

UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA



**Desenvolvimento de um gestor de palavras-passe acessível
para idosos**

João Pedro Bogalho Arcanjo

Mestrado em Engenharia Informática

Versão Provisória

Dissertação orientada por:

Profª. Doutora Soraia Vanessa Meneses Alarcão Castelo de Almeida Pires
Prof. Doutor Bernardo Luís da Silva Ferreira

Agradecimentos

Em primeiro lugar, quero agradecer à minha mãe pelo apoio incondicional que me deu ao longo de todo o meu percurso académico. A sua força e o facto de ter sempre acreditado em mim, especialmente nos momentos mais desafiantes, foram fundamentais. Agradeço-lhe, não só por me ter apoiado, mas também por me ter tornado na pessoa que sou hoje. Um agradecimento igualmente especial à minha irmã gémea, cujo apoio e compreensão foram constantes ao longo deste percurso. Quero também agradecer à minha namorada, Inês Lopes, pela sua presença diária, pelo carinho e pela força que me deu, especialmente durante este último ano, em que o seu apoio foi imprescindível.

Não posso deixar de mencionar os meus amigos que partilharam comigo esta importante etapa da minha vida e todo o meu percurso académico. Um agradecimento muito especial ao Diogo Novo, Francisco Ludovico e Rodrigo Pinto pela amizade, companheirismo e apoio.

Agradeço também de coração à minha família e aos restantes amigos que, de uma forma ou de outra, acompanharam-me durante esta fase e deram-me o suporte de que precisei. Um agradecimento especial àqueles que ajudaram no recrutamento de voluntários para a avaliação do projeto.

Gostaria também de expressar o meu sincero agradecimento a todos os idosos e respetivos cuidadores informais que, generosamente, disponibilizaram o seu tempo para participar neste projeto. A colaboração de todos foi crucial para o sucesso deste projeto, e sou-vos profundamente grato pela vossa contribuição.

Finalmente, gostaria de agradecer à professora Vânia Mendonça e aos meus orientadores, Soraia Alarcão e Bernardo Ferreira, pela disponibilidade, orientação e confiança que depositaram em mim, permitindo a concretização deste projeto, do qual me orgulho profundamente.

Para a minha avó, Piedade

Resumo

Com o crescimento das plataformas *online*, a necessidade de autenticação em múltiplas contas tornou-se um problema, especialmente para os utilizadores mais idosos, que enfrentam desafios significativos. As dificuldades cognitivas associadas à idade tornam a memorização de várias palavras-passe mais difícil, levando muitas vezes à reutilização das mesmas ou à escolha de combinações demasiado simples, o que compromete seriamente a segurança *online*.

Neste projeto, investigámos soluções que pudessem facilitar o processo de autenticação para os idosos. Apesar de já existirem métodos como autenticação através de som, desenhos ou *tokens*, estes apresentam algumas limitações. A necessidade de alterar os sistemas existentes para integrar estes métodos nos mesmos, a demora no processo de autenticação, e a dependência de dispositivos adicionais, são alguns exemplos dessas limitações.

Com base num *design* centrado no utilizador e prototipagem iterativa, desenvolvemos um gestor de palavras-passe com a participação de 9 idosos e um perito ao longo do desenvolvimento. Aplicámos algoritmos como o *Signal* e o *Secret Sharing* para garantir a segurança dos dados dos utilizadores, permitindo o armazenamento seguro das credenciais na *Cloud* e a sua interpretação pelos cuidadores.

O protótipo final foi avaliado com 17 idosos utilizando o questionário *System Usability Scale* (SUS). Obtivemos um valor médio de 81.3, sugerindo que o nosso protótipo é fácil de utilizar pelo público-alvo.

Palavras-chave: Cuidadores Informais; *Design* Centrado no Utilizador; Gestor de Palavras-passe; Idosos; Segurança

Abstract

With the growth of online platforms, the need for authentication across multiple accounts has become a problem, especially for elderly users, who face significant challenges. Cognitive difficulties associated with aging make it harder to memorize multiple passwords, leading to password reuse or the selection of simple combinations, which seriously compromises online security.

In this project, we investigated solutions that could ease the authentication process for the elderly. Although methods such as sound-based authentication, drawings, or tokens already exist, they present certain limitations. The need to modify existing systems to integrate these methods, the time-consuming authentication process, and the reliance on additional devices are some examples of these limitations.

As regard as user-centered design and iterative prototyping, we developed a password manager involving 9 elderly participants and an expert throughout the development process. We applied algorithms such as Signal and Secret Sharing to ensure the security of user data, enabling the safe storage of credentials in the Cloud and their interpretation by caregivers.

The final prototype was evaluated with 17 elderly participants using the System Usability Scale (SUS) questionnaire. We obtained an average score of 81.3, suggesting that our prototype is easy to use by the target audience.

Keywords: Elderly; Informal Caregivers; Password Manager; Security; User-Centered Design

Conteúdo

<u>Lista de Figuras</u>	xiv
<u>Lista de Tabelas</u>	xvii
1 Introdução	1
1.1 Motivação	1
1.2 Objetivos	2
1.3 Contribuições	3
1.4 Estrutura do documento	3
2 Trabalho relacionado	5
2.1 Métodos de Autenticação	5
2.2 Gestores de Palavras-passe	10
2.3 Secret Sharing	13
2.4 Sumário	15
3 Levantamento de Requisitos	17
3.1 Requisitos Funcionais	17
3.2 Requisitos Não Funcionais	19
3.3 Sumário	20
4 Desenho da Solução	21
4.1 Arquitetura do Sistema	21
4.1.1 Aplicações móveis	21
4.1.2 Servidor Intermédio	23
4.1.3 Servidor de Autenticação e Armazenamento	24
4.2 Segurança	26
4.2.1 Modelo de Adversário	26
4.2.2 Mecanismos de Segurança	26
4.3 Operações do Sistema	30
4.3.1 Criação da Conta	31
4.3.2 Atualizar os Dados Pessoais	31

4.3.3	Envio Pedido de Vinculação	31
4.3.4	Receber um Pedido de Vinculação	32
4.3.5	Aceitar Pedido de Vinculação	32
4.3.6	Cancelar ou Rejeitar Pedido de Vinculação	33
4.3.7	Desvinculação de uma Relação	33
4.3.8	Alteração das Permissões de um Cuidador	34
4.3.9	Atualização das Credenciais	34
4.3.10	Apagar Credenciais	34
4.3.11	Criar Identidade no Servidor Intermédio	35
4.3.12	Apresentação do Ecrã <i>SplashScreen</i>	35
4.4	Sumário	35
5	Implementação	37
5.1	Tecnologias	37
5.1.1	Firebase	37
5.1.2	React Native	39
5.1.3	NodeJS	40
5.1.4	Criptografia	40
5.2	Implementação do <i>Frontend</i>	41
5.2.1	Decisões de <i>Design</i>	41
5.2.2	Fluxos do <i>Frontend</i>	42
5.3	Sumário	47
6	Avaliação	49
6.1	Avaliação Heurística do Protótipo Funcional 1	49
6.1.1	Metodologia	49
6.1.2	Resultados e Melhorias Realizadas	49
6.2	Avaliação Heurística do Protótipo Funcional 2	50
6.2.1	Participantes	51
6.2.2	Metodologia	51
6.2.3	Resultados e Melhorias Realizadas	52
6.3	Avaliação da Usabilidade do Protótipo Funcional Final	58
6.3.1	Metodologia	58
6.3.2	Participantes	59
6.3.3	Resultados Experimentais	62
6.3.4	Conclusões Finais	62
6.4	Avaliações do Desempenho do Protótipo Funcional Final	64
6.4.1	Ambiente	64
6.4.2	Validação das credenciais	64
6.4.3	Rotatividade das Chaves	66

6.4.4	Operações Sobre as Credenciais	66
6.4.5	Operações Sobre a Conta	67
6.4.6	Conclusão dos Resultados	67
6.5	Sumário	67
7	Conclusão e trabalho futuro	69
7.1	Sumário	69
7.2	Contribuições e Limitações	70
7.3	Trabalho Futuro	71
Bibliografia		79
Índice		80
A	Protótipo de alta fidelidade (idoso)	81
B	Protótipo de alta fidelidade (cuidador)	83
C	Guião experimental	85
D	Avaliação heurística	95

Lista de Figuras

2.1	Esquema de funcionamento do <i>Secret Sharing</i> (SS) (melhor visto a cores).	14
2.2	Algoritmo <i>Secret Sharing</i> de Shamir com t=2 & n=3 (melhor visto a cores).	15
3.1	Fluxo do projeto (melhor visto a cores).	17
4.1	Arquitetura do sistema (melhor visto a cores).	22
4.2	Base de dados relacional das aplicações móveis.	23
4.3	Estrutura do Servidor de Autenticação e Armazenamento (melhor visto a cores).	25
4.4	Rotatividade das chaves criptográficas (melhor visto a cores).	29
4.5	Validação das credenciais (melhor visto a cores).	30
4.6	Validação no Servidor Intermédio (melhor visto a cores).	30
4.7	Geração de chave criptográfica (melhor visto a cores).	30
4.8	Operação de criação de conta (melhor visto a cores).	31
4.9	Operação de atualização dos dados pessoais (melhor visto a cores).	31
4.10	Operação de envio de um pedido de vinculação (melhor visto a cores).	32
4.11	Operação da receção de um pedido de vinculação (melhor visto a cores).	32
4.12	Aceitar pedido de vinculação (melhor visto a cores).	32
4.13	Cancelar ou Rejeitar pedido de vinculação (melhor visto a cores).	33
4.14	Rejeição automática de pedido de vinculação (melhor visto a cores).	33
4.15	Desvinculação de uma relação (melhor visto a cores).	33
4.16	Atualizar permissões do cuidador (melhor visto a cores).	34
4.17	Atualizar as credenciais pessoais (melhor visto a cores).	34
4.18	Atualizar as credenciais do idoso (melhor visto a cores).	34
4.19	Apagar credenciais pessoais (melhor visto a cores).	35
4.20	Criar identidade no servidor (melhor visto a cores).	35
4.21	Apresentação do ecrã <i>SplashScreen</i> (melhor visto a cores).	36
5.1	Fluxo da criação de conta (melhor visto a cores).	42
5.2	Fluxo de edição de dados pessoais (melhor visto a cores).	43
5.3	Fluxo gerador de palavras-passe fortes (melhor visto a cores).	44
5.4	Fluxo de gestão dos cuidadores (melhor visto a cores).	44
5.5	Fluxo de gestão dos idosos (melhor visto a cores).	45
5.6	Fluxo de edição de uma nova credencial (melhor visto a cores).	46

5.7 Fluxo de visualização e edição dos detalhes de uma credencial (melhor visto a cores).	46
5.8 Fluxo da página para ajudar os utilizadores (melhor visto a cores).	47
6.1 Progressão do menu inicial (melhor visto a cores).	53
6.2 Evolução da página com a informação dos cuidadores (melhor visto a cores).	54
6.3 Evolução da página para adicionar uma credencial (melhor visto a cores).	55
6.4 Evolução da página para listar as credenciais existentes	57
6.5 Resultados recolhidos para cada <i>construct</i> AT, PU, PEOU, SE e ANX, do STAM (melhor visto a cores).	61
6.6 Resultados recolhidos para cada pergunta do SUS (melhor visto a cores).	63
6.7 Comparação dos tempos médios para diferentes situações de manipulação independente das credenciais (melhor visto a cores).	65

Lista de Tabelas

2.1 Comparação dos diversos métodos de autenticação previamente discutidos.	10
6.1 Idosos que participaram na avaliação intercalar.	51
6.2 Idosos que participaram na avaliação final.	60
6.3 Resultados dos idosos na execução das tarefas.	62

Capítulo 1

Introdução

Neste capítulo, apresentamos a motivação e principais objetivos do nosso projeto. Detalhamos ainda as contribuições do nosso trabalho, concluindo com a descrição da estrutura do documento.

1.1 Motivação

O modo como nos identificamos num determinado serviço, na maioria das vezes, é por meio do nome de utilizador, e de uma palavra-passe. Estas credenciais são essenciais para garantir a privacidade e segurança dos utilizadores, mas, por outro lado, são também uma fonte de problemas e frustrações. Com o aumento do número de serviços *online* e a necessidade de criação de credenciais seguras e exclusivas para cada um deles têm levado muitas pessoas a enfrentar dificuldades em memorizar todas as informações exigidas.

As dificuldades mencionadas anteriormente suscitaram estudos que apresentam preocupações significativas relacionadas com a gestão de palavras-passe, nomeadamente o facto de serem pouco atualizadas [35], serem reutilizadas em várias contas distintas [2], a falsa crença de segurança relativamente às práticas utilizadas [51], a excessiva confiança na memória [19], e a crescente fragilidade das palavras-passe escolhidas com o avançar da idade [26].

Nos últimos anos, a utilização de serviços *online* entre a população mais idosa também aumentou, onde se incluem redes sociais, fóruns e serviços bancários [18]. A autenticação e memorização de credenciais tornam-se especialmente desafiantes para esta faixa etária, uma vez que o processo de lembrar múltiplas palavras-passe é um problema que muitos evitam devido a limitações cognitivas e de memória [8], (capacidades que tendem a ser afetadas com o avançar da idade [44]). O medo de se esquecerem das credenciais é uma preocupação recorrente [36], levando-os a optar por palavras-passe de fácil memorização em vez de seguirem as recomendações de criarem palavras-passe mais seguras, como o uso de sequências longas e aleatórias de caracteres. Adicionalmente, a falta de conhecimento sobre a gestão de credenciais é evidente entre os idosos, que não prestam igual atenção a todas as contas. Um estudo [17] revelou que estes são mais cuidadosos com credenciais que consideram importantes, não percebendo que a vulnerabilidade de uma conta menos crucial pode afetar a segurança de outras contas relacionadas.

Tradicionalmente, diz-se que os idosos são uma fonte de grande conhecimento e sabedoria

devido às suas experiências de vida, o que os torna eficientes a resolver problemas [22] e em encontrar correspondências entre situações atuais e antigas. No entanto, os idosos do século XXI foram subitamente inseridos num ambiente tecnológico vasto, tornando desafiante relacionar eventos passados com o cenário atual, o que torna o processo de aprendizagem mais complexo [43], e muito mais demorado [8]. Esses problemas de aprendizagem e falta de conhecimento levam os idosos a mencionar quatro obstáculos quando questionados sobre a sua proteção *online*: o esforço necessário, o receio de que algo corra mal, a frequência de mudanças nas interfaces das aplicações, ou a crença de que as ameaças são exageradas [36]. Uma consideração importante sobre o uso de palavras-passe por idosos envolve não apenas a sua escolha, mas também o seu armazenamento para futuras consultas, dado que a frustração por se esquecerem das palavras-passe é um sentimento comum. Por exemplo, quando tentam aceder às suas contas e falham após o número de tentativas permitido ser ultrapassado [44], acabam por desistir devido à falta de assistência.

Nos estudos de Merdenyan *et al.* e Ray *et al.* [35, 40], os autores constataram que o papel é a escolha predominante por parte dos idosos para registarem as suas palavras-passe, com quase metade dos entrevistados a adotarem esta abordagem. Cerca de 30% recorre a métodos digitais, justificando-se esta baixa percentagem pela falta de conhecimento e pelo *design* das ferramentas [35] ser pouco acessível. Entre os idosos que utilizam métodos digitais, os que recorrem a gestores de palavras-passe reconhecem limitações nestes sistemas e relatam dificuldades significativas na sua utilização [17]. Outras duas razões que levam os idosos a não recorrer a estes sistemas são por um lado, o facto destes serem pagos [40] e por outro, os idosos não possuírem noção mental correta do modelo de *software* implementado [12], ou seja, não entenderem se possuem o sistema bem configurado ou se concluíram a ação que pretendiam com sucesso. Concluímos que armazenar as palavras-passe é algo que os idosos entendem ser extremamente essencial, mas a falta de conhecimento leva-os a terem dificuldades em arranjar boas soluções.

1.2 Objetivos

Este trabalho tem como principal objetivo desenvolver um gestor de palavras-passe destinado a ser utilizado por idosos, algo solicitado por esta faixa etária [53]. Pretende-se que o sistema ajude a resolver desafios e riscos relacionados com a privacidade e segurança dos idosos no mundo *online*, garantindo a segurança das suas credenciais e auxiliando na sua manutenção. Em seguida apresentamos os principais sub-objetivos deste projeto:

- Identificar soluções de autenticação desenvolvidas para idosos ou que possam beneficiar esta faixa etária, explorando alternativas às palavras-passe e métodos auxiliares para a gestão das credenciais;
- Desenvolver um sistema que os idosos utilizem sem qualquer limitação, onde possam gerir as suas credenciais, e beneficiar da ajuda de um cuidador informal neste processo, uma vez que estes consideram os familiares peças fundamentais para a adoção destas tecnologias [40, 39], e a presença de alguém de confiança neste processo é essencial [44];

- Implementar mecanismos de criptografia que assegurem que as credenciais dos utilizadores estejam devidamente protegidas tanto na *Cloud* quanto localmente nos dispositivos dos utilizadores. Adicionalmente, pretendemos garantir que os dados confidenciais armazenados no sistema são trocados de forma segura entre os idosos e os cuidadores, bem como garantir que é possível realizar a recuperação segura das credenciais dos idosos;
- Incluir o público-alvo e um perito durante o desenvolvimento do sistema, bem como avaliar o protótipo final com esse público, é essencial para assegurar que a interface do gestor considera as características da população idosa.

1.3 Contribuições

O presente trabalho contribui para a área da segurança digital, com o desenvolvimento de um gestor de palavras-passe projetado para atender às necessidades dos idosos. Este sistema facilita o armazenamento seguro e a gestão de credenciais, abrangendo tanto *logins* em plataformas *online* assim como de informações sensíveis de cartões, garantindo uma solução adaptada ao perfil dos utilizadores mais velhos.

Entre as funcionalidades principais do sistema, destaca-se a geração de palavras-passe fortes e a verificação automática da sua robustez. O sistema permite a criação de vínculos entre os idosos e os seus cuidadores informais, oferecendo assistência remota na gestão de credenciais. Esta funcionalidade atua como uma medida de segurança adicional, permitindo que os cuidadores ajudem os idosos caso estes percam o acesso ao sistema. Para garantir a privacidade e segurança dos dados, foram implementadas técnicas avançadas, como o *Secret Sharing* e o protocolo *Signal*. O *Secret Sharing* assegura que as chaves criptográficas, utilizadas para cifrar as credenciais presentes na *Cloud*, nunca são armazenadas pelos cuidadores, protegendo assim a confidencialidade das informações partilhadas, enquanto o algoritmo *Signal* permite que os dados trocados entre as aplicações estejam devidamente protegidos. Além disso, o sistema inclui tutoriais em vídeo e texto, respostas a perguntas frequentes e recomendações de boas práticas de segurança. Estas funcionalidades foram desenvolvidas com o objetivo de maximizar a adesão dos idosos.

A interface desenvolvida foi orientada por requisitos recolhidos da literatura, pelas avaliações heurísticas realizadas por um perito e pelas interações com os idosos ao longo do desenvolvimento. Este processo assegurou o alinhamento do sistema com as melhores práticas de usabilidade e segurança, garantindo a eficácia e adequação da solução às necessidades dos idosos, e promovendo um ambiente digital mais seguro e acessível para todos.

1.4 Estrutura do documento

Este documento é dividido em sete capítulos, cada um organizado da seguinte forma:

- O Capítulo I introduz o trabalho realizado, apresentando as motivações que levaram ao seu desenvolvimento, os principais objetivos e as contribuições do mesmo;

- O Capítulo 2 apresenta o trabalho relacionado sobre a autenticação para idosos, e compara métodos de autenticação. Este capítulo também descreve o algoritmo *Secret Sharing*;
- O Capítulo 3 apresenta os requisitos que foram incluídos no projeto;
- O Capítulo 4 detalha a solução implementada, incluindo a arquitetura do sistema, o modelo adversário e os mecanismos de segurança implementados. Finaliza-se com a descrição das operações presentes no sistema quando determinadas ações são despoletadas;
- O Capítulo 5 descreve os detalhes da implementação, incluindo as tecnologias utilizadas, a criptografia aplicada, as decisões de *design* e as principais tarefas realizáveis através da interface da aplicação;
- O Capítulo 6 apresenta as diferentes avaliações realizadas ao sistema, incluindo avaliações de desempenho, avaliações heurísticas aos protótipos intermédios e a avaliação do protótipo final com o público-alvo;
- O Capítulo 7 apresenta um resumo do trabalho realizado, as contribuições, as limitações e as perspetivas para o trabalho futuro numa eventual versão do sistema.

Capítulo 2

Trabalho relacionado

O método de autenticação mais comum recorre a palavras-passe alfanuméricas, algo não bem aceite pela população idosa devido às dificuldades relacionadas com a memorização e segurança das mesmas. Neste capítulo apresentamos as soluções que foram desenvolvidas para ajudar a mitigar os problemas que esta faixa etária enfrenta na autenticação.

2.1 Métodos de Autenticação

Devido às diversas experiências negativas que os idosos têm sofrido no processo de autenticação, têm surgido outros métodos com o intuito de agilizarem este processo. Alguns métodos são projetados especificamente para atender às necessidades da população idosa, enquanto outros visam facilitar a autenticação para o público em geral, beneficiando especialmente os idosos. Os métodos de autenticação atuais são classificados em três categorias: baseados em conhecimento, *tokens* e biometria. A seguir, detalhamos cada uma dessas categorias:

- **Conhecimento:** Esta categoria diz respeito à validação da autenticação baseada no conhecimento do utilizador, como palavras-passe, PINs e padrões, tornando-se a que exige maior esforço por parte dos utilizadores. As palavras-passe são a opção mais comum;
- **Token:** Esta categoria autentica o utilizador com base em algo que ele possua. Exemplos relevantes incluem o telemóvel, *smart cards* e até pulseiras ou outros objetos pessoais com um sistema *Radio-frequency Identification* (RFID). O facto dos idosos poderem não querer usar estes dispositivos, bem como o seu custo elevado e a pouca acessibilidade para esta população, são algumas das desvantagens associadas a estes métodos. Contudo, a principal desvantagem é a necessidade de transportar o dispositivo físico, e, caso seja roubado ou perdido, a identidade do utilizador pode ficar em risco. Uma possível solução seria a duplicação do dispositivo, mantendo a cópia guardada num local seguro;
- **Biometria:** Esta categoria envolve a validação do utilizador com base em características físicas ou biológicas. Muitos idosos consideram a utilização de teclados complicada, pelo que, preferem outras alternativas, o que torna esta categoria uma opção viável. Um estudo realizado [27] revelou que os idosos consideram este método de autenticação mais

seguro do que outros conhecidos pelos mesmos. Contudo, a autenticação por meio de dados biométricos requer *hardware* e *software* específicos, que nem sempre estão disponíveis para os idosos. Por outro lado, os problemas de saúde dos idosos também são um fator limitante à utilização deste tipo de sistemas. Num estudo realizado por Kowtko et al. [31], foi analisado o uso deste método pelos idosos e concluiu-se que problemas de coração, pulmões, circulação, possíveis cataratas e condições de íris são fatores bastante comuns em idosos e que podem comprometer o uso destes sistemas. Estas implicações devem-se a sistemas terem que ser extremamente precisos e as condições físicas poderem gerar erros na autenticação devido à possível variação nos resultados apresentados pelos idosos. Outro estudo [28] também confirma que as mudanças físicas dos idosos podem afetar a sua autenticação. A re-inscrição periódica dos idosos poderia ajudar a mitigar este problema, mas, em alguns casos, pode ser um processo demorado e oneroso.

