativo de gerenciament o de senhas
   ( ) Outro (especifique)

8. Você já teve problemas com a memorização de senhas em alguma ocasião?
   ( ) Sim
   ( ) Não

9. Se sim, o que aconteceu e como você resolveu o problema?

APÊNDICE B – Cards de Memorização

Figura 13 – Card com caracteres

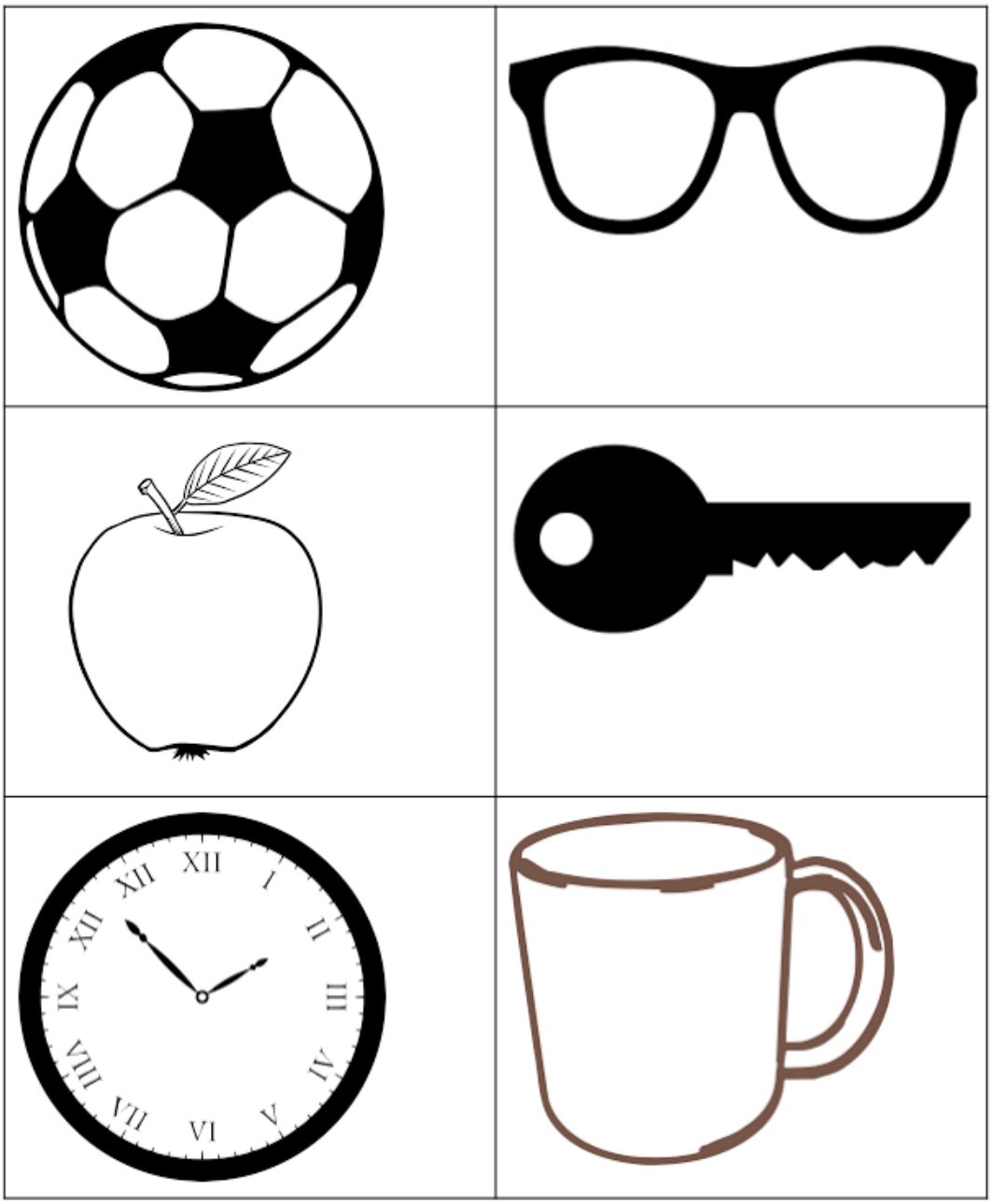
Forme uma senha com 3 palavras abaixo e memorize-a.

FELICIDADE	COMPUTADOR
AMIZADE	TRABALHO
ESCOLA	SAÚDE
FAMÍLIA	VIAGEM
DINHEIRO	AMOR

Fonte: Autor.

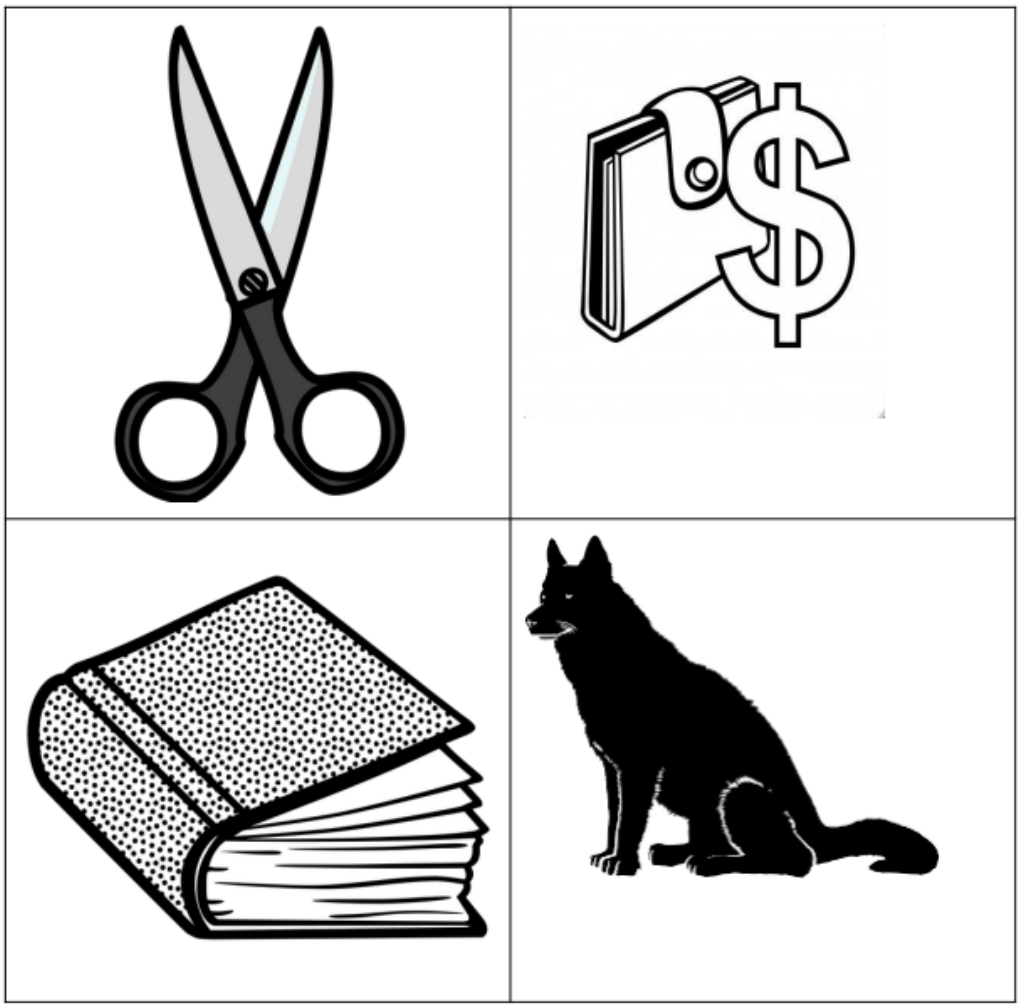
Figura 14 – Card com imagens

Forme uma senha com 3 objetos abaixo e memorize-a.



Fonte: Autor.

Figura 15 – Card com imagens



Fonte: Autor.

ANEXO A – Parecer Final do CEPSH-UFSC

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Memorização de senhas na população idosa: estudo comparativo entre senhas baseadas em objetos e palavras
Pesquisador: CARLA KNUST BASTOS
Área Temática:
Versão: 2
CAAE: 69431423.3.0000.0121
Instituição Proponente: Programa de Pós-Graduação em Informática em Saúde
Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 6.111.755

Apresentação do Projeto:
O projeto trata-se do estudo da dissertação da mestranda Carla Knust Bastos, SEM informação sobre quem orienta junto ao PPG em Informática em Saúde da UFSC.

Trata-se de estudo comparativo de corte transversal e que será realizado com 10 idosos com idade entre 60 e 80 anos, que concordarem em participar da pesquisa. Os participantes receberão um questionário básico sobre a frequência do uso de senhas e seus métodos de memorização. Em seguida, escolherão uma senha de 3 itens em um card com vários objetos e outra senha de 3 itens em um card com várias palavras. Cada participante terá um tempo máximo de 5 minutos para escolher cada senha. Após um intervalo de 40 minutos, em que terão atividades não relacionadas à pesquisa, eles serão solicitados a escrever as senhas escolhidas. A pontuação será baseada no número de itens corretos da senha.

Sistemas de informação são o conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem as informações para auxiliar na tomada de decisão, na coordenação e no gerenciamento de uma organização. Entre estes componentes podemos encontrar pessoas, procedimentos, hardware, software, bancos de dados e redes. Eles são projetados para atender às necessidades específicas da organização e atualmente são essenciais para melhorar a eficiência operacional, aumentar a produtividade e melhorar a comunicação entre

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 701
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br