De seguida, apresentamos alguns métodos de autenticação, que abrangem as categorias anteriormente mencionadas e que podem beneficiar esta faixa etária:

- **HandWing:** O HANDWING [43] é um sistema de autenticação baseado no conhecimento, projetado especialmente para facilitar a autenticação dos idosos, tendo como principal foco esta faixa etária. Para realizar a autenticação, os idosos necessitam de passar por três etapas. A primeira etapa envolve a identificação correta de um PIN por meio do reconhecimento da sua caligrafia, ou seja, é apresentado ao idoso o seu PIN escrito com diversas caligrafias e este necessita de escolher a opção correta. Na segunda etapa, é necessário que o idoso identifique o seu código postal, escrito com a sua caligrafia. Por fim, o idoso deve identificar o seu desenho num conjunto de imagens. É importante salientar que este método de validação pode tornar-se um processo demorado, e a necessidade de os idosos submeterem informações escritas manualmente pode causar constrangimentos;
- **Graphical-password:** Neste método de autenticação, recorre-se a uma grelha em que cada posição da mesma representa uma coordenada. O utilizador cria a sua palavra-passe ao escolher ou conectar diversas coordenadas da grelha, sendo que a combinação dessas coordenadas representa a respetiva palavra-passe. Este modo de autenticação tem vindo a ganhar popularidade ao longo das últimas décadas, nomeadamente nos dispositivos com o sistema operativo *Android*, o que tem motivado alguns estudos sobre o mesmo [5]. Neste estudo, os autores conduziram várias investigações que analisaram aproximadamente 25 métodos baseados em GRAPHICAL-PASSWORD. Estes métodos permitiam que os utilizadores personalizassem as suas palavras-passe na grelha utilizando informações pessoais, facilitando assim a memorização e melhorando a usabilidade do sistema. Os autores concluíram que, apesar da diversidade de métodos, ainda há uma falta de avaliação rigorosa quanto à segurança e à usabilidade dessas soluções. Um exemplo notável deste modo de autenticação é o DRAW-A-SECRET (DAS) [25]. O DAS requer que os utilizadores desenhem padrões sobre uma grelha que, após serem processados, são obtidas das mesmas as coordenadas do *input* inser-

rido. Essas coordenadas compõe a palavra-passe do utilizador. Um dos grandes motivos do desenvolvimento destes métodos, foi o facto dos humanos possuírem a ágil capacidade de se relembrarem de padrões, e, uma vez que os idosos possuem esta capacidade, torna este método viável para a autenticação desta faixa etária. Por outro lado, a necessidade de um ecrã com o tamanho adequado para que o idoso consiga visualizar a grelha sem qualquer limitação, bem como os passos necessários para criar ou atualizar as credenciais, podem ser obstáculos que os idosos tenham dificuldades em lidar;

- **Gesture-password:** Estes métodos de autenticação recorrem, normalmente, ao desenho realizado no dispositivo do utilizador, onde, ao contrário do método de autenticação apresentado anteriormente, este não recorre a qualquer grelha, mas sim a diversos fatores presentes na escrita, nomeadamente a velocidade, as pausas realizadas, os movimentos, entre outros. Uma investigação [13] sobre os métodos de GESTURE-PASSWORD concluíram que, além destes proporcionarem uma autenticação rápida, personalizável e fácil de memorizar, oferecem também maior segurança em comparação com algumas alternativas convencionais. Estes métodos exigem menor concentração e precisão por parte dos utilizadores. No entanto, o tamanho e a qualidade dos ecrãs pode representar uma limitação para parte da população. Outro estudo [49] onde o foco principal foram os idosos, destacou que esta abordagem representa uma solução viável para a faixa etária em questão, uma vez que os idosos tendem a recordar imagens a longo prazo, em contraste com palavras-passe alfanuméricas tradicionais. Além disso, os resultados indicam que, surpreendentemente, os idosos apresentaram melhor desempenho que os jovens, dado demonstrarem uma precisão mais elevada nos desenhos efetuados. Por outro lado, problemas relacionados com o tamanho e sensibilidade dos ecrãs dos dispositivos podem ser limitações que os mesmos possam vir a enfrentar;
- **Musipass:** A omnipresença da música nas nossas vidas impulsionou o desenvolvimento do MUSIPASS [20]. Especial atenção foi dada aos idosos, que representam um público-chave. Este sistema de autenticação exige que os utilizadores passem por quatro etapas, em cada uma das quais são apresentadas nove músicas e é solicitado ao utilizador que selecione a sua favorita. Se as preferências coincidirem, a autenticação é bem-sucedida. Os utilizadores consideram que este método é consideravelmente mais intuitivo quando comparado com a autenticação convencional por meio de palavras-passe alfanuméricas. No entanto, tal como o HANDWING [43], este processo é notavelmente demorado, o que representa a principal desvantagem deste sistema. Quanto à usabilidade deste método, o uso de auscultadores é necessário caso o utilizador se encontre num ambiente ruidoso, bem como para evitar que terceiros descubram as credenciais. No entanto, nem todos os idosos fazem uso regular destes dispositivos. Para além disso, problemas de audição é algo comum nesta faixa etária, o que pode representar um desafio em termos de acessibilidade;
- **Pico:** A necessidade dos utilizadores terem de memorizar as suas palavras-passe, resulta na escolha de palavras-passe mais fracas. Este problema motivou o desenvolvimento de métodos de autenticação baseados em *tokens*, sendo o PICO [50] um exemplo. Este sistema

implica o uso de um dispositivo, como por exemplo, uma pulseira, que acompanha o utilizador. Esse dispositivo utiliza dados biométricos e é automaticamente bloqueado quando não está em uso, exigindo a presença de outros dispositivos previamente configurado exclusivos como por exemplo, uns óculos. Estes óculos têm de ser capazes de comunicar com o dispositivo principal, a pulseira, de forma a autenticarem o utilizador para proceder ao desbloqueio do dispositivo principal. Ao longo do artigo, os autores detalham como é que este sistema pode ser aplicado a várias plataformas que necessitam de autenticação e como é que os dados mais sensíveis podem ser protegidos no hardware utilizado. Este sistema não foi desenvolvido nem testado, permanecendo apenas como um conjunto de ideias não materializadas. No entanto, apesar da necessidade de dispositivos adicionais, eventualmente caros, não acessíveis para a população e possivelmente difíceis de utilizar, a vantagem de não requerer que os utilizadores memorizem informações e a integração entre dados biométricos e *tokens* poderiam proporcionar maior confiança, especialmente para os idosos;

- **Palavras-passe baseadas em imagens:** Um dos principais desafios enfrentados pelos idosos, tal como já mencionado, é a tendência de se esquecerem das palavras-passe alfanuméricas mais complexas, o que muitas vezes os leva a optar por palavras-passe mais simples. Para abordar esse problema, estudos, como o conduzido por Deborah e Lu et al. [37], exploram como palavras-passe baseadas em imagens podem ser úteis para os utilizadores relembrarem-se das mesmas. Muito sucintamente, os autores propõem adicionar significado às senhas, ao mesmo tempo que garantem a sua segurança. Esse objetivo é alcançado por meio do uso de técnicas mnemónicas para melhorar a memorização. Estas técnicas consistem em obter uma frase da imagem e, a partir da mesma, colocar diversos caracteres especiais misturados na frase, de modo a acrescentar complexidade à mesma. Outro estudo [52], cujo foco são os idosos, aborda a aplicação destas mnemónicas em fotos pessoais dos mesmos. Por exemplo, tendo como base a imagem do idoso a andar de skate, a palavra-passe seria “gosto de skates”, sendo posteriormente convertida em algo mais seguro, como “G0stoD3\$k8tes”. Através dos resultados, foi possível concluir pelos autores que os idosos conseguem criar palavras-passe que são menos suscetíveis a serem esquecidas, e, ao mesmo tempo, de maior complexidade, tornando-as assim mais difíceis de decifrar. Por outro lado, embora contribua para a memorização, é essencial persistir na prática da mesma, além da necessidade de salvaguardar a imagem utilizada, algo crucial no caso de ser necessária para auxiliar o idoso a recordar a palavra-passe durante a autenticação;
- **2FA:** A fragilidade das palavras-passe frequentemente escolhidas por todos os utilizadores, nomeadamente os idosos, exige a implementação de uma camada adicional que comprove a sua identidade durante o processo de autenticação. O sistema de autenticação TWO-FACTOR-AUTHENTICATION (2FA) [46] é um mecanismo que incorpora duas etapas de autenticação. A primeira etapa geralmente envolve o recurso a um método baseado em conhecimento, enquanto a segunda etapa recorre normalmente a um *token* de autenticação. Um estudo [15] investigou a experiência dos idosos na adoção destes sistemas, salientando

algumas das questões com que se depararam. Entre os problemas relatados pelos idosos está a falta de um *design* pensado na sua faixa etária, a ausência de instruções claras que os leva muitas vezes a tomar decisões erradas, e a dependência de outros dispositivos. Além disso, a falta de *feedback* positivo após uma autenticação bem-sucedida é uma fonte de confusão para os mesmos, deixando-os sem perceber se conseguiram realizar a autenticação ou não;

- **PassKeys:** Este método de autenticação dispensa o uso de palavras-passe para validar os utilizadores. Em vez disso, a autenticação é baseada em criptografia, onde uma chave pública é armazenada no servidor onde o utilizador deseja autenticar-se, e a respetiva chave privada, que é nada mais que o *token* de autenticação do utilizador, fica armazenada localmente no dispositivo do utilizador. Apesar de amplamente considerado um dos métodos mais seguros por várias empresas, muitas encontram-se reticentes em adotá-lo. Um estudo [32] analisou os principais motivos pelos quais as empresas ainda não adotaram este método. Estes incluem a resistência à cultura atual de autenticação, particularmente às palavras-passe, a falta de opções padronizadas e seguras de *fallback* caso as credenciais sejam perdidas ou fiquem indisponíveis, a conformidade com regulamentos específicos, práticas de segurança enraizadas e a preocupação com a segurança ao compartilhar a chave privada através da nuvem. Exemplos como a *Apple*, que restringe o uso de *PassKeys* ao seu próprio ecossistema, e alguns dispositivos *Android* que não suportam de todo este método de autenticação, dificultam a sua adoção. No caso dos idosos, a transição para este método pode ser ainda mais desafiante, exigindo uma demonstração das suas vantagens e desvantagens em relação às palavras-passe, que já fazem parte do seu quotidiano. É também essencial fornecer assistência na configuração assim como na utilização deste método.

Na Tabela 2.1, é apresentada uma comparação concisa dos diversos tipos de autenticação previamente mencionados. Esta tabela foi elaborada para facilitar a identificação dos métodos que estamos a comparar, bem como para avaliar três parâmetros essenciais que consideramos ao escolher um método de autenticação para esta faixa etária. A informação da mesma foi extraída dos resultados e análises decorrentes dos estudos associados a este tópico, previamente apresentados. Relativamente ao significado de cada coluna, a primeira, denominada por “Tipo” refere-se ao tipo de autenticação utilizado no respetivo método. Por sua vez, a coluna “Rápida autenticação” visa identificar quais são os métodos, tal como o nome indica, cuja autenticação não é um processo demorado, com muitos passos e possivelmente exaustivo para o idoso. Já a coluna “Pensado nos Idosos” tende a realçar quais é que tiveram os idosos em conta no seu processo de planeamento e desenvolvimento. Por último, a coluna “Testado com idosos” tem o intuito de evidenciar quais os métodos de autenticação que foram testados com idosos e a partir dos quais foi possível obter conclusões adaptadas à nossa população alvo.

Apesar das diversas vantagens apresentadas por alguns dos métodos mencionados, todos compartilham um problema em comum: a necessidade de modificar a aplicação ou o serviço no qual o idoso se pretende autenticar. Para superar este problema, é necessário um sistema que não seja invasivo às diversas plataformas, que consiga garantir que os utilizadores utilizam credenciais for-

tes sem se preocuparem com a possibilidade de se esquecerem das mesmas, e que não necessite de dispositivos extra para a sua utilização diária, de modo a que não haja encargos financeiros para os idosos. Sendo estas algumas das características dos gestores de palavras-passe, adaptando à faixa etária mais idosa para que a mesma não sinta dificuldades na utilização do mesmo.

Nome	Tipo	Rápida autenticação	Pensado nos idosos	Testado com idosos
HANDWING	Conhecimento		✓	✓
MUSIPASS	Conhecimento		✓	
GESTURE-BASED	Conhecimento	✓		✓
GRAPHICAL-BASED	Conhecimento	✓		✓
IMAGE-BASED	Conhecimento	✓		✓
PICO	Token/Biometria	✓		
2FA	Todos	✓		✓
PASSKEYS	Token/Biometria	✓		

Tabela 2.1: Comparação dos diversos métodos de autenticação previamente discutidos.

2.2 Gestores de Palavras-passe

Os gestores de palavras-passe têm como objetivo simplificar o processo de autenticação de forma célere e sem a necessidade de modificar a aplicação ou serviço em que o utilizador se deseja autenticar. Isto significa que os métodos de autenticação desses serviços ainda continuam a envolver as habituais *username* e palavras-passe, no entanto, a utilização de um gestor de palavras-passe elimina a obrigatoriedade de memorizar todas as credenciais, uma vez que estas são armazenadas de forma segura e de fácil acesso no respetivo gestor de palavras-passe. Adicionalmente, estes oferecem funcionalidades suplementares, como a capacidade de gerar automaticamente palavras-passe altamente seguras, preencher formulários de *login* de forma conveniente e sincronizar as credenciais entre vários dispositivos, tornando o processo de autenticação mais eficiente e seguro.

Inicialmente pode parecer contraditório considerar um gestor de palavras-passe seguro, uma vez que o utilizador coloca todas as credenciais na mesma “cesta”. Contudo, quando este está devidamente protegido, o seu uso é definitivamente uma opção superior à reutilização de palavras-passe fracas que são facilmente descobertas por potenciais atacantes. De seguida, são destacadas de forma mais detalhada as principais características que geralmente são inerentes aos gestores de palavras-passe, conferindo-lhes uma utilidade notável na proteção dos utilizadores. De realçar que nem todas as seguintes características são intrínsecas a todos os gestores de palavras-passe, visto estar dependente das implementações e políticas de cada um.

- **Segurança das credenciais:** Para que um utilizador se autentique num gestor de palavras-passe, geralmente é necessário inserir um *username* e uma palavra-passe considerada a mestra palavra-passe. Estas credenciais são as únicas que o usuário necessita de memorizar. A maioria dos gestores de palavras-passe usa a palavra-passe mestra para cifrar as restantes

credenciais do utilizador antes de armazená-las, para que seja possível interpretar as credenciais armazenadas na *Cloud*, através de diferentes dispositivos;

- **Sincronização entre diversos dispositivos:** Um utilizador consegue obter as suas credenciais para qualquer serviço através de qualquer dispositivo onde a sua conta esteja autenticada;
- **Geração de palavras-passe fortes:** Por norma, os serviços que priorizam a segurança dos seus utilizadores requerem que os mesmos escolham palavras-passe fortes, com diferentes tipos de caracteres. Os gestores de palavras-passe conseguem ajudar os utilizadores a gerarem sequências únicas e que cumpram todos os requisitos desejados, sem grande esforço;
- **Assistência a inserir credenciais:** Possibilitam mecanismos para se preencher as credenciais em determinado serviço, sem a necessidade de escreverem manualmente as mesmas.

Uma vez que a principal solução passa por desenvolver um gestor de palavras-passe, é importante voltar a referir que essas ferramentas são frequentemente consideradas desafiadoras para os idosos. Assim sendo, conduziu-se uma minuciosa pesquisa com o intuito de analisar qual é o estado atual dos gestores de palavras-passe, procurando averiguar se existe alguma solução desenvolvida para a faixa etária em questão. De seguida é apresentado um conjunto de gestores de palavras-passe que agrupam recursos projetados para serem mais acessíveis e que facilitem o seu uso por parte dos utilizadores que necessitam da solução apresentada, soluções estas que indiretamente podem ser benéficas para os idosos, pois, até ao momento, não existe nenhum gestor de palavras-passe projetado especificamente para responder às necessidades desta faixa etária.

- **Tapas:** O TAPAS [33] foi desenvolvido com o principal objetivo das credenciais se encontrarem apenas armazenadas em dispositivos do utilizador, e sem a necessidade de uma palavra-passe mestra. Esta solução passa por armazenar as credenciais cifradas no telemóvel do utilizador e a chave que foi utilizada para as cifrar, no computador do mesmo, sendo que é necessário os dois dispositivos comunicarem para que as credenciais sejam legíveis. A principal ideia resolve um dos receios dos idosos, que corresponde ao facto das suas credenciais se encontrarem “guardadas algures na Internet”, o que não acontece neste caso. Por outro lado, dado serem necessários dois dispositivos, este gestor de palavras-passe deixa de ser acessível para grande parte dos idosos. Para além disso, caso um dos dispositivos seja perdido, apesar dos dados não ficarem elegíveis para quem encontrar o mesmo, o idoso perde total acesso às suas credenciais, não existindo qualquer forma de re-obter as mesmas;
- **Safepass:** Uma vez que os gestor de palavras-passe atuais possuem problemas em comum, tais como a utilização de tecnologias antigas e de interfaces desatualizadas, tal levou à criação do SAFEPASS [23]. O SAFEPASS considerado pelos seus autores como um gestor de palavras-passe conveniente, portátil, seguro e moderno, que aproveita as tecnologias atuais e que funciona como um gestor de palavras-passe *Cloud-based*, o que possibilita manter a disponibilidade e sincronização dos dados em diversas plataformas. O sistema apresentado é semi-independente do *backend*, ou seja, ao contrário da maioria dos sistemas nos

quais o *backend* controla o que o utilizador vê no *frontend*, o SAFEPASS é desenhado de maneira a que o *backend* não esteja ciente da informação que está a ser enviada para ele e que o servidor principal se encontre do lado do utilizador. Embora esta solução tenha abordado alguns problemas de *design*, uma vez que os autores consideram terem construído uma aplicação com uma simples navegação e focada na qualidade e usabilidade, as imagens apresentadas pelos mesmos transmitem a ideia de que a dimensão de determinados ícones não iria beneficiar toda a população, nomeadamente a população mais idosa. Para além disso, não existem funcionalidades que tenham sido pensadas e planeadas para faixas etárias específicas, tornando-se um sistema bastante genérico;

- **Melhoria do Bitwarden:** O BITWARDEN [6], é um gestor de palavras-passe amplamente utilizado que, ao contrário da maioria, é *open-source*, o que, para além de permitir que os utilizadores mais experientes consigam analisar e entender o que é que o sistema faz com os seus dados, permite ser alvo de melhorias, como foi o caso dos autores do artigo [10]. Estes autores pesquisaram os problemas comuns enfrentados pelos utilizadores ao interagirem com as interfaces dos gestores de palavras-passe disponíveis no mercado, colocando os idosos como potenciais utilizadores. A falta de suporte, informação e dicas sobre a ferramenta foram resolvidos através de uma página de FAQs, onde apresentam algumas das perguntas mais frequentes dos utilizadores quando se encontram a utilizar estes sistemas. Outro problema considerado foi a falta de consistência em alguns elementos que interagem com os utilizadores, tais como os botões, que, visivelmente eram iguais mas possuíam comportamentos diferentes, o que levou a que tivessem que ser redesenhados pelos autores. Apesar das alterações realizadas ajudarem os idosos, a interface em geral continua a não possuir um foco principal nos idosos, uma vez que continua a possuir muita informação e letras muito pequenas. Além disso, a falta de funcionalidades pensadas em exclusivo nesta faixa etária, como é o caso da possibilidade de associar um cuidador à sua conta, de forma simples e rápida continuam a ser limitações evidentes;
- **Parent-child:** Assim como os idosos, as crianças também representam um grupo importante da nossa sociedade que requer atenção especial, e é para este público que o gestor de palavras-passe PARENT-CHILD [24] está direcionado. Estes grupos etários, diferem significativamente dos adultos, o que significa que os mecanismos de autenticação preparados para adultos, geralmente, não são adequados para o resto da população. Os autores apresentam um gestor de palavras-passe que concede aos pais total controlo sobre as plataformas nas quais os seus filhos se podem autenticar, bem como a capacidade de gerir as credenciais e estabelecer horários para o acesso a determinadas plataformas. Esta abordagem é fundamental para as crianças, uma vez que estas muitas vezes não têm a capacidade de avaliar os riscos da segurança *online*. Os testes conduzidos pelos autores revelaram que o gestor de palavras-passe desenvolvido foi amplamente aceite graças às funcionalidades específicas implementadas. Esses resultados destacam a importância de criar soluções de autenticação personalizadas para diferentes faixas etárias, reconhecendo as suas necessidades e parti-

cularidades. Os resultados deste sistema sugerem que criar sistemas preparados para uma população específica, não melhora apenas a segurança, mas também torna a experiência *online* mais acessível e conveniente para todos os utilizadores.

Outros gestores de palavras-passe, embora não focados nas necessidades dos idosos, devem ser considerados por estarem ativamente disponíveis no mercado. Atualmente, os mais populares são o NORDPASS [38], 1Password [1], KEEPER [30], ROBOFORM [45], BITWARDEN [6], e DASHLANE [16]. Todos estes gestor de palavras-passe oferecem funcionalidades essenciais, como a geração e avaliação das credenciais. No entanto, alguns destacam-se pela sua interface moderna e amigável, como é o caso do NORDPASS [38], 1PASSWORD [1], KEEPER [30] e DASHLANE [16]. Com a orientação de um familiar que explique algumas particularidades destes sistemas, estas opções podem ser utilizadas pelos idosos que desejam explorar novas tecnologias, apesar de que, sendo gestores de palavras-passe pensados no público em geral, os mesmos contêm ícones que não são auto explicativos, bem como letras pequenas, interfaces com demasiada informação e funcionalidades cuja finalidade não é clara. Estes problemas são claramente obstáculos que os idosos vão enfrentar e que facilmente os levam a desistir da plataforma em questão.

A capacidade de compartilhar credenciais com terceiros é uma funcionalidade comum na maioria dos gestor de palavras-passe mencionados. Contudo, para além de não serem funcionalidades gratuitas, revelam-se pouco intuitivas para os idosos, uma vez que não constituem soluções simples e diretas em relação ao seu propósito. Isto ocorre devido à complexidade de configuração elevada, o que dificulta a adesão por parte dos idosos. Apesar dos avanços alcançados, nenhum deles foi concebido tendo como prioridade as necessidades dos idosos. Esta lacuna identificada no mercado sugere uma oportunidade para o desenvolvimento de um gestor de palavras-passe específico e pensado ao detalhe para esta faixa etária. No Capítulo 3 são apresentados os requisitos que foram incluídos no nosso sistema, de modo a tornar este gestor de palavras-passe o mais fácil de utilizar possível para a faixa etária em questão.

2.3 Secret Sharing

Um dos principais desafios associados às palavras-passe atuais consiste na complexidade de determinar como proceder à proteção das credenciais dos utilizadores. Frequentemente, os sistemas recorrem à palavra-passe que o utilizador utiliza para desbloquear o gestor de palavras-passe, sendo conhecida por palavra-passe mestra, para cifrar todas as restantes credenciais pessoais guardadas. Embora, seja imperativo, por motivos de segurança, que a palavra-passe mestra não deve ser compartilhada, surge a preocupação de que, em situações de esquecimento ou em eventos infortunados, como perda de capacidades ou óbito (situações frequentes na faixa etária em questão), a recuperação das credenciais se torne um desafio insuperável. Neste contexto, um algoritmo *Secret Sharing* oferece uma solução eficaz. Este algoritmo criptográfico foi criado de forma concorrente entre Shamir [47] e Blakley [7] em 1979. Posteriormente novos algoritmos com o mesmo fim acabaram por ser apresentados como o de Karpin, Greene e Hellman [29] em 1983.

Os algoritmos *Secret Sharing*, permitem que uma chave secreta s (sendo um exemplo desta chave a palavra-passe mestra) seja fragmentada em n peças distintas, denominadas por *shares*. Cada um dos *shares* possui informação suficiente para obter a chave s , desde que se junte num conjunto de t *shares* distintos. Este t é conhecido como o *quorum*, representando o número mínimo de partes necessárias para reconstruir o segredo. A Figura 2.1 apresenta a chave s que é assim fragmentada em 3 *shares* distintos ($n=3$), e que todos os diferentes *quorums* de 2 *shares* ($t=2$) possuem informação suficiente para reconstruir a chave inicial s . Este algoritmo permite não estar apenas dependente de um utilizador para obter o segredo, ou seja, se um deles se esquecer da chave, é sempre possível recorrer aos outros dois. Para além de não se estar somente dependente de uma chave, o facto de não ser necessário partilhar a chave principal para proceder à criptografia é uma outra grande vantagem que será um fator crucial no nosso projeto. A simplicidade do algoritmo *Secret Sharing* desenvolvido por Shamir, é uma das muitas características que o leva a continuar a ser bastante adotado. A Figura 2.2 apresenta, de forma sucinta, como é que este algoritmo baseado em polinómios, permite a partir de, pelo menos, dois pontos (denominados de *shares*) obter o segredo, a chave s , que corresponde a um ponto no eixo do y .

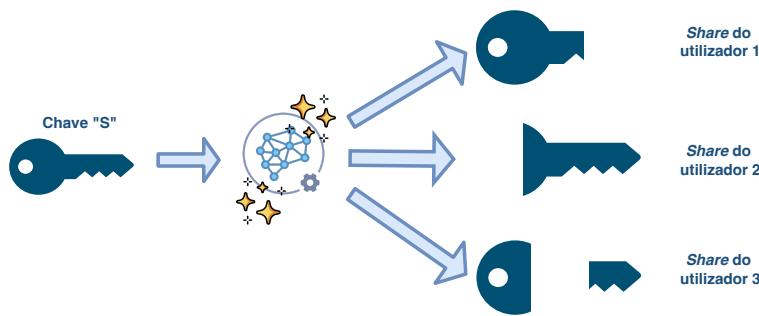


Figura 2.1: Esquema de funcionamento do *Secret Sharing* (SS) (melhor visto a cores).

Ao ser escolhido o segredo, representado pelo ponto laranja, é originado um outro ponto aleatório, o ponto cinza, que possibilita a formalização de uma reta, ou seja, um polinómio de grau 1. Os *shares*, são essencialmente todos os pontos que se encontram na reta secreta, com exceção do segredo, e são visualmente representados pelos pontos verdes. Vale ressaltar que o ponto cinza também pode ser considerado um *share*, uma vez que também é um ponto aleatório do mesmo polinómio. Com a combinação de dois destes pontos, e ao recorrermos à equação da reta de polinómio de grau 1, $y = mx + b$, possuímos informação suficiente para retraçar a reta secreta, e obter o segredo, que, tal como já referido, é a intersecção da reta com o eixo do y . O *Secret Sharing* é amplamente utilizado em cenários de segurança, incluindo a distribuição segura de chaves criptográficas e a proteção de informações confidenciais, garantindo que o acesso seja controlado e restrito a indivíduos autorizados. Estes factos são particularmente úteis em sistemas cujo objetivo é manter as informações cifradas e acessíveis a mais do que uma pessoa, sem compartilhar diretamente a chave principal. Também simplifica a obtenção de *backups* das credenciais,

caso seja necessário, uma vez que não há dependência exclusiva de uma única chave.

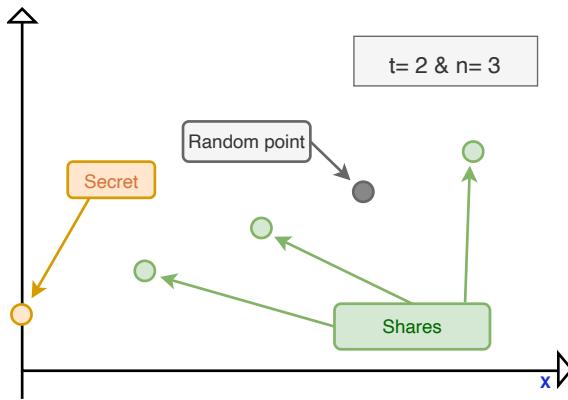


Figura 2.2: Algoritmo *Secret Sharing* de Shamir com $t=2$ & $n=3$ (melhor visto a cores).

2.4 Sumário

Neste capítulo, categorizamos os métodos de autenticação existentes, classificados em três categorias: baseados em conhecimento, em *tokens* e em biometria. Em seguida, analisamos os métodos de autenticação dentro dessas categorias que poderiam beneficiar a população idosa. Embora estes métodos tenham simplificado o processo de autenticação, apresentaram desvantagens significativas, como a demora do processo, a exigência de dispositivos com ecrãs maiores ou a necessidade de adquirir dispositivos adicionais, algo que os idosos frequentemente evitam devido aos custos envolvidos. Prosseguimos com a análise dos gestores de palavras-passe como uma potencial solução, destacando-se a vantagem de não requerer modificações nas aplicações ou serviços onde o utilizador se autentica, nem de alterar o modelo mental de autenticação presente nos mesmos. Foram examinados alguns gestores de palavras-passe desenvolvidos para resolver problemas comuns, como interfaces desatualizadas e a falta de suporte para utilizadores vulneráveis. No entanto, concluiu-se que essas soluções ainda eram insuficientes para atender às necessidades dos idosos. Posteriormente, realizamos a análise dos gestores de palavras-passe disponíveis no mercado, verificando-se que nenhum estava adequadamente preparado para a população idosa, pois foram desenvolvidos com foco em utilizadores mais experientes e familiarizados com tecnologia. Finalmente, explicamos o algoritmo *Secret Sharing*, uma componente crucial do sistema desenvolvido, que permite possibilitar a recuperação segura das credenciais dos idosos.

Capítulo 3

Levantamento de Requisitos

Este capítulo apresenta os requisitos considerados durante o desenvolvimento do sistema, que é composto por duas aplicações – uma para os idosos e outra para os seus cuidadores informais – e por dois servidores, conforme detalhado no Capítulo 4. Os requisitos são divididos em duas categorias: requisitos funcionais, que descrevem o comportamento do sistema do ponto de vista dos utilizadores, e requisitos não funcionais, que se referem a qualidades como a segurança dos dados. Estes requisitos foram obtidos a partir das necessidades dos idosos identificadas na literatura (representada pelo número 1 da Figura 3.1) e das avaliações heurísticas realizadas com um perito e com o público-alvo (representadas pelos números 5 e 7), seguindo uma abordagem de *design* centrado no utilizador [9] com prototipagem iterativa [4]. As avaliações heurísticas encontram-se detalhadas no Capítulo 6.

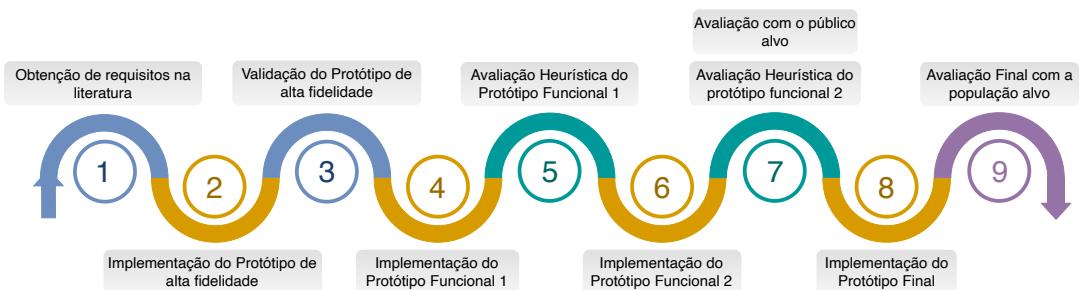


Figura 3.1: Fluxo do projeto (melhor visto a cores).

3.1 Requisitos Funcionais

Perfis de Credenciais: Um perfil de credencial contém as informações necessárias para o acesso a uma conta. O sistema disponibiliza dois tipos de perfis: “Login” e “Cartão”. Os perfis “Login” incluem dados para aceder a contas *online*, como o nome da plataforma, utilizador, palavra-passe e *URL*. Já os perfis “Cartão” contêm informações para a utilização de um cartão, como nome, proprietário, número do cartão, PIN e código de verificação. Todos os perfis podem ser atualizados, ficando registado quem fez a última alteração, ou eliminados caso deixem de ser úteis.

Auto preenchimento do campo plataforma e URL: O sistema permite que o utilizador, ao sele-

cionar a plataforma para a qual pretende adicionar uma nova credencial, o campo *URL* e o nome da plataforma sejam preenchidos automaticamente, facilitando a experiência do utilizador.

Termos “utilizador” e “palavra-passe” adaptáveis: Atualmente, termos como “utilizador” e “palavra-passe” são comuns em vários sistemas. No entanto, algumas plataformas usam e-mail ou número de telemóvel como identificador e podem substituir “palavra-passe” por “PIN” ou outros termos. No nosso sistema, os campos “utilizador” e “palavra-passe” são adaptados conforme a plataforma escolhida pelo utilizador.

Vinculação e Desvinculação do cuidador: O sistema permite que o idoso se vincule ao seu cuidador informal e vice-versa, facilitando a assistência na gestão das credenciais. Além disso, é possível tanto o idoso como o cuidador realizar a desvinculação de uma relação.

Permissões dos cuidadores: O sistema oferece flexibilidade, permitindo que o idoso escolha os direitos a conceder a cada cuidador. O idoso pode optar por permitir apenas a visualização das suas credenciais ou conceder direitos para criar, editar e apagar credenciais.

Número de relações: O sistema foi concebido de modo a permitir que um idoso possa vincular-se, no máximo, a dois cuidadores, e que um cuidador possa vincular-se a até quatro idosos. Estes limites foram estabelecidos com o intuito de proporcionar um apoio mais abrangente aos idosos, sem comprometer a consistência e a segurança dos mesmos.

Rejeição automática: Quando um idoso ou cuidador recebe um pedido de vinculação e o limite de relações já foi atingido, o pedido é automaticamente recusado, e ambas as partes são notificadas. Se um utilizador tem dois pedidos pendentes e só pode aceitar um, ao aceitar um pedido, todos os restantes são automaticamente recusados e ambas as partes notificadas.

Notificações: O sistema notifica os idosos sobre alterações nas suas credenciais ou, no caso dos cuidadores, nas credenciais dos idosos sob os seus cuidados. Além disso, os utilizadores são avisados sobre alterações nos dados pessoais de pessoas com quem estão vinculados, bem como sobre novos pedidos de vinculação ou desvinculações.

Avaliação das palavras-passe escolhidas: O sistema avalia a força da palavra-passe escolhida pelo utilizador para aumentar a sua confiança. O resultado da avaliação é apresentado através de um componente que usa uma escala com cores e ícones para facilitar a interpretação.

Alteração dos dados pessoais: Além das credenciais, os utilizadores podem atualizar os seus dados pessoais após a criação da conta. As atualizações são então enviadas aos utilizadores vinculados para garantir a consistência dos dados de contacto.

Página de tutoriais FAQs, e sugestões: O sistema inclui uma página de ajuda com três secções, disponível em ambas as aplicações. A primeira secção apresenta uma lista de perguntas frequentes com as respetivas respostas. A segunda inclui tutoriais em formato escrito e em vídeo que explicam como realizar diversas tarefas. A terceira secção oferece sugestões para a gestão das credenciais.

Gerador de palavras-passe fortes: O sistema permite gerar palavras-passe fortes que cumpram requisitos específicos, como tamanho e inclusão de caracteres variados. Além disso, permite aceder às últimas palavras-passe geradas pelo utilizador através desta funcionalidade.

Lembrete diário: Ambas as aplicações incluem um lembrete diário que apresenta uma mensagem sobre boas práticas na gestão de credenciais e a importância do sistema. Este lembrete é exibido diariamente através do *Splash Screen* das aplicações.

Credenciais dos cuidadores: Para maximizar a adesão dos cuidadores, a aplicação permite-lhes, além de se vincularem aos idosos e auxiliarem na gestão das suas credenciais, armazenar e gerir também as suas próprias credenciais.

Interface projetada para idosos: Dado que o sistema se destina principalmente a idosos, todo o *design*, incluindo textos, botões e animações acionadas pelas ações do utilizador, foi desenhado com ênfase na facilidade de identificação e interpretação.

Fácil aprendizagem: No sistema desenvolvido, as tarefas foram projetadas com um número reduzido de passos, para facilitar a memorização e a repetição futura das mesmas.

Rápida apresentação das credenciais: O sistema armazena as credenciais, tanto na *Cloud* como localmente no dispositivo do respetivo proprietário. Esta replicação reduz substancialmente o tempo de apresentação das mesmas ao utilizador.

Diferentes sistemas operativos móveis: Embora os idosos utilizem predominantemente o sistema operativo *Android*, ambas as aplicações foram desenvolvidas para serem compatíveis com os dois sistemas operativos, *Android* e *iOS*.

3.2 Requisitos Não Funcionais

Não partilhar a totalidade da chave criptográfica: O sistema permite que o cuidador interprete as credenciais do idoso armazenadas na *Cloud* sem necessitar de armazenar a totalidade da chave criptográfica, guardando apenas parte da mesma localmente no seu dispositivo. Este requisito é viabilizado pelo algoritmo *Secret Sharing*.

Rotatividade da chave criptográfica: De forma a aumentar a resiliência contra ataques e reduzir o risco de comprometimento da chave criptográfica utilizada para cifrar as credenciais que se encontram na *Cloud*, o sistema incorpora um mecanismo que permite substituir a chave criptográfica ao fim de determinado tempo.

Validação das credenciais presentes na Cloud: Para garantir que as credenciais na *Cloud* sejam iguais às armazenadas localmente, o sistema realiza uma sincronização periódica, atualizando-as caso detete alguma alteração ou remoção indevida, seja localmente ou na *Cloud*.

Operação de soft-delete para os cuidadores: Para distinguir uma operação de *delete* realizada por um cuidador de uma eliminação indevida na *Cloud*, o sistema não permite que o cuidador

apague completamente a credencial de um idoso. Em vez disso, o cuidador realiza um *soft-delete*, que consiste em atualizar a credencial, limpando todos os campos. A eliminação final é feita automaticamente pela aplicação do idoso.

Os cuidadores não armazenam localmente as credenciais do idoso: No sistema as credenciais dos idosos não são armazenadas localmente nos dispositivos dos cuidadores, sendo apenas armazenadas nos dispositivos dos idosos e na *Cloud*. Este requisito permite restringir o risco de acessos não autorizados após possíveis desvinculações.

Dados localmente armazenados, encriptados: Ambas as aplicações armazenam localmente dados sensíveis, como credenciais pessoais e informações sobre a sessão estabelecida com o protocolo *Signal*. Estes dados devem ser protegidos de forma a garantir que, mesmo que alguém acceda à memória interna do telemóvel, permaneçam ilegíveis.

Chaves armazenadas em cofre: Ambas as aplicações possuem chaves que devem ser devidamente protegidas. Para tal, as aplicações utilizam as *APIs Keychain* do respetivo sistema operativo para armazenar esses dados.

Backup das credenciais dos idosos: Os idosos ao estabelecerem relações com os cuidadores, beneficiam da possibilidade de utilizar as contas destes como *backup* em situações adversas, como a perda total de acesso à conta, seja por esquecimento das credenciais ou pela perda do dispositivo.

3.3 Sumário

Neste capítulo, apresentamos os requisitos estabelecidos para o projeto, obtidos principalmente da literatura existente e das avaliações heurísticas. Estes requisitos foram divididos em duas categorias: funcionais e não funcionais. Os requisitos funcionais referem-se ao comportamento do sistema do ponto de vista do utilizador, incluindo a vinculação e desvinculação de cuidadores, as permissões atribuídas a eles, as notificações, a interface projetada para idosos e a compatibilidade com diferentes sistemas operativos. Os requisitos não funcionais referem-se a qualidades do sistema que não são visíveis para o utilizador, mas são cruciais para garantir a segurança dos dados. Exemplos incluem a não partilha integral da chave criptográfica, a sua rotatividade, a validação das credenciais armazenadas na *Cloud*, a encriptação dos dados e o *backup* das credenciais dos idosos.

Capítulo 4

Desenho da Solução

Neste capítulo, detalham-se os componentes do sistema, as suas necessidades e relevância, bem como os fluxos de operações nas aplicações móveis e as interações entre os diferentes componentes. As Secções 4.2.2 e 4.3 incluem ilustrações para clarificar esses fluxos. O capítulo também aborda considerações essenciais para garantir a segurança da identidade dos utilizadores e a integridade dos dados.

4.1 Arquitetura do Sistema

Com base nos requisitos apresentados no Capítulo 3, apresentamos na Figura 4.1 a arquitetura do sistema proposta para que estes sejam cumpridos. A arquitetura é constituída por duas aplicações móveis distintas, e por dois servidores, o Servidor Intermédio que gera a comunicação entre duas aplicações, e o Servidor de Autenticação e Armazenamento, responsável pela autenticação e armazenamento. Na comunicação entre os componentes, existem dois tipos de comunicação disponíveis. *Hypertext Transfer Protocol* (HTTP), utilizado para enviar e obter dados armazenados nos servidores, representado pelos números 1, 2, 3, e *WebSocket*, necessário para comunicação bidirecional em tempo real, representado pelos números 4 e 5.

4.1.1 Aplicações móveis

O sistema conta com duas aplicações móveis, uma para os idosos e outra para os cuidadores. Cada uma das aplicações foi construída de modo a possuir todas as funcionalidades necessárias tendo em conta os requisitos do sistema. Através da comunicação entre a aplicação do cuidador e do idoso são trocados os dados pessoais de cada membro de uma relação (nomes e dados telefónicos). Todos estes dados são armazenados, exclusivamente, nos dispositivos dos utilizadores envolvidos, e nunca num servidor. Ambas as aplicações permitem a atualização dos dados pessoais do respetivo utilizador, sendo que após cada atualização, estes são enviados aos utilizadores vinculados, acompanhados de uma notificação. Os utilizadores são notificados sempre que ocorre uma alteração nas credenciais do idoso. Se um cuidador atualizar as credenciais, o idoso é informado; da mesma forma, se o idoso atualizar as suas credenciais, os cuidadores vinculados são notificados. De modo a garantir a privacidade dos dados pessoais transmitidos

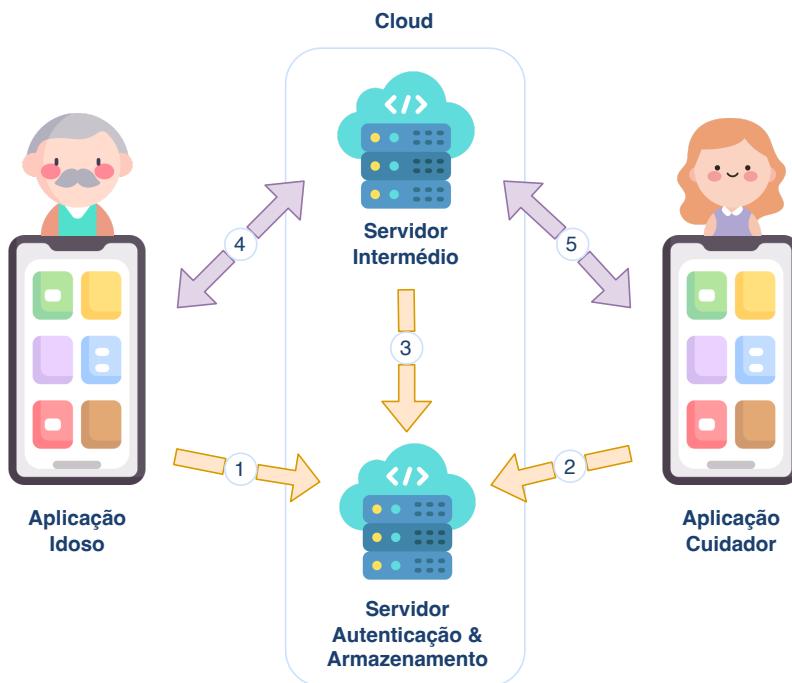


Figura 4.1: Arquitetura do sistema (melhor visto a cores).

entre as aplicações, bem como as notificações que são enviadas, que por vezes podem transportar informações sensíveis, implementá-mos a criptografia ponto a ponto na comunicação entre as aplicações, juntamente com metodologias apropriadas para assegurar os princípios fundamentais de proteção de dados, incluindo confidencialidade, integridade e autenticidade na comunicação entre as duas aplicações. Será também na comunicação entre as duas aplicações, que parte das informações necessárias para permitir que os cuidadores accedam às credenciais dos seus idosos, armazenadas na *Cloud*, será transmitida, nomeadamente o *share* que será atribuído ao cuidador e armazenado na sua aplicação.

Ambas as aplicações utilizam duas metodologias distintas para armazenar os dados localmente, nomeadamente a *KeyChain* do sistema operativo e uma base de dados *SQLite*. Estas abordagens foram escolhidas devido às suas capacidades de gestão de dados sensíveis e estruturados.

A *KeyChain* do sistema operativo é utilizada para armazenar os dados mais sensíveis da aplicação, nomeadamente todas as chaves criptográficas. Estas chaves são usadas para cifrar os dados presentes na base de dados relacional, que será explicada em seguida, bem como para cifrar os dados armazenados na *Cloud* e para realizar a comunicação segura entre as aplicações.

A base de dados relacional *SQLite* é utilizada para armazenar dados que não podem ser representados numa base de dados chave-valor, necessitando de uma estrutura com atributos que possam possuir diversos tipos, sobre os quais seja possível realizar *queries*, de acordo com as funcionalidades e requisitos da aplicação. A base de dados relacional de ambas as aplicações é composta por cinco tabelas, representadas na Figura 4.2. A tabela “credencial” é utilizada para armazenar as credenciais pessoais do utilizador em questão, a tabela “palavra-passe” é usada,

exclusivamente, para guardar o histórico das palavras-passe geradas, a tabela “timeout” permite manipular os tempos de execução de algumas tarefas da aplicação, como a rotatividade e o *Splash Screen*, a tabela “sessão” guarda o objeto que representa uma vinculação, que é explicado na secção 4.2.2 e, por último, a tabela “relação“ contém os dados pessoais e o estado das relações estabelecidas.

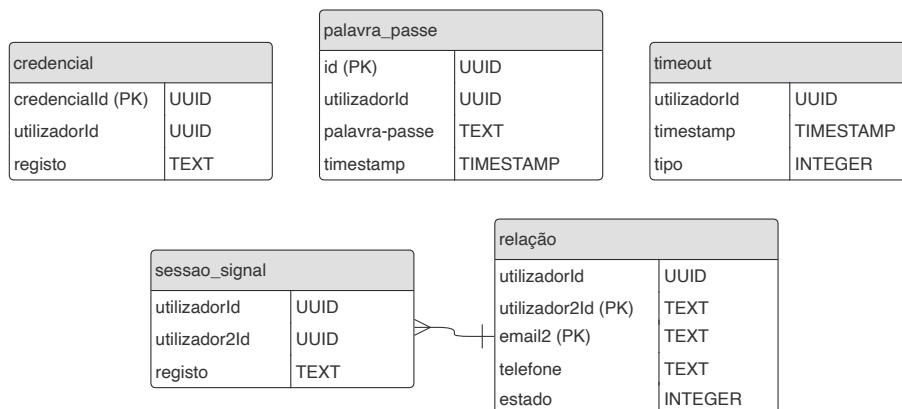


Figura 4.2: Base de dados relacional das aplicações móveis.

4.1.2 Servidor Intermédio

O Servidor Intermédio é crucial devido à limitação dos endereços privados atribuídos aos dispositivos móveis dos utilizadores. Sem este intermediário, as aplicações dos idosos não estariam acessíveis para as aplicações dos cuidadores e vice-versa. Por outras palavras, não era possível uma comunicação direta entre ambas as aplicações sem a existência de um intermediário.

O Servidor Intermédio permite a entrega de mensagens mesmo quando um dos utilizadores não está *online*, pois armazena temporariamente essas mensagens encriptadas, que apenas o destinatário pode decifrar. Sem este intermediário, seria necessário que ambas as aplicações estivessem *online* para garantir a entrega de todas as mensagens. Quando o receptor se conecta, o Servidor Intermédio entrega as mensagens pendentes, e, posteriormente, apaga os dados correspondentes. Por fim, um aspeto crucial do servidor é a sua capacidade de validar se um utilizador está a tentar fazer-se passar por outro, uma validação que é detalhada na secção 4.2.2.

Posto isto, o Servidor Intermédio é essencial para permitir que as duas aplicações troquem informação de forma segura. Além disso, este servidor é importante para que as aplicações possam despoletar notificações do tipo *push notifications* quando alguma ação realizada por um membro com quem esteja vinculado tenha sido realizada sobre dados sobre os quais também tenha acesso.

Adicionalmente, é neste servidor que os *bundles*, peças fundamentais para a encriptação ponto a ponto, são armazenados e obtidos por terceiros que queiram estabelecer uma relação. Outra vantagem do Servidor Intermédio é a capacidade de identificar quais utilizadores são cuidadores e quais são idosos, proibindo assim que utilizadores de iguais categorias se vinculem.

4.1.3 Servidor de Autenticação e Armazenamento

Este servidor tem como principais objetivos autenticar os utilizadores e armazenar informação, nomeadamente as credenciais e os *shares* que os cuidadores vão necessitar para interpretar as credenciais dos seus cuidadores. Através do mesmo, garantimos que as credenciais dos idosos não se encontram armazenadas nos dispositivos locais dos cuidadores. Esta condição obriga a que um cuidador necessite sempre de aceder a este para obter as credenciais mais recentes. Para além disso, em situações adversas, como a perda de acesso à conta pelo idoso ou mesmo a perda do dispositivo, o armazenamento neste servidor permitirá que as contas dos cuidadores funcionem como *backup* das credenciais dos idosos, evitando a perda irreparável destas. Será também neste servidor que as regras de quem tem acesso e de quem pode manipular as credenciais estarão definidas, sendo estas apenas alteráveis pelo proprietário dessas credenciais. Esta abordagem oferece um maior controlo em situações de desvinculação, dado que a obtenção das credenciais pelos cuidadores requer sempre o acesso ao servidor. Por outras palavras, se um cuidador for desvinculado e tentar aceder ao servidor para ler as credenciais do idoso que o desvinculou, o acesso será negado. Uma vez que o cuidador apenas possui armazenada na sua aplicação parte da chave criptográfica, ou seja, o seu *share*, este terá que obter a restante informação para conseguir decifrar as credenciais. É neste sentido que o servidor volta a ter um papel fundamental, será a componente externa, através da qual o cuidador irá obter os elementos complementares necessários para a leitura das credenciais dos seus idosos.

A estrutura da base de dados implementada no Servidor de Autenticação e Armazenamento, representada na Figura 4.3, é composta por três coleções principais, para os dados dos idosos (1), dos cuidadores (2), e do Servidor Intermédio (3).

Cada documento da coleção 1 (dados dos idosos) é composto por várias sub-coleções. Estas incluem: as credenciais do respetivo utilizador, uma sub-coleção contendo *Salts* utilizados para gerar as chaves criptográficas a partir da palavra-passe mestra (necessários para a regeneração dessas chaves), uma sub-coleção com os identificadores dos cuidadores e respetivas permissões de acesso, e, por fim, uma sub-coleção que armazena o *share* necessário para que os cuidadores possam reconstruir a chave criptográfica. Relativamente à coleção 2 (dados dos cuidadores), é composta por uma sub-coleção Credenciais, igual à dos idosos, como pela sub-coleção que representa os *Salt* para regenerar as chaves criptográficas. Por último, a coleção 3 (dados do Servidor Intermédio) possui um único documento, acessível por qualquer utilizador do sistema, onde os mesmos podem obter o endereço deste servidor.

No seguimento da estrutura da base de dados do Servidor de Autenticação e Armazenamento, é necessário estabelecer regras de acesso que respeitem a arquitetura definida. Todas as coleções possuem uma regra comum: é imprescindível que o utilizador se encontre autenticado para ler ou alterar qualquer dado nesta base de dados.

Relativamente à coleção com os dados dos idosos, representada na Figura 4.3 com o número 1, as regras de acesso são específicas. Na sub-coleção *Salts*, somente o idoso em questão pode ler ou modificar os dados. Quanto à sub-coleção Cuidadores, os cuidadores podem ler os dados apenas se

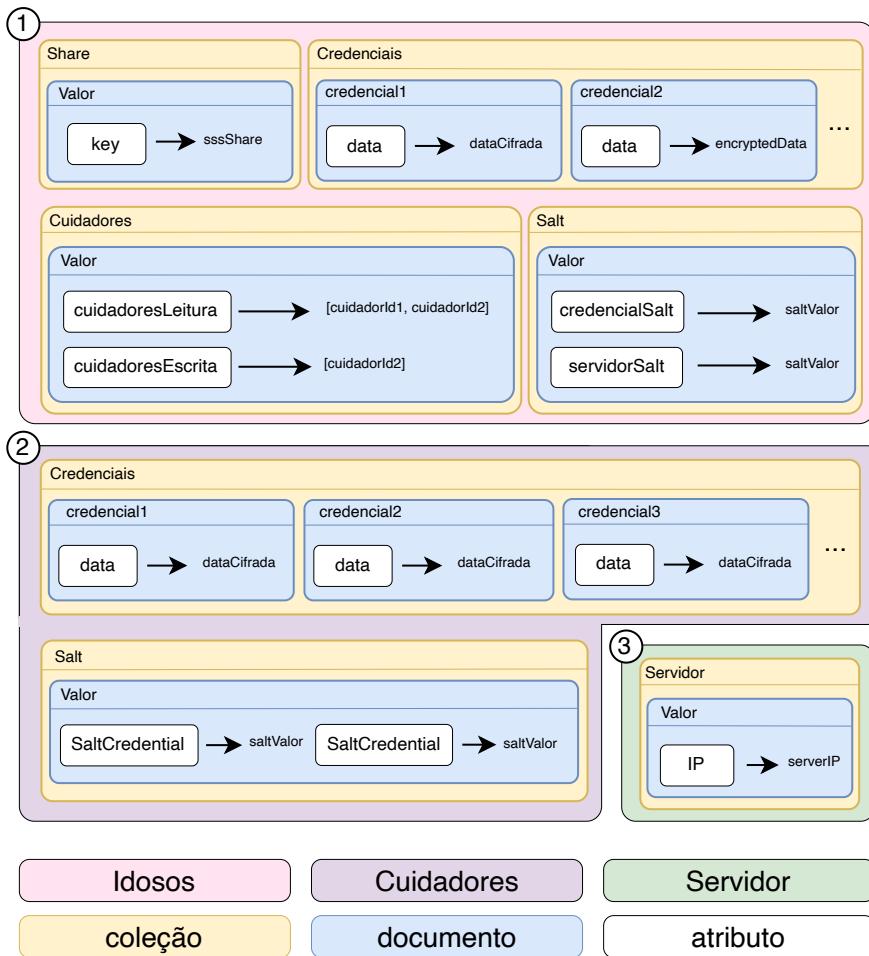


Figura 4.3: Estrutura do Servidor de Autenticação e Armazenamento (melhor visto a cores).

o seu ID estiver presente no *array* de cuidadores com acesso de leitura, sendo que esta sub-coleção é manipulável, exclusivamente, pelo idoso. Na sub-coleção Credenciais, o idoso pode ler, editar e apagar as credenciais a qualquer momento, enquanto os cuidadores podem realizar a operação de leitura caso o seu ID se encontre no *array* de leitores e apenas podem modificar os dados se o seu ID estiver no *array* de cuidadores com permissões de escrita. Os cuidadores, mesmo com permissões de escrita, e mesmo que realizem a operação de apagar uma credencial do idoso, esta credencial não é diretamente apagada do Servidor de Autenticação e Armazenamento, uma vez que apenas o respetivo proprietário da credencial a consegue apagar. Esta operação é explicada em detalhe na Secção 4.3.10. Na sub-coleção Share, o idoso pode realizar todas as operações, enquanto os cuidadores listados no *array* com permissões de leitura apenas podem ler os dados presentes.

Para a coleção 2, que corresponde aos dados dos cuidadores, as regras são idênticas. Tanto a sub-coleção Credenciais como a sub-coleção Salts podem ser lidas e manipuladas, exclusivamente, pelo cuidador proprietário. A coleção 3, pertencente ao Servidor Intermédio, pode ser alterada apenas pelo próprio, sendo necessário possuir uma chave de administrador para realizar qualquer operação sobre esta coleção.

4.2 Segurança

Esta secção inicia-se com a descrição do modelo de adversário, detalhando o seu possível poder, seguida pela apresentação dos diversos mecanismos de segurança incorporados no nosso sistema.

4.2.1 Modelo de Adversário

No modelo adversário, consideramos um cenário em que os ataques podem ser realizados por um atacante passivo. No que toca à rede, assumimos que o atacante controla a rede na qual ocorre a comunicação entre as aplicações e os servidores. Quanto aos dados sensíveis que se encontram em ambos os servidores, assumimos que um possível atacante consiga ter acesso aos dados que nestes se encontram. Relativamente aos dados que se encontram armazenados localmente nos dispositivos móveis, um atacante não tem qualquer acesso a estes.

4.2.2 Mecanismos de Segurança

Nesta secção, abordam-se as medidas de segurança dos dados dos utilizadores, destacando as metodologias adotadas para garantir a confidencialidade, autenticidade, e integridade de todos os dados armazenados e partilhados entre os utilizadores. São também evidenciados alguns aspectos no que toca aos acessos dos atacantes, e o que se fez para se proteger destes.

Autenticação: O processo de autenticação permite à aplicação validar a identidade do utilizador, garantindo que determinado utilizador apenas consegue aceder aos dados sobre os quais possui direitos de leitura. Além da autenticação no acesso à aplicação e na obtenção de dados do Servidor de Autenticação e Armazenamento, o sistema também valida a autenticidade das mensagens enviadas para o Servidor Intermédio quando este deseja realizar qualquer alteração nos dados armazenados neste. Esta validação é possível porque, quando um utilizador comunica pela primeira vez com o Servidor Intermédio, este envia uma chave pública, que será utilizada pelo servidor para validar futuras atualizações feitas por esse utilizador. Esse mecanismo assegura que nenhum utilizador consiga roubar a identidade de outro ou modificar dados no Servidor Intermédio que não lhe pertençam.

Comunicação: No sistema, tal como explicado na Secção 4.1, existem três possíveis relações de comunicação entre entidades distintas: a comunicação entre a aplicação (tanto do cuidador como do idoso) e o Servidor de Autenticação e Armazenamento, a comunicação entre ambos os servidores, ou seja, entre o Servidor de Autenticação e Armazenamento e o Servidor Intermédio, e a comunicação entre ambas as aplicações (a do cuidador e a do idoso). Esta última, conforme já referido, requer o Servidor Intermédio para ser realizada, sendo composta por duas sub comunicações, entre cada uma das aplicações e o Servidor Intermédio. Nas comunicações entre o Servidor de Autenticação e Armazenamento e as aplicações, recorre-se ao protocolo *Transport Layer Security* (TLS) cujos esquemas criptográficos são *Rivest–Shamir–Adleman*(RSA) e *Advanced Encryption Standard — Galois/Counter Mode* (AES-GCM) para a criptografia assimétrica e simétrica, respetivamente. A comunicação entre as aplicações e o Servidor Intermédio, também recorremos

ao mesmo protocolo, com os mesmos esquemas criptográficos. Por sua vez, é necessário que a comunicação entre as aplicações do cuidador e do idoso seja cifrada ponto a ponto, dado que as mensagens passam pelo Servidor Intermédio, e, por vezes, ficam armazenadas neste, mesmo que temporariamente. Para que esta proteção seja possível, recorremos ao protocolo criptográfico *Signal*, que assegura comunicações seguras e privadas através de criptografia de ponta a ponta. Este protocolo utiliza a técnica de *Ratcheting Forward Secrecy*, uma vez que as chaves de sessão utilizadas para cifrar os dados trocados são atualizadas a cada mensagem que é enviada entre os utilizadores. Para que uma sessão seja estabelecida, primeiramente as aplicações geram um conjunto composto por chaves públicas, ao qual é denominado por *bundle*, e guardam localmente as chaves privadas também derivadas deste processo. Quando um utilizador pretende estabelecer uma sessão com outro utilizador, este recorre ao Servidor Intermédio para obter o *bundle* do destinatário, e, através da junção das suas chaves privadas geradas no processo de criação do seu *bundle*, com as chaves públicas presentes no *bundle* do destinatário, é gerada a sessão. Uma sessão é um objeto armazenado localmente no dispositivo do utilizador, devidamente cifrado, e contém dados sobre a vinculação, como o número de sequência da mensagem, as chaves de sessão utilizadas, as chaves de confirmação das mensagens, que garantem a consistência e segurança das chaves de sessão, além de informações como *Hash-based Message Authentication Codes* (HMACs), que são aplicados às mensagens para assegurar que estas não foram alteradas durante o envio. Caso uma aplicação receba uma mensagem, que, por alguma razão, tenha sido alterada e tornada inválida, essa mensagem é descartada pela aplicação. Todas estas considerações têm como objetivo garantir que, mesmo que um atacante consiga obter as comunicações realizadas entre os diversos componentes, não conseguirá comprometer as mensagens.

Armazenamento: De seguida, abordamos como é que os dados são armazenados no sistema devidamente protegidos, tanto aqueles que se encontram armazenados localmente nas aplicações como nos servidores. Relativamente aos dados armazenados localmente, as aplicações, tal como já explicado, recorrem a dois métodos para armazenar os dados, ou seja, a uma base de dados relacional *SQLlite* e à *Keychain/Keystore* do sistema operativo. Na base de dados *SQLlite*, os dados mais sensíveis, nomeadamente as palavras-passe geradas no gerador, as sessões utilizadas pelo protocolo *Signal*, e as credenciais, encontram-se cifradas com uma chave criptográfica apenas utilizada para cifrar os dados desta base de dados. Os dados que ficam armazenados na *Keychain/Keystore*, nomeadamente todas as chaves criptográficas necessárias para o funcionamento do sistema, encontram-se protegidos pelos recursos nativos de segurança dos sistemas operativos, nomeadamente no *hardware* do mesmo. Esta tecnologia assegura que as chaves não possam ser acedidas por outras aplicações instaladas, a não ser pela aplicação que originalmente armazenou as chaves. No caso do sistema operativo *iOS*, é utilizado o *Secure Enclave* para armazenar chaves de forma segura em hardware. Por outro lado, o sistema operativo *Android* recorre ao *Trusted Execution Environment* ou ao *Secure Element* para o armazenamento seguro de chaves em *hardware*. Embora se tenha assumido, durante o desenvolvimento do sistema, que um possível atacante não teria acesso aos dados armazenados nos dispositivos pessoais do utilizador, os mecanismos adicionais

apresentados ajudam a prevenir situações em que esses dados sejam de facto acedidos. Relativamente aos dados armazenados no Servidor de Autenticação e Armazenamento, estes encontram-se devidamente cifrados pela respetiva plataforma, onde as chaves utilizadas são geridas pelo mesmo sistema que a respetiva plataforma utiliza para proteger os seus próprios dados, bem como as auditorias e controlos rígidos de acesso às chaves também são aplicados. Todas as chaves utilizadas pela plataforma são cifradas com um conjunto de chaves mestras alteradas regularmente pela própria plataforma. Por sua vez, os dados mais sensíveis do nosso sistema, nomeadamente as credenciais do utilizador, são sempre cifrados nas aplicações dos utilizadores antes de serem enviados para o Servidor de Autenticação e Armazenamento, garantindo que mesmo que a segurança da própria plataforma seja quebrada, as credenciais continuam a ser totalmente imperceptíveis para os atacantes. No Servidor de Autenticação e Armazenamento também se estipula regras de segurança que, determinam quem é que pode aceder ao quê. Através destas regras, é estipulado quais cuidadores podem ler e alterar as credenciais do idoso, que o *share* partilhado pelo idoso apenas pode ser alterado pelo mesmo, mas lido por todos os seus cuidadores, e que dados como *Salts* apenas podem ser lidos e alterados pelos respetivos proprietários. Relativamente aos dados que o Servidor Intermédio armazena no Servidor de Autenticação e Armazenamento, como o seu endereço, apenas utilizadores com chave de administrador podem editar essas informações. No nosso sistema, apenas o Servidor Intermédio possui essa chave. O Servidor Intermédio também possui dados armazenados no mesmo, nomeadamente os *bundles* dos utilizadores, bem como as mensagens que se encontram pendentes de serem entregues, quando o respetivo receptor se encontra *offline*. Se um atacante tiver acesso aos dados armazenados neste servidor, ele poderá obter apenas informações públicas, como as chaves e o *bundle*, ou dados que estão devidamente cifrados. Essas garantias asseguram que os atacantes não consigam extraír informações relevantes durante a leitura. No desenvolvimento do sistema foi assumido que nenhum atacante consegue alterar qualquer dado que se encontre armazenado neste Servidor Intermédio.

Rotatividade das chaves: Esta funcionalidade permite que a chave criptográfica utilizada para cifrar as credenciais que se encontra na *Cloud*, mais precisamente no Servidor de Autenticação e Armazenamento, não seja sempre a mesma, permitindo uma maior resiliência contra atacantes que pretendam descobrir a mesma. Esta rotatividade é despoletada em três situações distintas:

- **Quando o idoso se desvincula de determinado cuidador:** É necessário gerar uma nova chave, de modo a tornar o *share* que o cuidador desvinculado possui, totalmente inutilizável;
- **Quando um cuidador se desvincula de um idoso:** Quando a aplicação do idoso é notificada de uma desvinculação, é gerada uma nova chave para invalidar o *share* do cuidador;
- **A partir de um timeout:** As chaves criptográficas utilizadas para cifrar as credenciais presentes no servidor, possuem, no nosso sistema, um tempo de vida limitado, ou seja, o sistema periodicamente despoleta esta ação de rotatividade.

Quando ocorre a rotatividade da chave criptográfica utilizada sobre as credenciais presentes no servidor, é necessário realizar outros passos, nomeadamente, atualizar as credenciais que se

encontram no mesmo, dado estarem cifradas com a chave criptográfica antiga, bem como enviar tanto para o respetivo servidor como para os cuidadores que se encontram vinculados, os seus novos *shares*. Na Figura 4.4 é possível visualizar todo o fluxo deste processo, onde o quadrado com a cor roxa representa um sub-fluxo que também é explicado neste capítulo.

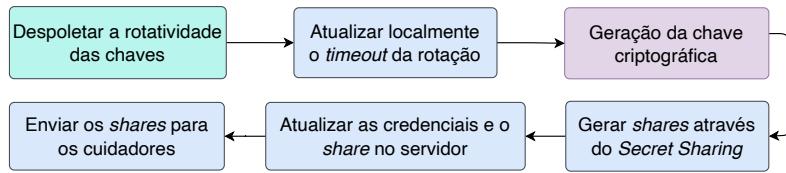


Figura 4.4: Rotatividade das chaves criptográficas (melhor visto a cores).

Validação das credenciais: Uma vez que as credenciais estão armazenadas na aplicação do proprietário e no Servidor de Autenticação e Armazenamento, é fundamental verificar que elas são idênticas em ambos os locais. Posto isto, a aplicação valida as credenciais presentes no servidor tendo por base as credenciais guardadas localmente. De seguida são apresentados os diversos cenários que foram tidos em conta:

- **Manipuladas indevidamente no servidor:** As aplicações estão preparadas para que, caso verifiquem que alguma credencial foi indevidamente alterada no servidor, os dados presentes localmente, considerados corretos, sejam replicados para esse. As condições a serem consideradas incluem: atualização da credencial com uma chave inválida, atualização da credencial com os dados de outra credencial, bem como a atualização da credencial com dados mais antigos do que os presentes localmente;
- **Apagadas indevidamente do servidor:** As aplicações também estão preparadas para casos extremos, tais como a coleção total ou parcial das credenciais do utilizador serem indevidamente apagadas do servidor. Caso essa situação seja verificada pela aplicação, ou seja, caso a aplicação verifique que possui credenciais que não se encontram no servidor, essas serão replicadas de imediato para o mesmo;
- **Perdidas localmente:** Caso as credenciais desapareçam localmente da aplicação do utilizador, a aplicação ao verificar que existem credenciais válidas no Servidor de Autenticação e Armazenamento que não se encontrem localmente, essas serão replicadas para a aplicação.

Na Figura 4.5 é possível verificar todo este fluxo, desde a obtenção das credenciais de ambos os ambientes, até à normalização das credenciais por todo o sistema.

Validação no Servidor Intermédio: Apesar da comunicação entre as aplicações e o Servidor Intermédio ser realizada recorrendo ao protocolo TLS, é necessário o servidor, do seu lado, realizar algumas validações das mensagens recebidas por parte das aplicações, para evitar que algum utilizador se esteja a passar por outro. Para tal, dado que o servidor possui uma chave pública de cada utilizador para validar as mensagens que recebe, para cada mensagem enviada que visa manipular os dados, seja o *bundle* ou a chave pública do utilizador, é verificado se os campos cifrados foram

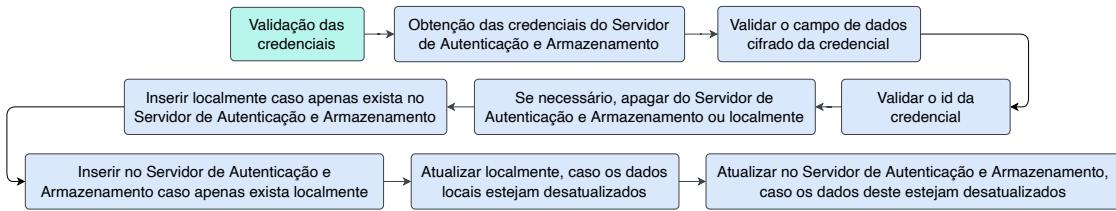


Figura 4.5: Validação das credenciais (melhor visto a cores).

cifrados com a chave privada correta. Além disso, depois da mensagem ser decifrada, o campo *username* é validado para confirmar que a mensagem corresponde ao utilizador que a enviou. O campo *timestamp* também é validado de modo a confirmar que os dados que se está a receber não são mais antigos que os dados que já se encontram neste servidor. Através da Figura 4.6 é possível visualizar esta operação de validação de forma mais detalhada.

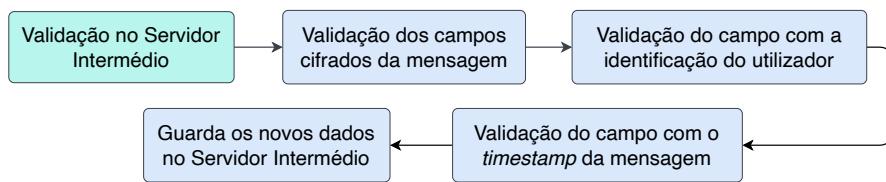


Figura 4.6: Validação no Servidor Intermédio (melhor visto a cores).

Geração de chaves criptográficas: Dado que pretendemos que os utilizadores, caso percam o telemóvel, ao realizarem a autenticação na mesma aplicação noutra dispositivo, consigam aceder às suas credenciais que se encontram no Servidor de Autenticação e Armazenamento, foi necessário que as principais chaves, nomeadamente a chave utilizada para cifrar as credenciais neste servidor e a chave utilizada no Servidor Intermédio, fossem geradas a partir da palavra-passe principal do utilizador. A Figura 4.7 apresenta toda esta operação.

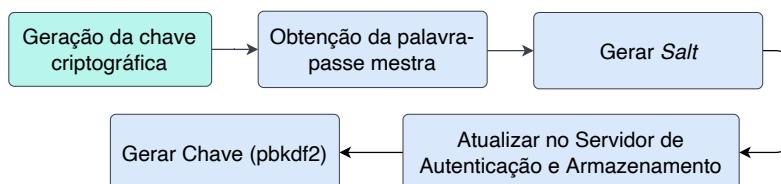


Figura 4.7: Geração de chave criptográfica (melhor visto a cores).

4.3 Operações do Sistema

Esta secção, tem como objetivo apresentar as principais operações construídas no sistema, derivadas das ações realizadas pelos utilizadores ao executar tarefas através da interface da aplicação. Serão destacados os processos mais importantes, organizados na ordem em que são executados.

4.3.1 Criação da Conta

Esta operação, representada na Figura 4.8, descreve todas as ações realizadas pela aplicação quando uma conta é criada. O processo inicia-se com o registo e criação de todos os recursos iniciais no Servidor de Autenticação e Armazenamento, seguido da instanciação da base de dados local e da criação da identidade no Servidor Intermédio. Por último, os quadrados amarelos, que correspondem, exclusivamente, a ações realizadas na aplicação dos idosos, representam a geração dos *shares* a partir da chave criptográfica que irá operar sobre as credenciais armazenadas no Servidor de Autenticação e Armazenamento, sendo um desses *shares* partilhado com essa mesma plataforma.

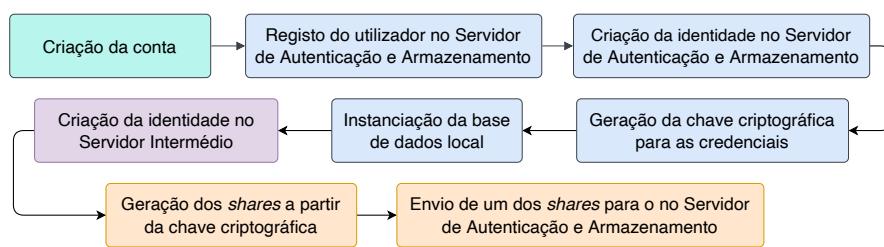


Figura 4.8: Operação de criação de conta (melhor visto a cores).

4.3.2 Atualizar os Dados Pessoais

Os dados pessoais são armazenados, exclusivamente, nos dispositivos locais. Quando um utilizador atualiza os seus dados, estas são apenas atualizadas localmente e enviadas para os utilizadores vinculados. A Figura 4.9 ilustra todo esta operação.

Os dados pessoais são armazenados, exclusivamente, nos dispositivos locais. Quando um utilizador atualiza os seus dados, estes são apenas atualizados localmente e enviados para os utilizadores vinculados. A Figura 4.9 ilustra esta operação.

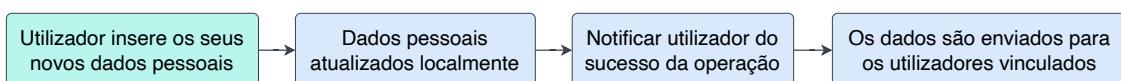


Figura 4.9: Operação de atualização dos dados pessoais (melhor visto a cores).

4.3.3 Envio Pedido de Vinculação

Nesta operação, a pessoa que deseja vincular-se deve inserir o email do utilizador alvo, que é validado através de dois critérios: se existe um utilizador registado com aquele email e se a vinculação é permitida, evitando que cuidadores se vinculem entre si ou idosos a outros idosos. Essas condições são validadas ao obter o *bundle* do Servidor Intermédio. Ao obter o *bundle*, é criada a sessão, enviado o pedido ao destinatário, guardado localmente o pedido. Quando o idoso envia o pedido, o *share* do futuro cuidador é enviado apenas após a aceitação. Se o cuidador envia o pedido, o *share* é enviado junto com a resposta de aceitação. A Figura 4.10 ilustra toda a operação.

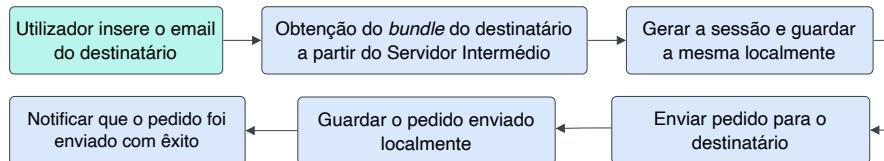


Figura 4.10: Operação de envio de um pedido de vinculação (melhor visto a cores).

4.3.4 Receber um Pedido de Vinculação

Quando um pedido de vinculação é recebido, ocorre a operação representada pela Figura 4.11, antes de ser apresentado o pedido ao utilizador recetor. Primeiramente, a aplicação obtém o *bundle* do utilizador que enviou o pedido e cria uma sessão. Posteriormente, verifica se já foi atingido o número máximo de relações, rejeitando automaticamente, caso se verifique. De seguida, guarda o pedido localmente e finalmente notifica o respetivo utilizador.

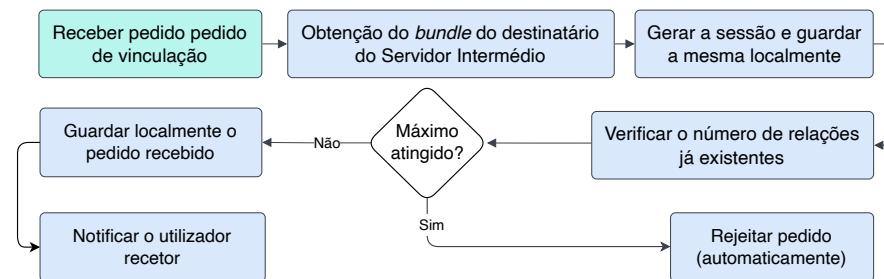


Figura 4.11: Operação da receção de um pedido de vinculação (melhor visto a cores).

4.3.5 Aceitar Pedido de Vinculação

Quando o utilizador aceita o pedido, o estado do utilizador vinculado é atualizado localmente. Em seguida, a aplicação do idoso informa ao Servidor de Autenticação e Armazenamento que o cuidador vinculado tem permissão para ler as suas credenciais. Após a aceitação, o utilizador é informado do sucesso da operação e os dados pessoais são enviados aos destinatários. Se o idoso aceitar o pedido, será enviado o *share* correspondente ao cuidador vinculado. Por último, se houver algum pedido pendente que não possa ser aceite por ultrapassar o limite de cuidadores, este será cancelado ou rejeitado. A Figura 4.12 possui todos os passos desta operação.

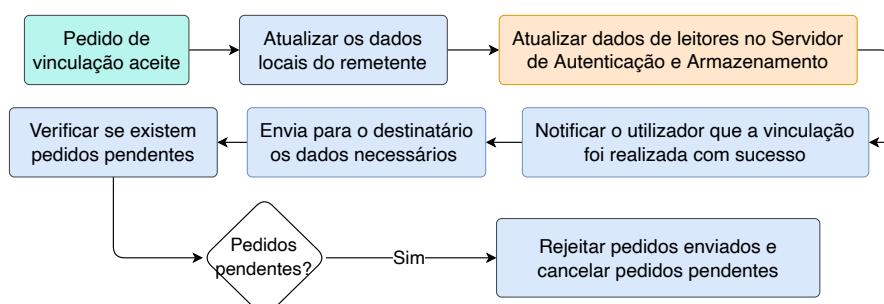


Figura 4.12: Aceitar pedido de vinculação (melhor visto a cores).

4.3.6 Cancelar ou Rejeitar Pedido de Vinculação

A operação correspondente às tarefas a serem executadas no cancelamento e na rejeição de um pedido, conforme apresentado na Figura 4.13, são idênticas. Em ambos os casos, todos os registo do utilizador são apagados, incluindo a sessão estabelecida e o pedido, que se pode encontrar num estado de “por aceitar” ou “à espera de resposta”. Por fim, ambos os utilizadores são notificados da ação realizada e informados de que os pedidos foram revertidos. No entanto, conforme ilustrado na Figura 4.14, a rejeição automática difere ligeiramente da rejeição manual. A verificação da necessidade de uma rejeição automática é feita antes do armazenamento local do pedido recebido, sendo assim a sessão, o único registo a ser apagado.

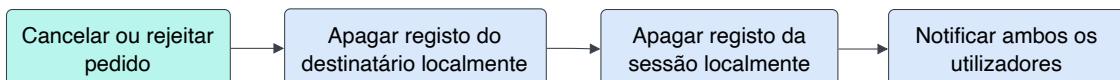


Figura 4.13: Cancelar ou Rejeitar pedido de vinculação (melhor visto a cores).

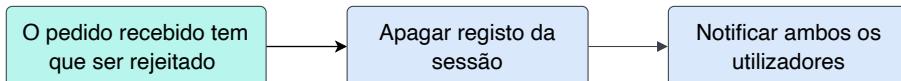


Figura 4.14: Rejeição automática de pedido de vinculação (melhor visto a cores).

4.3.7 Desvinculação de uma Relação

Como já explicado anteriormente, a desvinculação pode ser realizada tanto pelo idoso como pelo seu cuidador. Quando esta ação é iniciada, a aplicação apaga todos os dados referentes ao utilizador, incluindo os seus dados pessoais, o *share* referente ao idoso (no caso do cuidador) e os dados da sessão. Após a eliminação dos dados, é enviada uma notificação ao outro utilizador para informá-lo da desvinculação, para que este também apague tudo o que possui da respetiva relação. No caso dos idosos, realizam-se dois passos adicionais quando ocorre uma desvinculação, nomeadamente a atualização dos dados no Servidor de Autenticação e Armazenamento, removendo o respetivo cuidador da lista de leitores, e a rotatividade da chave criptográfica que protege as credenciais presentes neste servidor, cuja operação é apresentada na Secção 4.2.2. Na Figura 4.15, é possível visualizar todos os passos desta operação.

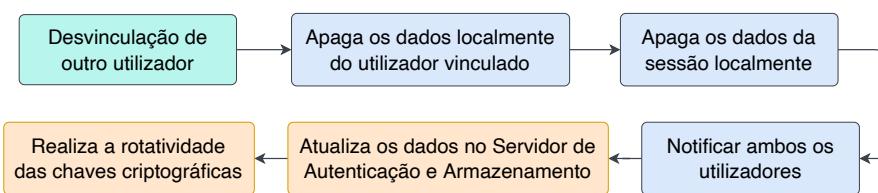


Figura 4.15: Desvinculação de uma relação (melhor visto a cores).

4.3.8 Alteração das Permissões de um Cuidador

A alteração das permissões de um cuidador só pode ser feita através da aplicação do idoso, que pode definir se os cuidadores têm acesso para manipular as credenciais, incluindo atualização, criação e eliminação. Quando há uma alteração nessas permissões, a aplicação do idoso atualiza as permissões no Servidor de Autenticação e Armazenamento. Após a alteração, uma notificação é enviada ao cuidador informando-o da mudança. Esta operação é ilustrado na Figura 4.16.

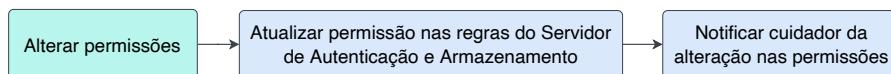


Figura 4.16: Atualizar permissões do cuidador (melhor visto a cores).

4.3.9 Atualização das Credenciais

A atualização das credenciais pode ser realizada tanto pelo respetivo idoso, conforme mostrado na Figura 4.17, como pelos cuidadores com as permissões adequadas, ilustrado na Figura 4.18. Ao atualizar uma credencial, os campos alterados são atualizados no Servidor de Autenticação e Armazenamento, incluindo informações sobre quem realizou a atualização, a data e hora da mesma. Após uma atualização bem-sucedida, o utilizador é notificado. Quando um idoso atualiza as suas credenciais, todos os cuidadores são notificados. Da mesma forma, se o cuidador atualiza a credencial do idoso, este também é informado da alteração.

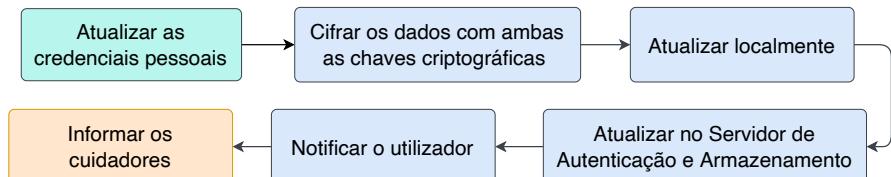


Figura 4.17: Atualizar as credenciais pessoais (melhor visto a cores).

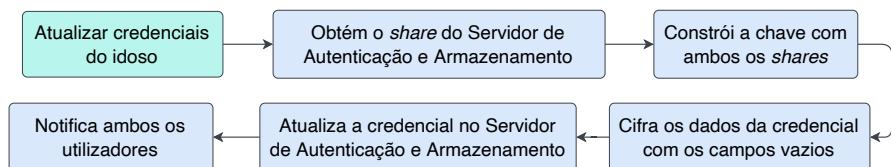


Figura 4.18: Atualizar as credenciais do idoso (melhor visto a cores).

4.3.10 Apagar Credenciais

A operação para apagar uma credencial pessoal difere da operação para apagar uma credencial do idoso por parte do cuidador. Quando um utilizador apaga uma credencial pessoal, representado na Figura 4.19, os dados são eliminados tanto do Servidor de Autenticação e Armazenamento como localmente, sendo os cuidadores notificados. Por outro lado, quando o cuidador elimina a

credencial do idoso, a operação é semelhante à da atualização, pois realiza apenas um *soft-delete*, i.e., limpa os campos. Esta abordagem assegura que apenas os proprietários das credenciais as podem eliminar diretamente do servidor. Quando o idoso valida as credenciais, conforme explicado na Secção 4.2.2, ao verificar que um dos cuidadores realizou um *soft-delete*, apaga a credencial definitivamente.

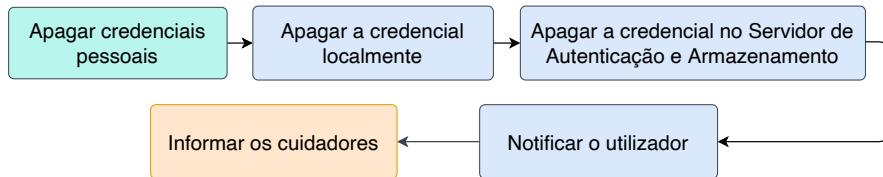


Figura 4.19: Apagar credenciais pessoais (melhor visto a cores).

4.3.11 Criar Identidade no Servidor Intermédio

Para que uma aplicação comunique com outra, é necessário criar a identidade do utilizador no Servidor Intermédio, como detalhado na Figura 4.20. Inicialmente, estabelece-se uma comunicação via *socket* com o servidor. Em seguida, gera-se o *bundle* do protocolo *Signal* e um par de chaves pública/privada para identificar o utilizador. O *bundle* é cifrado com a chave privada obtida anteriormente e enviado ao Servidor Intermédio, juntamente com o identificador do utilizador e a chave pública correspondente.

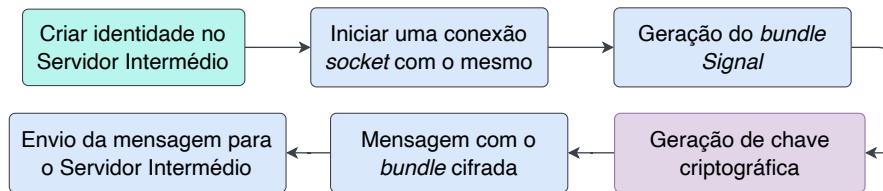


Figura 4.20: Criar identidade no servidor (melhor visto a cores).

4.3.12 Apresentação do Ecrã *SplashScreen*

Como o ecrã *Splash Screen* não deve ser sempre exibido, foi implementada uma operação específica para a sua apresentação, conforme a Figura 4.21. Na base de dados local, um tuplo na tabela *timeout* armazena o *timestamp* da última exibição. A aplicação verifica esse valor e, se o tempo transcorrido for suficiente, atualiza o tuplo com a data atual e exibe o *Splash Screen*.

4.4 Sumário

Neste capítulo, apresentamos o sistema implementado. Começamos com a descrição da arquitetura, composta por duas aplicações móveis distintas (uma para cuidadores e outra para idosos) e por dois servidores na *Cloud*: um dedicado ao armazenamento seguro de dados sensíveis, como

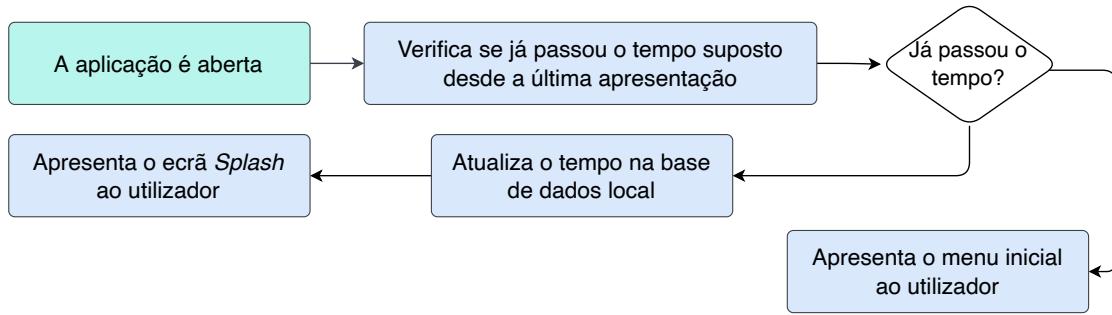


Figura 4.21: Apresentação do ecrã *SplashScreen* (melhor visto a cores).

credenciais cifradas, e outro que assegura a comunicação entre as aplicações. Em seguida, introduzimos o modelo adversário e os mecanismos de segurança, onde descrevemos as metodologias adotadas para garantir a segurança do sistema, incluindo a autenticação do utilizador, o recurso a protocolos de segurança, a rotatividade das chaves criptográficas, a validação das credenciais e os mecanismos de segurança no Servidor Intermédio. Finalizamos o capítulo com a descrição das principais operações do sistema, detalhando as ações executadas pelo sistema e pelo utilizador quando determinadas operações são despoletadas.

Capítulo 5

Implementação

Neste capítulo, descrevemos a implementação do sistema em duas secções principais. A primeira apresenta as tecnologias utilizadas no desenvolvimento dos diversos componentes. A segunda foca-se na implementação do *Frontend*, cobrindo tanto as decisões de *design* como os principais fluxos disponíveis através da interface das aplicações.

5.1 Tecnologias

Considerando todos os fluxos e a estrutura a serem implementados no sistema, tornou-se imprescindível selecionar, entre as diversas opções disponíveis no mercado, a tecnologia que melhor nos permitisse concretizar os objetivos estabelecidos. Nas seguintes secções, iremos analisar detalhadamente todas as tecnologias escolhidas para o desenvolvimento dos diferentes componentes do sistema. Para cada tecnologia selecionada, apresentaremos uma justificação detalhada da sua escolha, destacando os benefícios específicos e as vantagens que cada uma proporciona ao projeto.

5.1.1 Firebase

Tal como já referido anteriormente, o nosso sistema necessita de recorrer a um servidor na *Cloud* para que seja possível existir uma cópia de segurança das credenciais e para que os cuidadores possuam um local onde possam consultar e manipular as credenciais dos idosos, caso lhes seja permitido. Para além da possibilidade de armazenar dados no sistema, pretendemos que este servidor seja suficientemente seguro para que seja possível estabelecer quem pode aceder a determinados dados, evitando que possíveis atacantes, ao acederem à *API* disponibilizada pelo serviço escolhido, consigam obter qualquer credencial.

Após a análise das opções disponíveis no mercado, concluiu-se que o serviço de *Backend as a Service* (BaaS) fornecido pela *Google* e denominado *Firebase* [21] atendia plenamente aos requisitos do projeto. Além disso, este serviço oferece um portal acessível através de um *browser*, que é bastante intuitivo e permite realizar diversas configurações conforme necessário pelo administrador do sistema, bem como esclarecer dúvidas relativamente ao seu uso.

Adicionalmente, a *Firebase* possui uma comunidade extensa e ativa, através da qual é possível resolver dúvidas variadas relacionadas às diferentes configurações possíveis, tanto pelo portal

quanto pelas aplicações desenvolvidas. De seguida, são apresentadas as diversas funcionalidades da *Firebase* que foram cruciais para o desenvolvimento do sistema:

- **Integração Fácil com Aplicações Móveis:** O *Firebase* oferece SDKs nativos para *iOS* e *Android*, além de suporte para frameworks híbridos como *React Native* [41]. Esta funcionalidade é crucial para o nosso sistema, pois estabelecemos como requisito o desenvolvimento para ambos os sistemas operativos;
- **Firebase Authentication:** Esta funcionalidade, quando se encontra ativa, permite que um utilizador valide a sua identidade através da aplicação, possibilitando assim a obtenção dos seus dados que se encontram no servidor. Além disso, impede que um email já utilizado por outro utilizador seja reutilizado, verifica a validade do e-mail e protege a conta do utilizador contra diversos ataques, como ataques de força bruta (*brute-force attacks*), ao estipular limites para tentativas de *login* e outras operações num curto espaço de tempo;
- **Firebase Firestore:** A *Firestore* é a base de dados *NoSQL* da *Firebase*, que é altamente flexível e escalável desenvolvida na infraestrutura da *Google Cloud*. A sua estrutura é composta por coleções que contêm documentos. Cada documento pode conter sub-coleções e múltiplos campos de diferentes tipos. A *Firestore* foca-se no armazenamento de dados estruturados em documentos, tornando-a ideal para guardar configurações, dados de utilizador e informações de perfil, entre outros documentos de texto. A *Firebase* garante que os dados armazenados nos seus servidores não estão em texto simples (*Plain Text*), mas sim cifrados com chaves protegidas e rotativas, utilizando o mesmo sistema de segurança aplicado aos dados confidenciais da própria instituição;
- **Firebase Storage:** A *Firebase Storage*, ao contrário da *Firestore*, utiliza uma estrutura simples de pastas e ficheiros binários (como fotos ou vídeos). Este serviço é ideal para armazenar dados de grande dimensão, evitando a ocupação do espaço interno dos dispositivos dos utilizadores. Os dados podem ser acedidos diretamente através de URLs, tornando o acesso fácil e direto, sem necessidade de código adicional ou de uma aplicação específica. Essa funcionalidade foi fundamental para apresentar os tutoriais aos utilizadores;
- **Security Rules:** Esta funcionalidade é essencial na *Firestore*, dado que fornece um conjunto de configurações que permitem definir como e quem pode aceder a determinados dados. Estas regras são cruciais para proteger os dados contra acessos não autorizados e prevenir manipulações indevidas. Com elas, é possível verificar se um utilizador está autenticado antes de aceder aos dados, validar permissões de leitura e/ou escrita, e definir permissões detalhadas com base em atributos do utilizador, do documento a ser acedido ou de outras partes da base de dados. Além disso, as *Security Rules* permitem configurar regras específicas para diferentes coleções e documentos, proporcionando uma camada adicional de segurança, para além da lógica do cliente. Estas regras escalam automaticamente, sem necessidade de manutenção adicional, garantindo a segurança e integridade dos dados ao longo do tempo.

5.1.2 React Native

Para o desenvolvimento das aplicações móveis, foi necessário utilizar uma *framework* que permitisse a criação de aplicações tanto para os sistemas operativos *Android* como *iOS* apenas com uma única base de código. O *React Native*, desenvolvido pela *Meta*, é uma *framework* que possibilita a criação de aplicações móveis utilizando *JavaScript/TypeScript* e *React*, uma *framework* popular para o desenvolvimento de aplicações web, adaptada o cenário de aplicações móveis. Apesar da *framework* gerar binários para ambos os sistemas operativos a partir de um único código, o recurso à mesma não influência a performance das aplicações. Esta recorre a componentes nativos e quando renderiza a aplicação, renderiza a mesma diretamente para o código nativo, proporcionando uma performance próxima de aplicações nativas. Para gerirmos as bibliotecas recorremos ao *Node Package Manager* (NPM) que nos permite utilizar as mais diversas bibliotecas desenvolvidas em *Javascript* e em *TypeScript*. No contexto da *framework* *React Native*, utilizamos também o *Expo*. Esta ferramenta funciona como uma extensão do *React Native*, que visa simplificar e acelerar o desenvolvimento de aplicações móveis. A seguir, apresentam-se as razões que justificam a integração do *Expo*:

- **Ferramentas integradas:** O *React Native Expo* [42], através do *Expo SDK* oferece um conjunto de *APIs* e componentes que podem ser utilizados durante o desenvolvimento, facilitando o acesso a funcionalidades nativas do dispositivo de forma simplificada. Além disso, este *SDK* está em constante inovação e atualização, com novas funcionalidades desenvolvidas em parceria com a equipa da *Meta*;
- **Facilidade de configuração:** O uso do *React Native Expo* permite o desenvolvimento de aplicações sem a necessidade dos ambientes de desenvolvimento integrado (IDEs) necessários para ambos os sistemas operativos, nomeadamente o *Android Studio* para o *Android* e o *Xcode* para o *iOS*. Esta abordagem elimina a complexidade das configurações que anteriormente eram necessárias resolver em cada nova construção (*build*) do projeto;
- **Comunidade e Suporte:** Durante o desenvolvimento de um sistema, a existência de uma comunidade e um suporte, que permita o esclarecimento de dúvidas, é um fator importante para evitar problemas demorados. Além da grande comunidade que utiliza *JavaScript*, *TypeScript* e *React Native*, o *Expo* conta com fóruns e servidores onde os utilizadores podem debater temas e esclarecer dúvidas com a equipa responsável pela desenvolvimento e manutenção da *framework*;
- **Expo Go:** Finalmente, uma das maiores vantagens desta *framework* reside na facilidade com que se pode testar o desenvolvimento diretamente num dispositivo móvel em questão de segundos. O *Expo Go* é, essencialmente, uma *sandbox* que pode ser instalada em qualquer dispositivo com sistema operativo *iOS* ou *Android*. Através da leitura de um *QR code*, é possível emular a aplicação no dispositivo móvel de forma quase instantânea. Esta funcionalidade permite testar a aplicação como se estivesse instalada localmente, oferecendo um processo de desenvolvimento mais ágil e eficiente.

5.1.3 NodeJS

A tecnologia escolhida para o Servidor Intermédio foi selecionada após a definição da tecnologia utilizada para o desenvolvimento das aplicações móveis. Considerando que o Servidor Intermédio precisará de comunicar constantemente com as aplicações móveis como, possivelmente, com o Servidor de Autenticação e Armazenamento, também presente na *Cloud*, optámos por uma *framework* que utilizasse a mesma linguagem de programação das aplicações móveis para garantir consistência e facilitar o desenvolvimento.

Assim, optou-se pela utilização do *Node.js* como base para o Servidor Intermédio. O *Node.js* permite a utilização de *JavaScript* e *TypeScript*, oferecendo flexibilidade no desenvolvimento. Além disso, é amplamente reconhecido pela sua eficiência em operações de entrada e saída (I/O) não bloqueantes, o que o torna ideal para um Servidor Intermédio que necessita de gerir múltiplas conexões simultâneas e comunicação em tempo real. A sua capacidade de gerir um elevado número de conexões simultâneas com baixo *overhead* constitui uma vantagem significativa.

Outro fator determinante foi a vasta coleção de bibliotecas e módulos disponíveis através do *NPM*, o mesmo que é utilizado nas aplicações móveis, tal como referido anteriormente, garantindo assim uma maior consistência durante o desenvolvimento do sistema.

5.1.4 Criptografia

Nas aplicações móveis como no Servidor Intermédio, as operações criptográficas são um fator bastante importante no nosso sistema. Posto isto, de seguida são apresentadas as bibliotecas que foram escolhidas para serem utilizadas na execução das diversas operações que remetem para a proteção dos dados mais sensíveis:

- **Pbkdf2:** Para a geração de chaves criptográficas com base na palavra-passe principal do utilizador, esta biblioteca permite o uso da função *pbkdf2*, que, através da palavra-passe e de um valor aleatório denominado *Salt*, gera uma chave criptográfica;
- **TweetNaCl:** *TweetNaCl* é uma implementação da biblioteca de criptografia *NaCl*, focada em facilidade de uso, eficiência e segurança robusta. Esta recorre ao algoritmo *x25519-xsalsa20-poly1305* para garantir criptografia de ponta a ponta, autenticação de mensagens e assinaturas digitais, protegendo dados sensíveis contra ataques. Além disso, esta biblioteca possui funções que, através de uma chave criptográfica, geram pares de chave pública e chave privada, essenciais para a validação realizada pelo Servidor Intermédio;
- **Libsignal-protocol-typescript:** Biblioteca que permite a implementação do protocolo *Signal* utilizado para criptografia de ponta a ponta, entre as aplicações móveis, através do Servidor Intermédio;
- **Zxcvbn:** Visto que um dos requisitos do nosso sistema consiste na avaliação das palavras-passe escolhidas pelos utilizadores, o algoritmo *Zxcvbn* disponibilizado nesta biblioteca permite avaliar as mesmas tendo em conta diversos fatores, como padrões, palavras-passes co-

muns e até mesmo palavras presentes em dicionários, fatores que podem tornar uma palavra-passe fraca.

5.2 Implementação do *Frontend*

Neste secção, descrevemos a implementação do *Frontend* das duas aplicações móveis, destacando as principais decisões de *design* e os fluxos de navegação nas interfaces.

5.2.1 Decisões de *Design*

Dado que o objetivo do sistema é desenvolver um gestor de palavras-passe para idosos, foi essencial aplicar boas práticas no desenvolvimento de interfaces para esta faixa etária. Com base nos requisitos da literatura e nas melhorias sugeridas nas avaliações heurísticas, apresentamos a seguir as diretrizes adotadas no desenvolvimento do *Frontend* das duas aplicações:

- **Cores escolhidas:** A quantidade de cores escolhidas foi minimizada, mantendo-se sempre a necessidade de se distinguir as operações desencadeadas pelos diferentes botões. Os botões assumem a cor verde quando despoletam uma ação de “criar” ou “ligar” algo. Por sua vez, os botões vermelhos despoletam ações de “desligar”, “cancelar” ou “apagar”. Botões de edição e de alteração da visibilidade dos dados têm cores distintas para se destacarem dos restantes: amarelo e salmão, respetivamente. Azul e cinza são utilizados para despoletar ações neutras, como copiar valores, navegar na aplicação ou em barras de pesquisa. A cor de fundo dos componentes na aplicação varia entre branco e cinza, dependendo dos elementos da interface. O texto na aplicação utiliza duas cores, cinza escuro ou branco, dependendo da cor de fundo. Os ícones podem ser nas cores azul, cinza escuro ou salmão;
- **Contraste:** Como o público-alvo do sistema são os idosos, é essencial que o contraste entre o texto e o fundo seja o máximo possível. Assim, as cores dos botões e textos foram selecionadas para garantir um rácio de contraste superior a 8. Todas as cores foram verificadas com a plataforma *Contrast Finder* [14] para assegurar esse rácio mínimo;
- **Ícones utilizados:** Utilizamos ícones que representam objetos ou conceitos familiares aos idosos para ajudar na compreensão e memorização das funcionalidades. Esta abordagem facilita o entendimento intuitivo. Quando a função de um ícone é ambígua, ele é acompanhado por um pequeno texto explicativo;
- **Texto:** O texto na aplicação utiliza a fonte padrão do sistema operativo para proporcionar familiaridade aos utilizadores. Os tamanhos variam entre 35pt para títulos, 21pt para legendas, 19pt para elementos comuns e 16pt para detalhes informativos. Todos os textos são ajustados automaticamente caso o dispositivo não suporte o tamanho escolhido;
- **Navegação na aplicação:** À exceção do menu inicial, todos os ecrãs das aplicações mostram a localização atual do utilizador. Nesses ecrãs, a barra de navegação está sempre visível, permitindo voltar à página anterior ou retornar ao menu inicial;

- **Edição da informação:** Em qualquer ecrã que permita editar informações, como os detalhes de uma credencial ou a informação pessoal, há um botão para ativar a edição, prevendo edições indesejadas. Quando a edição está ativada, os campos editáveis são destacados com uma cor diferente, indicando que o modo de edição está ativo. Também existe um botão específico para cancelar esse modo;
- **Confirmação das ações:** Ações que alterem dados presentes na plataforma, são acompanhadas por um *popup* com opções de confirmação. Esta funcionalidade assegura que nenhuma ação destrutiva seja executada sem a confirmação explícita do utilizador;
- **Apresentação de informação relevante:** A aplicação apresenta apenas a informação minimamente relevante para os utilizadores, facilitando a leitura da interface e permitindo que se concentrem no que é realmente importante;
- **Animações evitadas:** Em ambas as aplicações, não incluímos animações que poderiam distrair os utilizadores, garantindo que não são perturbados por elementos desnecessários.

5.2.2 Fluxos do Frontend

De seguida, apresentamos os fluxos disponíveis nos ecrãs das aplicações para executar as diversas funcionalidades do sistema desenvolvido:

- **Entrar/Criar conta pessoal:** Quando um utilizador abre a aplicação, é direcionado para a página de *login*, onde deve inserir o seu email e palavra-passe, conforme ilustrado no ecrã 1 da Figura 5.1. Se ainda não tiver uma conta, pode navegar para o ecrã 2 através do botão “Criar conta”. Neste, é apresentado um formulário onde o utilizador preenche as informações necessárias. Após preencher os dados, ao selecionar o botão “Criar”, o utilizador desencadeia a validação e criação da conta, sendo apresentado um estado de *loading*, visível no ecrã 3. Quando a conta é criada, o utilizador é redirecionado para o ecrã de *SplashScreen* (ecrã 4), onde pode aguardar pelo *timeout* ou fechar o ecrã usando o botão “Fechar Sugestão”. Em seguida, é apresentado o menu principal da aplicação (ecrã 5);



Figura 5.1: Fluxo da criação de conta (melhor visto a cores).

- Manipular dados pessoais:** Para editar os dados pessoais, o utilizador deve navegar até à página de definições, selecionando o botão “Definições” no menu inicial, conforme ilustrado no ecrã 1 da Figura 5.2. Na página de definições, o utilizador pode selecionar o botão “Editar” para ativar a edição dos campos. Quando os campos estão editáveis, são destacados com uma borda azul, indicando que podem ser alterados, como mostrado no ecrã 3. Neste ecrã, o botão “Editar” desaparece, sendo substituído pelos botões “Cancelar” e “Guardar”, este último visível apenas se houver alterações nos valores. Após realizar as alterações desejadas e clicar no botão “Guardar”, é exibido um *popup* para confirmar se deseja efetuar as modificações, seguindo o padrão de confirmação utilizado para todas as ações importantes na aplicação, como ilustrado no ecrã 4. Após a confirmação, as informações alteradas são atualizadas. Neste ecrã, o utilizador também pode terminar a sessão, ação que requer confirmação através de um *popup*. O ecrã 5 da Figura 5.2 ilustra o botão para terminar a sessão e os dados após a atualização;

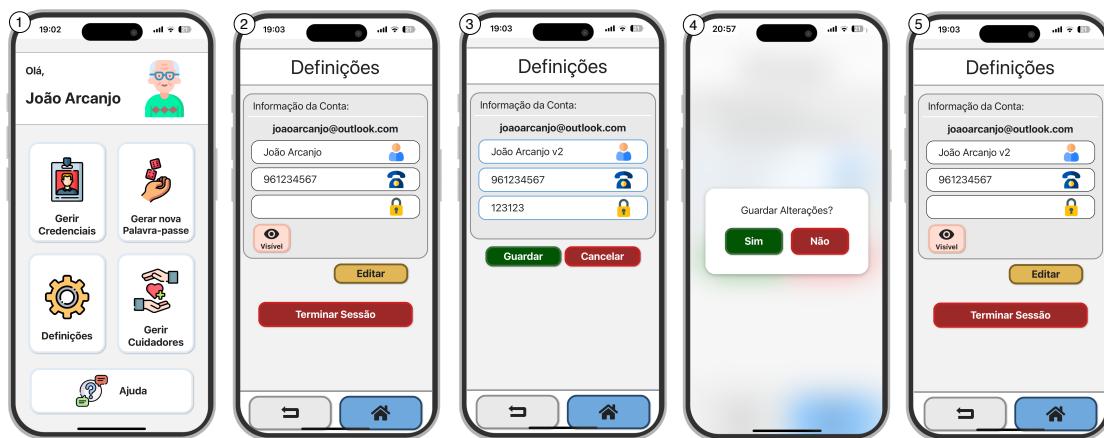


Figura 5.2: Fluxo de edição de dados pessoais (melhor visto a cores).

- Gerador de palavras-passe:** Para aceder ao gerador de palavras-passe, o utilizador deve usar o menu inicial. Ao selecionar o botão “Gerar nova palavra-passe”, é redirecionado para o ecrã 2 da Figura 5.3, que apresenta os requisitos da palavra-passe, incluindo comprimento e tipos de caracteres. O ecrã também inclui um botão de histórico, que, ao ser selecionado, leva o utilizador ao ecrã 3, onde pode consultar as últimas 10 palavras-passe geradas e o respetivo *timestamp*;
- Relação com cuidadores:** As relações com os cuidadores são totalmente editáveis através de um ecrã acessível apenas pela aplicação dos idosos. Ao selecionar o botão “Gerir Cuidadores” no ecrã inicial, o idoso é redirecionado para o ecrã 2 da Figura 5.4. Neste ecrã, aparece o botão “Adicionar Cuidador”, que, ao ser selecionado, apresenta um *popup* onde é necessário inserir o email do cuidador. No ecrã 3 da mesma figura, é demonstrado o pedido realizado no estado pendente, juntamente com o botão para adicionar outro cuidador. Quando o idoso recebe um pedido de vínculo, a aplicação exibe tanto o pedido enviado



Figura 5.3: Fluxo gerador de palavras-passe fortes (melhor visto a cores).

como o recebido, como mostrado no ecrã 4. Ao aceitar o pedido recebido, o ecrã passa a apresentar os dados do cuidador, incluindo um botão para desvinculação, botões para contacto rápido e um interruptor para ajustar as permissões do cuidador, conforme visível no ecrã 5;

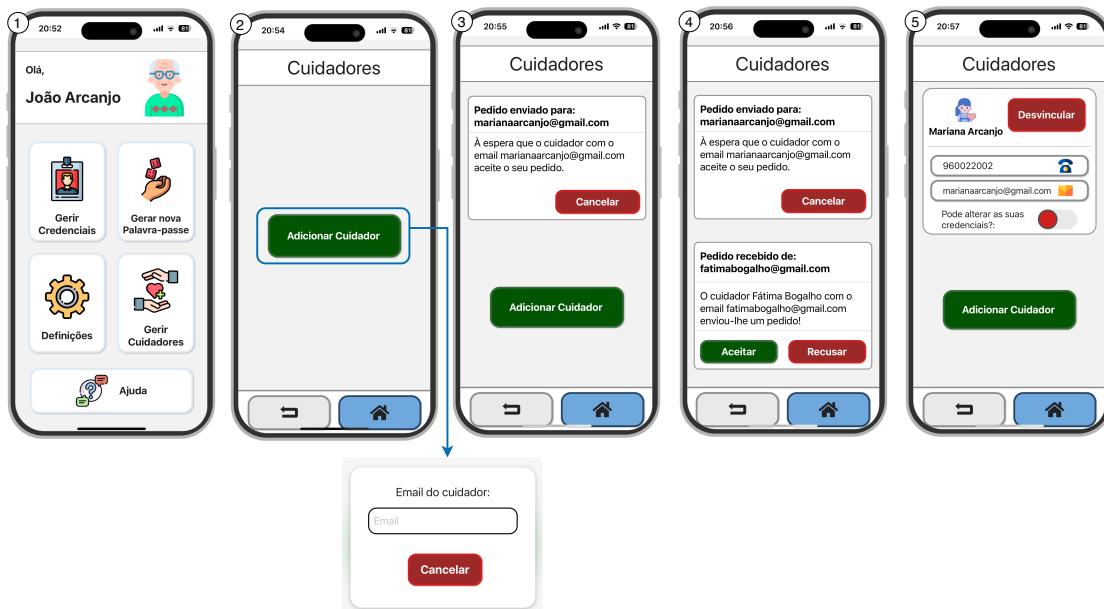


Figura 5.4: Fluxo de gestão dos cuidadores (melhor visto a cores).

- Relação com os idosos:** Na aplicação dos cuidadores, ao selecionar o botão “Gerir Idosos” no ecrã 1 da Figura 5.5, os cuidadores são direcionados para o ecrã 2. Neste ecrã, podem enviar pedidos de vinculação através do botão “Adicionar Idoso”, utilizando apenas o email, num processo semelhante ao seguido pelos idosos para se vincular a um cuidador. Adicionalmente, o cuidador pode visualizar todos os idosos aos quais está vinculado (ecrã 2), onde o atual cuidador está vinculado a um idoso. No ecrã 3, é evidente a alteração do estado desta lista após o cuidador ter enviado um pedido e recebido um pedido de outro idoso.

Se o pedido recebido for rejeitado e o pedido enviado for aceite, a interface muda para o estado do ecrã 4, onde é exibido um item referente ao novo idoso. O cuidador pode aceder a opções de contacto, desvinculação e gestão das credenciais. Ao selecionar “Credenciais”, é redirecionado para o ecrã 5 da Figura 5.5, onde pode visualizar e, se autorizado, adicionar ou alterar credenciais. Se não tiver permissões, será notificado via *popup*;

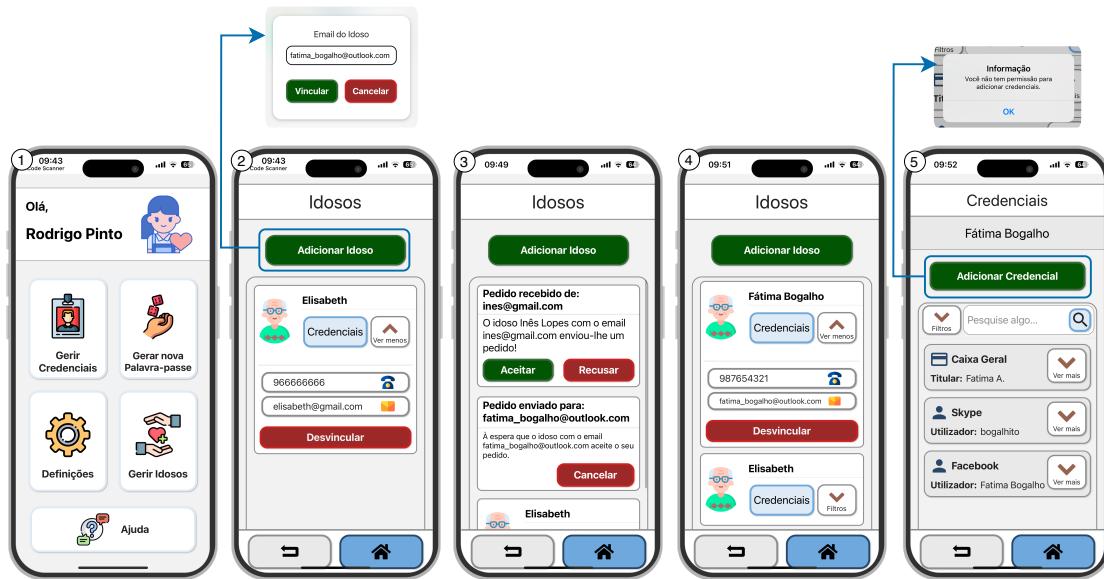


Figura 5.5: Fluxo de gestão dos idosos (melhor visto a cores).

- **Adicionar uma credencial:** Para adicionar uma nova credencial, o utilizador deve selecionar o botão “Gerir Credenciais” no ecrã 1 da Figura 5.6. Ao selecionar esse botão, o utilizador é redirecionado para o ecrã 2, onde lista as credenciais e encontra o botão “Adicionar Credencial”. Ao clicar, surgem duas opções, conforme ilustrado no ecrã 3: “Login” ou “Cartão”. Se escolher “Cartão”, verá o ecrã 4; se optar por “Login”, será apresentado o ecrã 5, onde poderá selecionar a plataforma desejada. Para definir a palavra-passe, o utilizador deve selecionar o botão “Opções”, que apresenta um *popup* onde pode escolher os requisitos desejados. Após definir os requisitos, o utilizador pode gerar uma nova palavra-passe ao clicar em “Gerar nova palavra-passe”. Depois de preencher todos os campos necessários, ao selecionar o botão “Adicionar Credencial”, a nova credencial é adicionada;
- **Detalhes de uma credencial:** Para visualizar os detalhes de uma credencial, o utilizador deve aceder à lista de credenciais no ecrã 2 da Figura 5.7. Esta lista pode ser filtrada pelo tipo (“Login” ou “Cartão”) e/ou pelo nome da credencial. Ao selecionar o botão “Ver mais” em cada item, o utilizador pode obter os mesmos valores ou navegar diretamente para a plataforma, no caso de credenciais do tipo “Login”. Ao clicar no item da credencial, a aplicação redireciona para o ecrã 5 da Figura 5.7, onde é possível visualizar, editar e apagar a credencial. Devido à natureza destrutiva das ações de edição e eliminação, a aplicação sempre exibe um *popup* para confirmar se o utilizador realmente deseja prosseguir;



Figura 5.6: Fluxo de edição de uma nova credencial (melhor visto a cores).

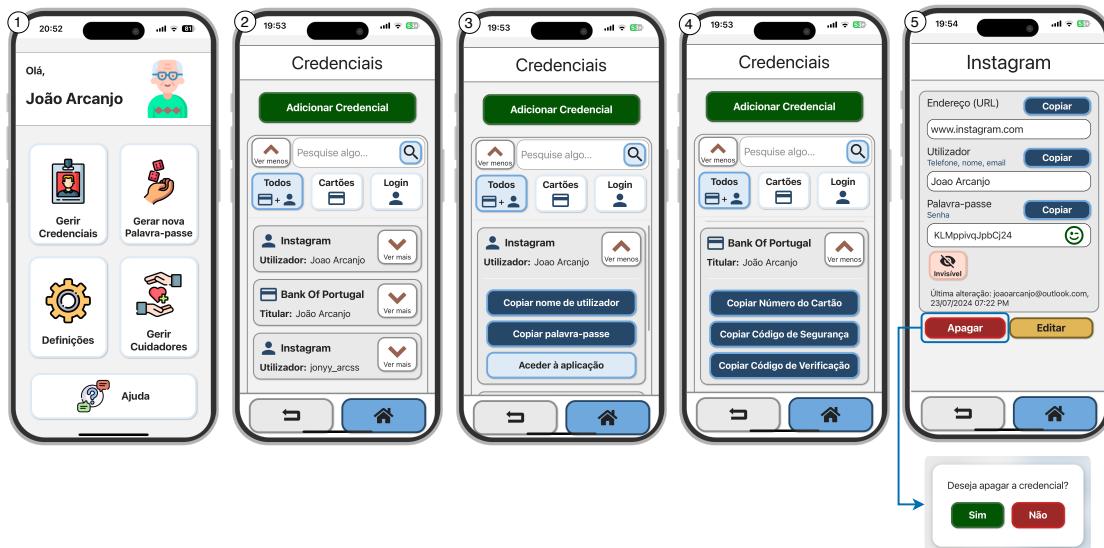


Figura 5.7: Fluxo de visualização e edição dos detalhes de uma credencial (melhor visto a cores).

- Ajuda aos utilizadores:** Em ambas as aplicações, existem auxiliares para ajudar os utilizadores. Através do menu inicial, ao selecionar “Ajuda”, o utilizador é redirecionado para o ecrã 2 da Figura 5.8, que inclui três novos botões de navegação. O primeiro, “Perguntas”, exibe perguntas frequentes, permitindo ao utilizador visualizar respostas ao pressionar “Ver mais”, conforme o ecrã 2. Na opção “Tutoriais”, é apresentada uma lista de ações que o

utilizador pode querer realizar. Ao clicar no botão “Ver Mais”, são fornecidas instruções passo a passo visíveis no ecrã 3, juntamente com um vídeo explicativo visível no ecrã 4. O último botão “Sugestões” lista um conjunto de sugestões, conforme ilustrado no ecrã 5, que podem ser úteis durante o uso da aplicação.



Figura 5.8: Fluxo da página para ajudar os utilizadores (melhor visto a cores).

5.3 Sumário

Neste capítulo, apresentamos as tecnologias utilizadas no desenvolvimento do sistema e as decisões de *design* implementadas. Iniciamos com a *Firebase*, que foi utilizada para autenticação e armazenamento de dados, seguido do *React Native Expo*, escolhido para desenvolver as aplicações móveis, devido à sua capacidade de gerar binários para diferentes plataformas. Também discutimos a utilização do *Node.js* no Servidor Intermédio, valorizando a sua eficiência em operações não bloqueantes. Foram ainda destacadas as bibliotecas criptográficas usadas para garantir segurança. Na parte de *design*, abordamos as decisões que foram tomadas para melhorar a usabilidade, como, por exemplo, a escolha das cores, os ícones e o texto. Detalhamos os principais fluxos das aplicações, como a criação de contas, edição de dados e gestão de credenciais, além das interações entre utilizadores, finalizando com as funcionalidades auxiliares que oferecem suporte adicional aos utilizadores.

Capítulo 6

Avaliação

Neste capítulo, apresentamos a avaliação do nosso sistema em duas vertentes: usabilidade da aplicação e o desempenho. A avaliação da usabilidade inclui três etapas distintas: duas avaliações heurísticas aos protótipos intermédios e a avaliação do protótipo final com o público-alvo.

6.1 Avaliação Heurística do Protótipo Funcional 1

A primeira avaliação heurística foi realizada quando se considerou que o primeiro protótipo funcional possuía as funcionalidades mínimas necessárias para serem testadas, nomeadamente a possibilidade do idoso se autenticar, adicionar e manipular as credenciais, e gerar palavras-passe fortes. Após o desenvolvimento destas, foi possível obter a primeira avaliação heurística do perito. As duas secções seguintes têm como principal objetivo, explicar como foi realizada esta primeira avaliação, bem como expor as melhorias efetuadas, tendo em conta as sugestões recebidas.

6.1.1 Metodologia

Na primeira avaliação heurística, foi consultado um perito com o objetivo de obter um primeiro *feedback* sobre o estado da aplicação e verificar se o seu desenvolvimento estava a seguir a direção adequada. O perito, mulher de 33 anos à data da avaliação, é professora universitária e investigadora na área da informática, com especialização em Interação Pessoa-Máquina.

Para que o perito conseguisse testar livremente a aplicação, foi gerado um *Android Application Package* (APK) do protótipo funcional da aplicação do idoso construído até à data e entregue ao mesmo, para que este instalasse a aplicação no seu dispositivo. Após a instalação, o perito explorou as funcionalidades já implementadas, e reportou todos os problemas de usabilidade que detetou durante os testes, bem como sugestões de implementações e melhorias. Na seguinte secção são expostos os problemas e melhorias aconselhadas pelo perito nesta fase.

6.1.2 Resultados e Melhorias Realizadas

Nesta secção, são apresentados os problemas e aspetos que o perito considerou que deviam ser melhorados. A aplicação, nesta primeira avaliação, já estava estruturada de modo a permitir o

registro de várias pessoas no mesmo dispositivo. No entanto, quando um utilizador realizava *logout* de uma conta previamente criada, ao voltar a entrar na mesma, não conseguia visualizar as credenciais que tinham sido adicionadas anteriormente, deparando-se com um aviso de erro. Este problema ocorria devido à função assíncrona responsável por armazenar as chaves criptográficas na *KeyChain/KeyStore* do dispositivo não estar corretamente implementada. Como a aplicação não garantia que a chave era guardada corretamente, por vezes tornava impossível a sua recuperação durante um novo *login*, e, por sua vez, a interpretação das credenciais. Este problema foi resolvido ao adicionarmos a operação *await* à chamada da respetiva função.

Na fase inicial do projeto, o utilizador inseria o seu email e a palavra-passe na primeira página da aplicação, e, posteriormente, podia optar por selecionar o botão “Entrar” para aceder a uma conta já existente, ou o botão “Criar uma conta” para utilizar os dados inseridos para criar uma nova conta. Contudo, esta abordagem foi considerada inadequada pelo perito, pois misturava a ação de entrar numa conta existente com a de criar uma nova conta. Para mitigar este problema, foi criada uma página dedicada, exclusivamente, à criação de novas contas, acessível através do botão “Criar uma conta” na página de *login*. Nesta nova página, foi possível adicionar outros campos que foram considerados necessários, tais como os dados pessoais do utilizador, incluindo o nome e o contacto telefónico. Esta alteração permitiu uma clara separação entre o processo de *login* e o de criação de conta, melhorando a experiência do utilizador.

Outro problema identificado pelo perito foi a incoerência na utilização de termos em português e inglês. Esta questão foi resolvida uniformizando todos os termos para a língua portuguesa, garantindo consistência linguística em toda a aplicação.

Relativamente ao *design* da aplicação, o perito indicou que devia ser evitado o uso das caixas retangulares em redor dos títulos, visto que pareciam botões, podendo causar confusão. O mesmo problema verificou-se no menu inicial, no botão com o termo “Cuidadores”. Esta questão foi corrigida, através da remoção destas caixas retangulares.

Uma das funcionalidades principais do sistema é a geração de palavras-passe fortes. Inicialmente, esta funcionalidade estava disponível apenas num ecrã específico, não estando acessível nos ecrãs de criação ou atualização de credenciais, algo que o perito considerou que poderia causar constrangimentos nos utilizadores, uma vez que, caso os utilizadores pretendessem atualizar uma credencial com uma nova palavra-passe forte, tinham que saltar de ecrã em ecrã. Esta limitação foi resolvida, integrando a funcionalidade de geração de palavras-passe fortes diretamente nos ecrãs onde se cria ou atualiza uma credencial.

Após a resolução de todos os problemas detetados na primeira avaliação heurística, iniciou-se a implementação dos restantes requisitos do sistema. Uma vez implementados, foi possível realizar a segunda avaliação heurística, que é descrita detalhadamente na seguinte secção.

6.2 Avaliação Heurística do Protótipo Funcional 2

O objetivo desta avaliação foi validar o protótipo com o público-alvo ao nível da facilidade de utilização, servindo também como teste piloto para uma avaliação em maior escala. O perito

Idoso	Idade	Género	Grau Académico	Dificuldade em memorizar?
1	63	Feminino	4º classe	Sim
2	61	Masculino	4º classe	Sim
3	75	Feminino	Licenciatura	Não
4	75	Masculino	4º classe	Sim
5	60	Masculino	6º classe	Sim
6	62	Feminino	4º classe	Sim
7	61	Masculino	9º classe	Não
8	72	Feminino	4º classe	Sim
9	81	Feminino	4º classe	Sim

Tabela 6.1: Idosos que participaram na avaliação intercalar.

voltou a avaliar este protótipo com foco na usabilidade do mesmo. Todo o *feedback* recebido foi incorporado na versão final do protótipo. Procurou-se garantir que todos os requisitos iniciais do projeto fossem cumpridos e que as funcionalidades desenvolvidas fossem suficientemente claras.

6.2.1 Participantes

Nesta fase, participaram nove voluntários, quatro homens e cinco mulheres, todos com um nível mínimo de escolaridade equivalente à 4.^a classe, com uma média de idades de 68 anos. Os dados demográficos detalhados encontram-se na Tabela 6.1. Além das informações demográficas, verificámos que apenas dois dos nove idosos consideraram que não possuíam dificuldades em memorizar palavras-passe e PINs, sendo a justificação destes o facto de utilizarem sempre as mesmas credenciais para todas as plataformas. Nenhum dos participantes conhecia a existência de gestores de palavras-passe, mas, após a explicação do que se tratava, sete idosos indicaram que confiariam nestes sistemas, enquanto os restantes manifestaram uma atitude recetiva, mas cautelosa. Outro dado relevante foi que todos os idosos recorriam a familiares, como filhos e netos, para ajuda na gestão das suas credenciais.

6.2.2 Metodologia

Para cada idoso, esta fase da avaliação começou com uma breve introdução ao sistema, onde foram apresentados os motivos do seu desenvolvimento e os principais objetivos estabelecidos. Também solicitámos o consentimento dos idosos para a recolha dos seus dados. Posteriormente, foi apresentada uma lista de questões, as quais foram denominadas por questões pré-testes. Estas perguntas abrangem dados demográficos dos utilizadores e questões essenciais para compreender as suas necessidades em relação ao sistema, incluindo itens do modelo *Senior Technology Acceptance Model* (STAM) [11] e questões específicas sobre a proteção dos idosos *online*, como a gestão das suas palavras-passe. Estas perguntas permitiram avaliar o nível de conhecimento e a percepção sobre segurança *online* neste grupo etário.

Posteriormente, foi possível os idosos testarem a aplicação destinada a eles. Nesta parte da avaliação foram realizadas as tarefas que consideramos mais importantes, onde tivemos em conta,

como métricas de avaliação, o tempo de resolução das mesmas e o número de cliques errados (sendo considerado um clique errado quando os idosos perguntavam se era determinado botão que devia ser selecionado, quando na verdade não era). No fim de cada tarefa foi também pedido ao idoso a sua avaliação da mesma, onde recorreu-se à escala *Single Ease Question* (SEQ) [48].

No final da avaliação, foi apresentado aos idosos um último questionário, desta vez recorrendo à escala *System Usability Scale* (SUS) [34], onde foi possível obtermos uma avaliação final relativamente à usabilidade da aplicação e da necessidade da mesma. Após a avaliação com os nove idosos, recorremos ao perito para consolidarmos as melhorias que deviam ser realizadas no protótipo funcional. Ao mesmo, foi apresentada a aplicação dos idosos, da mesma forma que foi apresentada ao grupo etário alvo. O perito realizou as mesmas tarefas, e ao mesmo tempo foi realizando a sua avaliação heurística, avaliação esta que se encontra no Apêndice D. O mesmo explorou outras funcionalidades da aplicação que não foram incluídas nas tarefas devido a questões de tempo. Através desta análise foi possível complementar a avaliação heurística, com melhorias a serem realizadas. Esta interação com o perito também permitiu validar as perguntas pré-testes, cujas melhorias sugeridas também foram tidas em conta. De seguida, apresentamos todos os problemas expostos pelo perito, bem como a resolução dos mesmos.

6.2.3 Resultados e Melhorias Realizadas

Após os testes com os idosos, e a avaliação heurística realizada pelo perito, foi possível obter diversos *feedbacks* relativamente a melhorias que deviam ser realizadas, nomeadamente *bugs*, termos e elementos interativos a serem melhorados.

Uma das primeiras ações realizadas por um utilizador no sistema desenvolvido é a criação de uma conta. Após o preenchimento dos dados da conta a ser criada, e ao selecionar o botão que despoleta a criação da conta, era apresentado um efeito de *loading*, que não se mantinha ativo até ao final de todo o processo, ou seja, parava antes da aplicação navegar para outro ecrã, ficando num estado difícil de compreender. Este problema suscitou confusão aos idosos, tendo sido algo que o perito também considerou que era importante resolver. Posto isto, esta alteração foi efetuada, sendo que o estado do *loading* apresentado é apenas desligado quando todo o processo de criação de conta é terminado, nomeadamente quando a aplicação navega para o ecrã seguinte.

No menu principal da aplicação destinada a idosos, inicialmente, existiam quatro botões denominados por “Credenciais”, “Nova Pass”, “Definições” e “FAQs”. Durante os testes realizados com os idosos, ficou evidente que os termos escolhidos não eram os mais adequados, mesmo quando acompanhados por uma imagem ilustrativa. A avaliação heurística realizada pelo perito confirmou este problema, uma vez que este indicou que os termos utilizados eram demasiado vagos. Considerando estas observações, os termos foram devidamente atualizados para “Gerir Cuidadores”, “Gerir Credenciais”, “Gerar Nova Palavra-passe”, e “Ajuda”, respetivamente. Para além dos termos, o posicionamento dos botões e as cores utilizadas também foram melhorados. Através da Figura 6.1 é possível visualizar a evolução deste ecrã.

Navegando até ao ecrã destinado a apresentar os cuidadores vinculados, no objeto que repre-

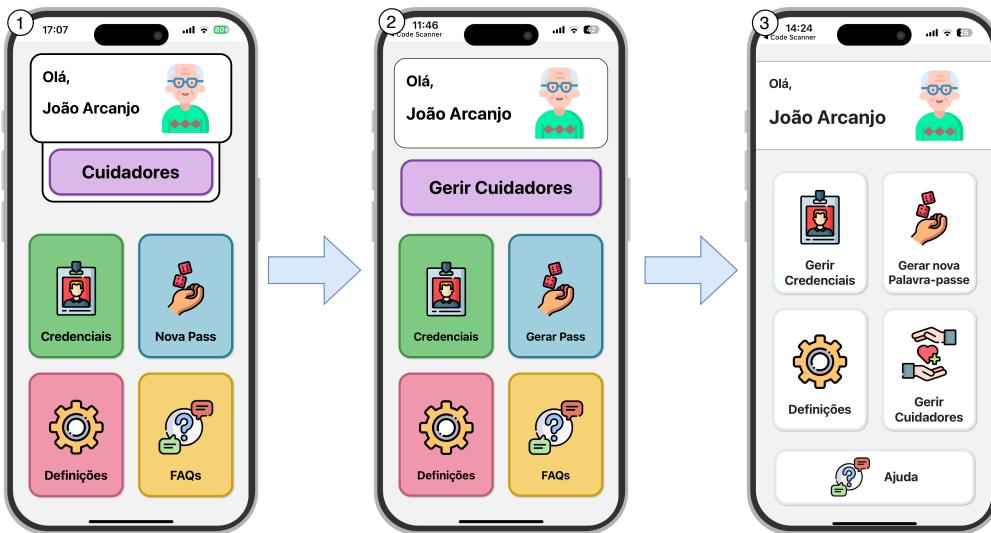


Figura 6.1: Progressão do menu inicial (melhor visto a cores).

senta o cuidador vinculado, era apresentada ao idoso a frase “Alterar credenciais?:” com um botão à frente, tal como visível no ecrã 5 da Figura 6.2. Este botão exibia o termo “Sim” em cor verde, quando o idoso permitia que o respetivo cuidador alterasse as suas credenciais, ou o termo “Não” em cor vermelha, quando o cuidador não possuía permissões para tais alterações. Para alterar as permissões, o idoso precisava selecionar o botão, conforme as suas necessidades. Durante os testes com os idosos, ficou evidente que esta funcionalidade não era intuitiva, pois frequentemente selecionavam a frase em vez do próprio botão. O especialista também considerou esta forma de atualização do estado pouco clara e recomendou substituir o botão convencional por um botão do tipo interruptor. Foi exatamente essa a melhoria que foi implementada posteriormente, onde a cor se mantém, sendo apenas alterado o tipo de botão, suficiente para tornar a funcionalidade mais intuitiva, tal como visível no ecrã 6.

Uma vez que o perito considerou que as cores usadas neste ecrã não eram adequadas, essas foram alteradas, bem como alguns textos mais importantes ficaram a *bold* de modo a ficarem mais destacados, tal como visível nos diversos ecrãs da Figura 6.2, nomeadamente os ecrãs 2, 4 e 6.

O ecrã disponibilizado aos utilizadores para adicionar uma credencial também apresentou alguns problemas durante os testes e a avaliação heurística. O sistema, uma vez que permite aos utilizadores adicionar tanto credenciais do tipo *login* como credenciais do tipo cartão, era necessário disponibilizar ao utilizador dois formulários, um para cada um dos tipos. A primeira solução implementada consistia em dois botões no topo do formulário, um com o termo “Login” e outro com o termo “Cartão”, acompanhados por uma seta que apontava para o botão que correspondia ao formulário ativo, funcionalidade visível nos ecrãs 1 e 2 da Figura 6.3. No entanto, durante os testes com os idosos e na avaliação realizada pelo perito, tornou-se evidente que esta abordagem era problemática. A seta sugeria a existência de uma sequência de passos, o que não correspondia à realidade. Além disso, se o formulário de uma nova credencial de “Cartão” estivesse preenchido e o botão “Login” fosse selecionado, todo o conteúdo do formulário era apagado.

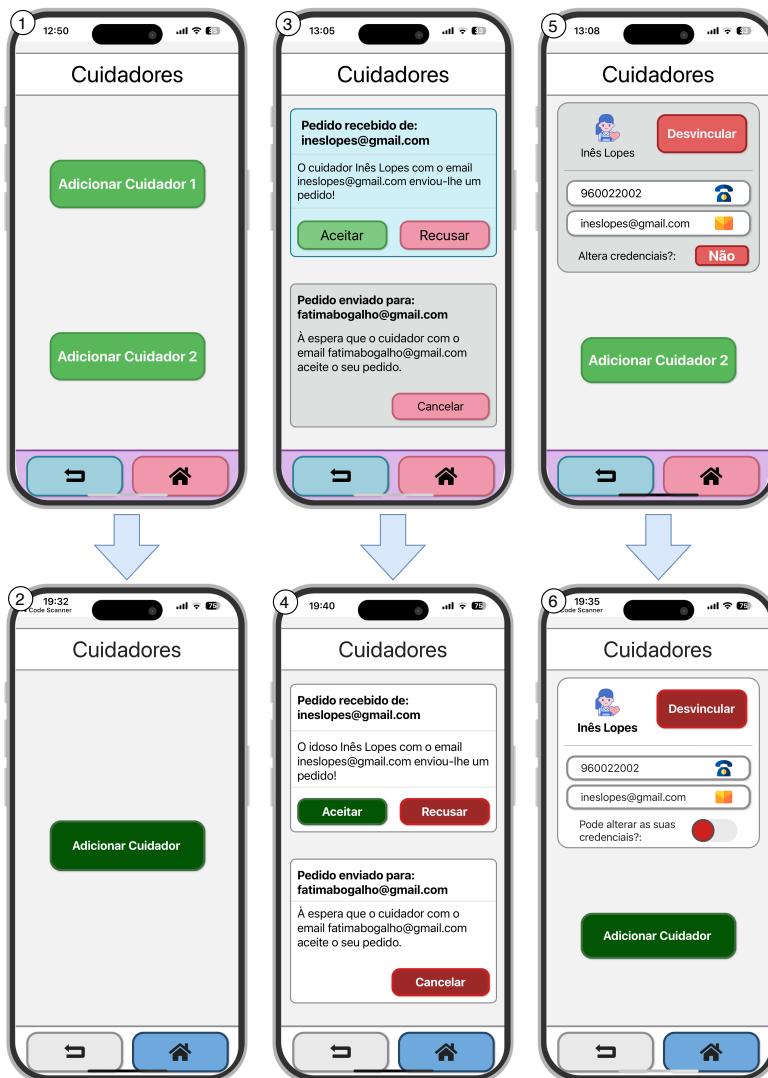


Figura 6.2: Evolução da página com a informação dos cuidadores (melhor visto a cores).

Para resolver este problema, utilizámos a sugestão do perito. O botão para adicionar uma nova credencial que se encontra na página de listagem de credenciais, ao ser selecionado gera um *popup* que é apresentado ao utilizador com as opções “Login” e “Cartão”. Somente após a seleção de uma dessas opções é que o formulário correspondente é disponibilizado, ou seja, o formulário representado pelo ecrã 3 ou 4 da Figura 6.3, evitando os problemas identificados anteriormente. Uma pequena inconsistência foi detetada pelo perito neste ecrã, relativamente ao estado do ícone para mostrar/ocultar os campos considerados segredos, ou seja, encontrava-se em modo “ocultar” quando o segredo já estava oculto e em modo “mostrar” quando o segredo já estava a ser mostrado. Esta inconsistência foi devidamente corrigida.

Uma das funcionalidades presentes é a possibilidade dos campos denominados por *Plataforma* e *URL* serem automaticamente preenchidos, apresentando aos utilizadores uma lista de alternativas para tal efeito. A primeira solução implementada consistia em colocar, do lado direito do campo *Plataforma*, uma varinha mágica que, ao ser selecionada, apresentava um *popup* com uma lista

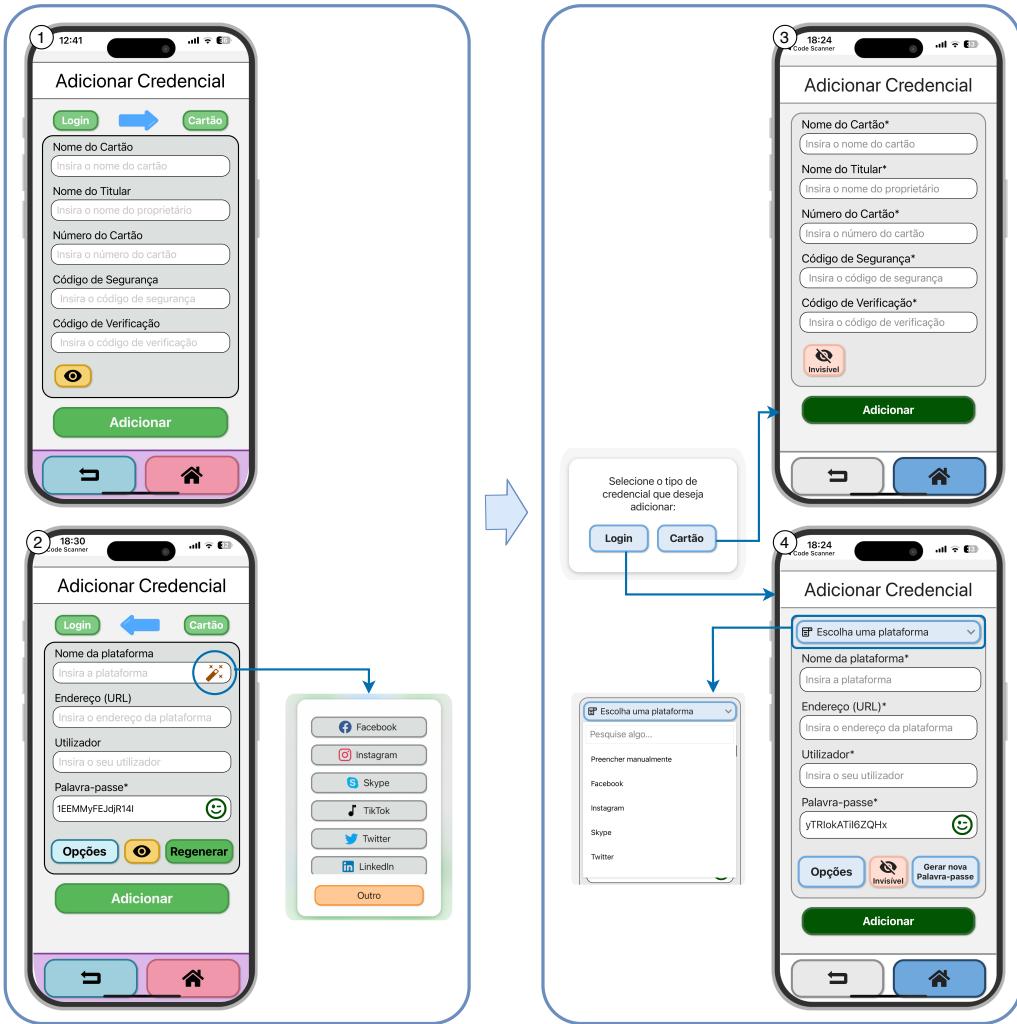


Figura 6.3: Evolução da página para adicionar uma credencial (melhor visto a cores).

de possíveis plataformas para o pré-preenchimento do formulário, tal como é visível no ecrã 2 da Figura 6.2. Durante os testes, ficou evidente que o ícone da varinha não era familiar para os idosos, uma limitação também apontada pelo perito. Para mitigar esse problema, o ícone da varinha foi substituído por um botão, com o texto “Escolher uma plataforma”, que, quando selecionado, apresenta ao utilizador uma *dropdown* com a lista de plataformas, acompanhadas por um campo que possa ser utilizado para ajudar na pesquisa pelas mesmas, tal como é visível no ecrã 4 da Figura 6.2. Esta mudança ajuda a entender a funcionalidade do botão e desperta a curiosidade dos utilizadores para seleccioná-lo, permitindo-lhes tirar partido da funcionalidade.

Após a criação de uma credencial, é possível editá-la ou apagá-la no ecrã que apresenta os detalhes da própria credencial. A ação de apagar era realizada recorrendo a um botão cujo termo variava conforme o tipo de credencial: “Apagar Login” para credenciais do tipo “Login” e “Apagar Cartão” para credenciais do tipo “Cartão”. De acordo com o perito, esse dinamismo tornava a interface menos consistente e clara. A recomendação foi utilizar o termo “Apagar Credencial” para ambos os tipos de credenciais.

Ao longo de toda a aplicação, também era evidente o uso das palavras *username* e *password*. Apesar de muito usados globalmente, estes termos foram considerados uma limitação pelo perito, especialmente para idosos que não estão familiarizados com a língua inglesa. Foi recomendado substituir esses termos por “utilizador” e “palavra-passe” em todo o sistema. Além disso, dado que diferentes plataformas podem usar outros termos para “utilizador” e “palavra-passe”, como “e-mail” ou “nº de telemóvel”, para o caso de “utilizador” e “PIN” para o caso da “palavra-passe”, foi aconselhado que o sistema adaptasse os termos de acordo com a plataforma escolhida pelo utilizador. Assim, a solução desenvolvida foi a seguinte: se o nome da plataforma escolhida pelo utilizador contiver um nome conhecido pelo nosso sistema, a aplicação vai indicar o que a plataforma em questão pretende receber no campo “utilizador” e no campo “palavra-passe”. Por exemplo, se o utilizador escolher a plataforma *Facebook*, o sistema vai indicar que, para o nome do utilizador, a plataforma aceita ou o e-mail, ou o nº de telemóvel. Estas adaptações visam tornar a aplicação mais acessível para os idosos, reduzindo possíveis confusões e facilitando a utilização de diferentes plataformas.

No ecrã destinado a listar todas as credenciais do utilizador, foi identificada a necessidade de criar um método de filtragem devido à quantidade elevada de credenciais que podem ser criadas. Assim, foi implementado um filtro baseado no tipo de credencial a ser apresentada. Inicialmente, este método utilizava um botão cuja cor e símbolo mudavam conforme a seleção, e a lista de credenciais apresentada variava de acordo com o que o botão representava. Por exemplo, para listar todas as credenciais, era apresentado o símbolo de infinito; para cartões, o símbolo de um cartão; e para credenciais de *login*, o típico símbolo de utilizador, tal como visível no ecrã 2 da Figura 6.4. No entanto, o perito considerou que o uso desses símbolos, sem qualquer descrição adicional, não era muito claro, especialmente o símbolo de infinito. A resolução deste problema é visível no ecrã 3 da Figura 6.4, onde foi implementada uma solução que consiste num botão com uma seta a apontar para baixo, acompanhada com o termo “Filtros”. Quando selecionado, este botão, para além da seta ficar a apontar para cima e o termo alterar para “Ver menos”, é também apresentado ao utilizador três novos botões. Nestes botões mantiveram-se os símbolos tendo em conta o tipo que representam, mas, como não eram claros por si só, foram acompanhados por termos, ou seja, “Todas”, “Cartões” e “Login”. A primeira opção, “Todas”, encontra-se selecionada por defeito, representando a lista de todas as credenciais. Essa abordagem melhora a usabilidade do filtro, permitindo que os utilizadores entendam facilmente as opções disponíveis e selecionem a categoria de credenciais que desejam visualizar.

A lista de credenciais é composta por uma série de componentes, onde cada um representa uma credencial distinta. Cada componente possuía um botão com o termo “Ações” que, ao ser selecionado, apresentava um *popup* com três botões: “Copiar utilizador”, “Copiar credencial” e “Navegar”. Tanto os testes com os idosos como a avaliação heurística do perito revelaram que esta solução não era viável, pois não era claro o que o botão “Ações” faria. Para melhorar esta funcionalidade, foi seguida a recomendação do perito. Em cada componente de cada credencial, foi adicionado um botão com uma seta a apontar para cima, complementada pelo termo “Ver



Figura 6.4: Evolução da página para listar as credenciais existentes

mais”. Ao ser selecionado, a seta altera, ficando a apontar para baixo e com o termo “Fechar”, e são apresentados ao utilizador três botões, dentro do próprio componente e sem qualquer tipo de *popup*. Esses botões mantêm as mesmas ações que os da implementação anterior, mas os termos utilizados agora descrevem as ações de forma mais clara: “Copiar nome de utilizador”, “Copiar palavra-passe” e “Aceder à aplicação”.

No ecrã anteriormente denominado “FAQs”, agora denominado “Ajuda”, mais precisamente na secção dos tutoriais, além do texto que descreve passo a passo, o necessário para realizar cada tarefa, é, ainda, acompanhado por um vídeo, sendo que, para visualizar o mesmo, era necessário selecionar um botão que redirecionava para a plataforma *YouTube*. Este redirecionamento poderia assustar utilizadores menos experientes ou fazê-los sentir-se obrigados a utilizar uma aplicação externa que podem não ter ou querer usar. Esta funcionalidade foi melhorada sem a necessidade de guardar os vídeos localmente no dispositivo do utilizador e sem obrigar os utilizadores a recorrer a outra aplicação para visualizar os vídeos. A solução adotada foi utilizar o componente de *Video Player* do respetivo sistema operativo, que permite apresentar um vídeo sem ser necessário sair da aplicação.

6.3 Avaliação da Usabilidade do Protótipo Funcional Final

Nesta secção, apresentamos a avaliação do protótipo funcional final com os idosos, incluindo a metodologia aplicada, a caracterização dos participantes envolvidos, e os resultados obtidos.

6.3.1 Metodologia

A avaliação foi realizada com idosos com 60 anos ou mais, que utilizassem um *smartphone*. Todas as sessões foram conduzidas presencialmente, no local onde os idosos preferissem, garantindo um ambiente em que se sentissem confortáveis.

Cada sessão realizada teve início com uma breve introdução ao trabalho desenvolvido e aos seus objetivos. Agradecemos aos participantes pelo interesse e colaboração, salientando que quaisquer dúvidas seriam esclarecidas e que todos os dados recolhidos seriam anonimizados e analisados posteriormente pela equipa de investigação. Solicitámos o consentimento dos idosos para a gravação do áudio da sessão, com o objetivo de permitir uma análise mais aprofundada. Pedimos também a captação de uma fotografia, a ser utilizada pelo investigador no final do estudo como forma de agradecimento a todos os que contribuíram para o projeto.

Posteriormente, solicitámos o consentimento dos idosos para preencherem um questionário composto por questões demográficas e questões relacionadas com o modelo STAM. Incluímos também perguntas que considerámos relevantes para entender como é que esta faixa etária utiliza e gera as suas credenciais, como se sente ao usá-las e se considera que os seus métodos são suficientes para garantir a proteção no mundo *online*.

Em seguida, os idosos realizaram uma sessão experimental, onde lhes foi pedido para executarem um conjunto de tarefas e que utilizassem a técnica *think-aloud* (para comentarem a sua experiência enquanto realizavam a tarefa). Para cada tarefa, os idosos foram avaliados tendo em conta duas métricas distintas: tempo necessário para completarem a tarefa e o número de cliques incorretos durante a execução. Cenários em que o idoso demonstrou a intenção de clicar num botão e aguardar a confirmação do avaliador, foram considerados como um clique errado. Depois de cada tarefa, o idoso avaliou a execução da mesma, recorrendo à escala SEQ. Para a realização dos testes, utilizámos os seguintes cenários de tarefas:

- T_1 : Para utilizar a aplicação, é necessário registar-se na mesma. Utilize o nome “Pedro”, o email “pedro1@gmail.com”, o telefone “912345678” e a palavra-passe “teste123”;
- T_2 : Decidiu modificar a sua palavra-passe da conta do Facebook, mas quer garantir que ela é segura e que não se esquece da mesma, então decide utilizar a aplicação para adicionar uma credencial. Utilize o nome da plataforma “Facebook”, o URL “www.facebook.com”, o nome de utilizador “pedro”, e escolha uma palavra-passe forte;
- T_3 : A sua aplicação do Facebook alertou-o que alguém tentou entrar na sua conta, por isso pediu-lhe que inserisse as suas credenciais novamente. Uma vez que possui esses dados guardados na aplicação, recorra aos mesmos para realizar *login* na sua conta do Facebook;

- T_4 : Visto que tentaram entrar na sua conta do facebook, sentiu a necessidade de alterar a sua palavra-passe por precaução. Realize essa alteração na aplicação;
- T_5 : Uma vez que o seu neto é a pessoa que o ajuda na gestão das suas credenciais, convide-o para que ele seja o seu cuidador na aplicação, sendo o seu email: neto123@gmail.com;
- T_6 : O seu neto está com muito trabalho e não o pode ajudar durante uns meses. Desvincule-se dele de modo a que ele deixe de ter acesso aos seus dados.

Após a conclusão de todas as tarefas, cada participante foi convidado a preencher o SUS para avaliar a usabilidade do sistema desenvolvido.

6.3.2 Participantes

Participaram nesta avaliação 17 idosos, dos quais 8 do sexo masculino e 9 do sexo feminino. Na Tabela 6.2 são apresentados outros dados demográficos dos participantes. A partir das respostas dos idosos, verificou-se que apenas um não utiliza um *smartphone* há mais de 7 anos. Em contraste, o tempo diário de uso do *smartphone* varia significativamente entre os participantes: 1 idoso afirmou utilizá-lo por menos de 1 hora, 9 relataram um uso entre 1 e 3 horas, enquanto os 7 restantes indicaram utilizá-lo por mais de 3 horas diariamente.

Com base em algumas das perguntas realizadas com o âmbito de analisar a adoção da tecnologia por esta faixa etária, foi possível concluir que a maioria dos idosos concorda que a tecnologia tem um impacto positivo nas suas vidas, destacando que facilita o seu dia a dia e proporciona diversos benefícios. Entre as afirmações mais comuns encontram-se: “A tecnologia foi criada para nos evoluir”, “Ajuda-nos a lembrar ocorrências e datas antigas...”, “Manter o contacto com as pessoas”, “Combater o isolamento”, “Facilitar o nosso dia a dia”, “Serve para o nosso entretenimento” e “Consegue salvar pessoas que precisem de ajuda”. Além disso, um dos participantes sublinhou: “Dominando minimamente a tecnologia, uma pessoa tem mais à mão tudo o que precisa, é mais fácil”.

Apesar dos benefícios identificados, as desvantagens da tecnologia foram motivo de opiniões mais divididas. Oito idosos atribuíram respostas iguais ou inferiores a 3, numa escala de *Likert*, a uma pergunta que pretendia avaliar se concordavam com a existência de desvantagens na utilização da tecnologia. “As vantagens anulam as desvantagens” e “Se não usarmos a tecnologia, temos de utilizar métodos menos seguros”, foram algumas das justificações. Por outro lado, os restantes participantes expressaram preocupações como “Ficarmos completamente dependentes da tecnologia, não lemos, não puxamos pela memória, nem fazemos um esforço para recordar as coisas”, “Podemos sofrer burlas”, “Podemos sofrer ataques de *phishing*”, “Podemos ser enganados por vi-garistas”, “Comunicamos com pessoas com poucos princípios”, “É mais fácil sermos enganados quando estamos sozinhos” e “Se ficarmos sem bateria, ficamos sem acesso a nada”.

No que diz respeito à segurança, apenas 2 idosos relataram ter tido uma experiência negativa relacionada com o acesso não autorizado às suas contas. Contudo, 13 idosos afirmaram que não são alvos fáceis para possíveis atacantes, justificando essa confiança com o facto de se conside-

rarem desconfiados e conservadores. Em contraste, 3 participantes reconheceram que podem ser alvos fáceis, enquanto um outro manifestou incerteza, argumentando que o que pode ser seguro para ele, pode não o ser para outros, dada a rápida evolução tecnológica.

Como o nosso sistema propõe oferecer uma alternativa segura aos métodos atualmente utilizados pelos idosos, questionámos os participantes sobre como costumam armazenar as suas palavras-passe. A maioria dos idosos recorre à sua própria memória para guardar as credenciais, sendo esta a escolha de 7 dos 17 participantes. Outros métodos incluíram o uso de cadernos, mencionado por 5 participantes, o recurso a terceiros, relatado por 3 idosos, e a utilização de gestores de palavras-passe, referido por 2 participantes. Além disso, metade dos entrevistados revelou que conta com a ajuda de outra pessoa para gerir as suas credenciais, sendo filhos, netos e cônjuges as opções mais comuns nesta faixa etária.

Idoso	Idade	Género	Grau Académico	Dificuldade visual	Horas diárias
1	67	Masculino	9º ano	Hipermetropia	1 - 3 horas
2	64	Masculino	12º ano	Hipermetropia	1 - 3 horas
3	74	Feminino	4º classe	Hipermetropia	- 1 hora
4	72	Feminino	4º classe	Hipermetropia	+ 3 horas
5	65	Feminino	12º ano	Hipermetropia	1 - 3 horas
6	70	Masculino	4º classe	Hipermetropia	1 - 3 horas
7	63	Masculino	Licenciatura	Nenhuma	1 - 3 horas
8	61	Feminino	Licenciatura	Hipermetropia e Miopia	+ 3 horas
9	62	Masculino	12º ano	Miopia	+ 3 horas
10	76	Feminino	4º classe	Hipermetropia e Miopia	+ 3 horas
11	76	Feminino	4º classe	Miopia	1 - 3 horas
12	80	Masculino	4º classe	Hipermetropia e Miopia	+ 3 horas
13	63	Masculino	12º ano	Miopia	1 - 3 horas
14	63	Feminino	11º ano	Hipermetropia e Miopia	1 - 3 horas
15	73	Masculino	Licenciatura	Hipermetropia e Miopia	1 - 3 horas
16	71	Feminino	4º classe	Nenhuma	+ 3 horas
17	68	Feminino	12º ano	Hipermetropia	+ 3 horas

Tabela 6.2: Idosos que participaram na avaliação final.

Dez dos 17 idosos sabem o que faz uma palavra-passe ser considerada forte. Após esclarecermos os restantes idosos no que é que consiste uma palavra passe ser considerada forte, concluímos que apenas 5 consideram todas as suas palavras-passe fortes. Três idosos consideram que apenas algumas palavras-passe são fortes, sendo influenciados pela obrigatoriedade imposta pela plataforma, pela importância da mesma e pelo *feedback* fornecido sobre a força da palavra-passe escolhida. Os restantes 9 idosos consideram que as suas palavras-passe não são fortes de todo.

Para concluir, 7 dos 17 idosos afirmaram não conhecer qualquer método seguro para armazenar as suas credenciais. Entre os restantes, 7 consideram a memória uma opção segura, um idoso confia no recurso ao papel, e os 2 utilizadores atuais de gestores de palavras-passe consideram essas ferramentas seguras. Quando questionados sobre o conhecimento acerca de gestores de palavras-passe, apenas 6 dos 17 idosos sabiam em quê que consistem. Relativamente à disposição para usar este tipo de sistema, 7 idosos mostraram-se indecisos, expressando algum receio e apreensão. No

entanto, 8 participantes afirmaram que estariam dispostos a utilizar um gestor de palavras-passe, desde que fosse considerado seguro. Dois idosos indicaram que não recorreriam a esse tipo de sistema, embora tenham aceite testar a aplicação para avaliar as suas vantagens.

Em relação ao uso do STAM, as perguntas realizadas com o objetivo de se entender a aceitação dos idosos em relação à tecnologia e ao sistema desenvolvido focaram-se nos *constructs Attitude towards using* (AT), *Perceived Usefulness* (PU), *Perceived Ease of Use* (PEOU), *Gerontechnology Self-efficacy* (SE) e *Gerontechnology Anxiety* (ANX). Através da Figura 6.5 é possível visualizar tanto as perguntas realizadas bem como um diagrama de extremos e quartis que representa a distribuição das respostas obtidas nas mesmas (em que 1 discordo totalmente e 5 concordo totalmente). Através deste diagrama é possível concluir que os idosos tiveram respostas bastante semelhantes nas perguntas dos *constructs* AT, PU, PEOU e SE, havendo uma maior dispersão de opiniões no construtor ANX, evidenciando variações no nível de ansiedade percebida em relação à tecnologia. Os losangos indicam a presença de valores discrepantes. Para todos os *constructs*, foi calculado o α de Cronbach, uma medida de consistência interna ou fiabilidade de um conjunto de itens pertencentes ao questionário. Este índice avalia o grau de correlação entre as perguntas que visam medir o mesmo conceito. O α de Cronbach para o *construct* AT foi de 0.89, PU obteve 0.94, PEOU apresentou 0.92, SE registou 0.86 e ANX alcançou 0.97, indicando elevada fiabilidade em todos os *constructs*. Os resultados sugerem que os idosos apresentaram uma atitude positiva em relação ao uso da tecnologia, percebem a utilidade da mesma e demonstram confiança nas suas capacidades. No entanto, a dispersão observada no *construct* ANX aponta para diferentes níveis de ansiedade entre os participantes, o que pode refletir a necessidade de abordar a ansiedade de forma personalizada para garantir uma maior inclusão e aceitação da tecnologia entre os idosos.

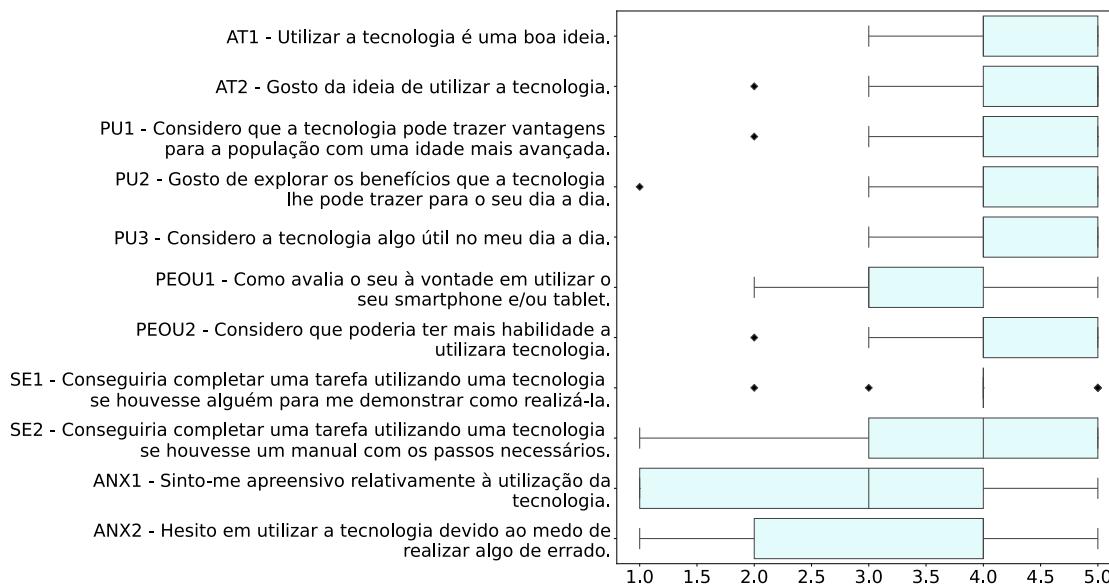


Figura 6.5: Resultados recolhidos para cada *construct* AT, PU, PEOU, SE e ANX, do STAM (melhor visto a cores).

6.3.3 Resultados Experimentais

Esta secção, apresenta a performance dos idosos para cada tarefa descrita anteriormente, e, por fim, os resultados do SUS. A Tabela 6.3 apresenta os resultados das tarefas realizadas pelos idosos. Para cada tarefa, são indicados o tempo médio de execução e respetivo desvio padrão, a média de cliques incorretos e o respetivo desvio padrão, bem como a média das respostas ao questionário SEQ, também com o desvio padrão. O SEQ é avaliado numa escala de 1 a 7, onde valores mais elevados indicam que os idosos consideraram a tarefa mais fácil de executar.

	Tarefa 1	Tarefa 2	Tarefa 3	Tarefa 4	Tarefa 5	Tarefa 6
Tempo	113.7 ± 38.9 s	92.9 ± 28.3 s	71.9 ± 35.6 s	52.1 ± 19.1 s	44.0 ± 37.4 s	6.7 ± 3.1 s
Nº Cliques errados	0.4 ± 0.5	0.7 ± 1.0	1.3 ± 1.1	1.1 ± 1.1	0.4 ± 0.7	0 ± 0
SEQ	6.1 ± 0.9	5.4 ± 1.2	5.1 ± 1.6	6.2 ± 1.2	6.4 ± 1.0	6.4 ± 0.8

Tabela 6.3: Resultados dos idosos na execução das tarefas.

A partir dos resultados apresentados na tabela, pode-se concluir que a maioria das tarefas foi concluída com êxito pelos idosos. Contudo, foi notório que, em algumas situações, os participantes não analisavam completamente a interface antes de interagir, o que resultou num aumento de cliques errados. Além disso, embora o uso do teclado não fosse extensivo, os idosos mostraram-se bastante cautelosos ao preencher certos campos, o que contribuiu para uma maior demora na conclusão de algumas tarefas. De acordo com os resultados do SEQ, as tarefas 2 e 3 receberam uma avaliação inferior. No entanto, os idosos que encontraram maior dificuldade afirmaram que estas dificuldades resultaram da sua primeira interação com o sistema e de estarem a realizar algo fora da sua rotina habitual.

Através do SUS, obtivemos uma média de 81.3 (*Grade A*), que sugere que os idosos consideraram o nosso sistema fácil de usar. Através da Figura 6.6 é possível visualizar tanto as perguntas realizadas bem como um diagrama de extremos e quartis que representa a distribuição das respostas. Quanto à fiabilidade dos nossos resultados, os coeficientes de consistência interna apresentaram um α de Cronbach de 0.90 para as questões pares e de 0.95 para as questões ímpares.

6.3.4 Conclusões Finais

Muitos idosos consideram que utilizar palavras-passe baseadas em memórias pessoais é uma estratégia fácil e eficaz, sendo o mais importante para eles a capacidade de se lembrarem das mesmas. No entanto, alguns aventuraram-se na criação de palavras-passe com palavras aleatórias ou mnemónicas, mas começaram a sentir-se limitados por certas plataformas que exigem o uso de caracteres especiais, um número mínimo de caracteres, entre outros requisitos.

Após a utilização do nosso sistema, os idosos apreciaram a ideia de ter um local considerado seguro onde pudessem armazenar as suas palavras-passe, libertando-os da necessidade de as memorizar. Valorizaram, ainda, o facto de o sistema ter sido desenvolvido especificamente para atender às suas necessidades. Além disso, destacaram a importância da vinculação com o

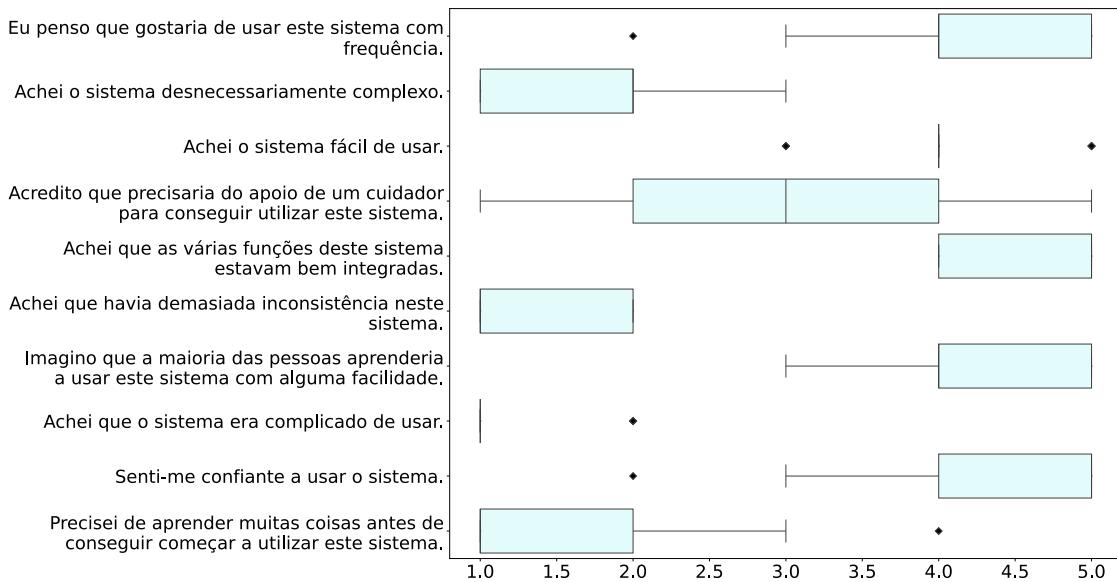


Figura 6.6: Resultados recolhidos para cada pergunta do SUS (melhor visto a cores).

cuidador, uma vez que os familiares, devido a uma vida ocupada ou à distância geográfica, muitas vezes não dispõem de um método que lhes permita prestar esse apoio de forma remota. Os idosos também realçaram que, quando um deles falece, os familiares frequentemente enfrentam dificuldades para apagar a pegada digital deixada pelo falecido, um processo que o sistema poderia facilitar consideravelmente.

Antes de concluir a sessão, os idosos foram questionados se possuíam alguma observação final sobre o que lhes foi apresentado. Embora a maioria tenha afirmado que não tinha nada a acrescentar, ou apenas desejasse sucesso e boa sorte ao projeto, alguns deixaram observações relevantes. Um dos participantes sugeriu a vinculação do sistema a uma identidade do Governo, permitindo que a identidade tanto do cuidador como do idoso fosse registada, e a relação entre ambos fosse reconhecida noutras plataformas, garantindo maior autenticidade nas interações. Outro idoso, ao notar que a aplicação requer uma palavra-passe para o registo, e que essa palavra-passe pode ser alterada posteriormente, sugeriu que, caso dois cuidadores de um idoso concordassem, pudessem realizar um *reset* à palavra-passe do idoso, caso este a alterasse por engano e se tivesse desconectado da aplicação. Um participante destacou a importância de reforçar a segurança, comparando a situação a um “jogo do gato e do rato”, em que, enquanto houver quem tente tirar proveito das falhas, é essencial dificultar-lhes a tarefa com medidas de segurança mais robustas. Outro mencionou que, apesar de geralmente sentir receio de usar certas aplicações por causa da complexidade das interfaces e de considerar que tem conhecimento limitado sobre o tema, achou esta aplicação bastante fácil de utilizar. Houve também quem reconhecesse que algumas tarefas iniciais podem parecer complicadas, mas reforçou a importância de se esforçar e aprender, especialmente quando o objetivo é proteger-se melhor. Além disso, foi apontado que os telemóveis muitas vezes não são projetados com os idosos em mente, seja para aqueles com dificuldades de visão, seja pela presença de aplicações desnecessárias. Por isso, consideraram importante que iniciativas como

esta tenham em conta os problemas comuns a esta faixa etária. Outro utilizador destacou a utilidade da aplicação em permitir que mais de um cuidador seja vinculado à gestão das credenciais, facilitando a relação entre os idosos e seus cuidadores. Por fim, um idoso comparou a experiência com a aplicação ao “jogo do Pião”, comentando que, embora inicialmente pareça complicada, com o tempo, tudo se torna mais simples.

6.4 Avaliações do Desempenho do Protótipo Funcional Final

Nesta secção, apresentamos os testes de desempenho realizados sobre o protótipo funcional final, onde abordamos tanto o ambiente em que foram realizados os testes como os resultados obtidos.

6.4.1 Ambiente

Durante os testes de desempenho, foi criado um ambiente que simulava um cenário comum para a maioria dos potenciais utilizadores. Foi gerado um APK da aplicação e instalado num *smartphone* com sistema operativo *Android*. O processador utilizado é o *Qualcomm Technologies, Inc.* *SDM765G 5G*, composto por 8 núcleos com uma arquitetura *Kryo 475* e com velocidade variável entre 300 MHz e 2.40 GHz. A rede utilizada possui uma velocidade de *download* e *upload* de aproximadamente 180 Mbps e 151 Mbps respetivamente, e uma latência de 4 ms.

Para avaliar o desempenho das funcionalidades, foi introduzida uma medida de tempo no início de cada função. Esta medida capta o *timestamp* do momento em que a função começou a ser executada. Posteriormente, no final da execução da mesma, outro *timestamp* foi capturado, registando o momento em que a função terminou. Com base nestes *timestamps*, foi possível determinar o tempo de execução de cada funcionalidade.

De seguida, apresentamos os tempos de execução obtidos para cada uma das funcionalidades testadas. Cada cenário foi executado dez vezes, sendo que os resultados apresentados correspondem à média e ao desvio padrão dessas dez execuções.

6.4.2 Validação das credenciais

Nesta secção, são apresentados os tempos que a função responsável pela validação das credenciais necessita para ser executada, recorrendo a quatro cenários distintos, com diferentes escalas de número de credenciais a serem processadas, nomeadamente 1, 5, 10, 25, 50, 75 e 100 credenciais.

O primeiro cenário remete ao cenário ideal. Neste, as credenciais que o utilizador possui armazenadas localmente são as mesmas que as credenciais armazenadas no servidor destinado a tal. Posto isto, a função limita-se, neste caso, a interpretar as credenciais presentes no servidor, validar a encriptação e assinatura de cada uma, e verificar se os dados são iguais aos que se encontram armazenados localmente. Relativamente aos resultados, os tempos de resposta variaram com o número de credenciais. Com uma única credencial, a média foi de 149.4 ± 32.3 ms.. Para 25 credenciais, a média foi de 344.4 ± 30.2 ms, enquanto com 50 credenciais a média subiu para 647.8 ± 56.2 ms. Por último, com 100 credenciais, a média foi de 1230.7 ± 13.5 ms.

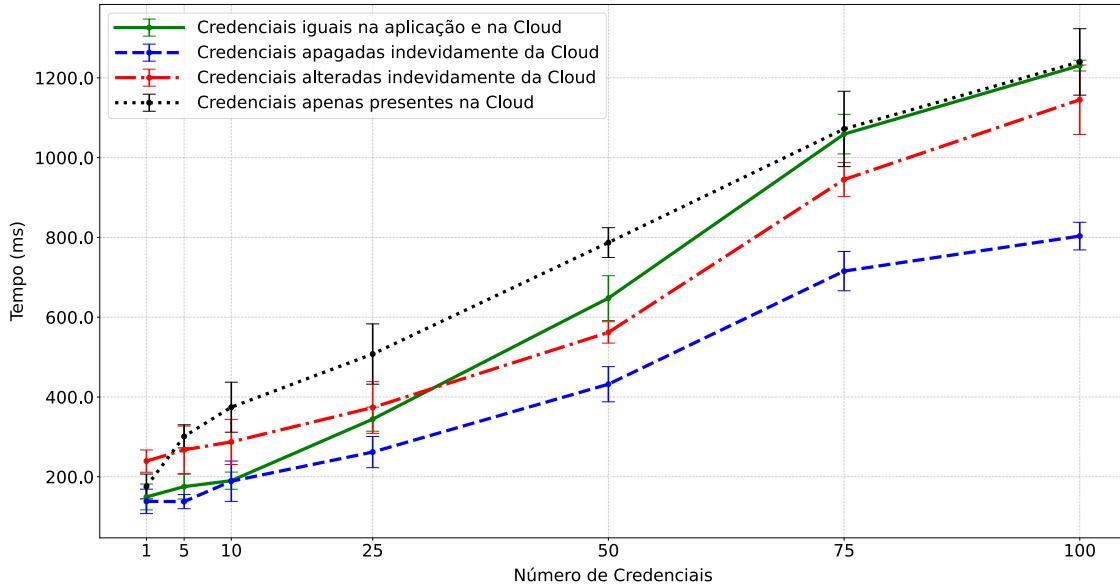


Figura 6.7: Comparação dos tempos médios para diferentes situações de manipulação indevida das credenciais (melhor visto a cores).

O segundo cenário remete para o caso em que toda a coleção de credenciais do utilizador foi, indevidamente, apagada do servidor. Este é também o cenário que exige menos do sistema, visto que a aplicação, simplesmente, volta a colocar no servidor aquilo que possui armazenado localmente. Para que este cenário fosse possível, utilizou-se o portal da *Firebase* com a conta de administrador para apagar manualmente toda a coleção de credenciais da conta do utilizador de teste. Como referido anteriormente, a funcionalidade começa por obter todas as credenciais do servidor, e, uma a uma, compara com a credencial que se encontra localmente. Posto isto, dado não existir nenhuma credencial no servidor, a função vai obter todas as credenciais que se encontram armazenadas localmente e são replicadas para o servidor. Relativamente aos resultados, os tempos de resposta também variam com o número de credenciais utilizadas. Com uma única credencial, o tempo médio foi de 138.3 ± 30.6 ms. Para 25 credenciais, foi de 261.9 ± 39.1 ms, enquanto para 50 credenciais foi de 432.0 ± 44.1 ms. Por fim, com 100 credenciais, o tempo médio foi de 803.3 ± 34.6 ms.

O terceiro cenário remete para o caso em que todas as credenciais do utilizador, que se encontram no servidor, foram alteradas individualmente. De forma a criarmos o cenário de teste, foi realizada a alteração no servidor de todas as credenciais do utilizador que pretendemos testar. Ao contrário do caso anterior, esta alteração não foi realizada manualmente no portal, uma vez que para testar a mesma, eram necessárias mais de duas mil operações manuais de atualização através do portal. Portanto, recorremos a um servidor em *NodeJS* com uma chave de administrador da *Firebase*, que, através da execução de uma função, realizou as alterações pretendidas. Posto isto, a aplicação do utilizador, ao obter todas as credenciais do servidor, e ao analisar uma a uma, verificou que todas se encontravam inválidas. Posteriormente, a aplicação atualiza o servidor com os dados que se encontram armazenados localmente. Relativamente aos resultados, com uma

única credencial, o tempo médio foi de 239.3 ± 27.9 ms. Para 25 credenciais, foi de 373.6 ± 64.8 ms, para 50 credenciais foi de 561.8 ± 26.8 ms, e para 100 credenciais, o tempo médio foi de 1145.0 ± 86.9 ms.

Por último, este cenário remete para situações em que as credenciais se encontram válidas no servidor, mas que não se encontram armazenadas localmente. Para testar devidamente este cenário, foi necessário garantir que as credenciais não se encontram armazenadas localmente e que apenas se encontram no servidor. Posto isto, foi adicionada à aplicação um botão apenas para apagar todas as credenciais armazenadas localmente. Após serem adicionadas localmente e replicadas no servidor, foi apenas necessário selecionar o botão, e forçar a função de validação. Neste cenário, a aplicação vai obter as credenciais que se encontram no servidor e vai validar cada credencial, vai verificar que a mesma não se encontra localmente e vai então proceder à sua adição. Com uma única credencial, o tempo médio foi de 175.7 ± 31.0 ms. Para 25 credenciais, foi de 507.7 ± 75.6 ms, para 50 credenciais, de 787.0 ± 37.4 ms, e, para 100 credenciais, o tempo médio foi de 1239.9 ± 83.3 ms.

Na Figura 6.7 é possível observar e comparar os tempos de validação das credenciais nos quatro cenários. Em todos, verifica-se um aumento progressivo do tempo de validação à medida que cresce o número de credenciais a serem verificadas. Para além do aumento de tempo não ser significativo, este processo ocorre de forma imperceptível, sem impactar a usabilidade.

6.4.3 Rotatividade das Chaves

Tal como já referido anteriormente, esta função despoleta a alteração da chave que é utilizada para cifrar as credenciais que se encontram no Servidor de Autenticação e Armazenamento. Posto isto, a média de execução desta tarefa foi 2285.9 ± 137.2 ms. Importa destacar que esta ação de rotatividade das chaves é completamente imperceptível, ou seja, o tempo que a função demora não se reflete na usabilidade do utilizador.

6.4.4 Operações Sobre as Credenciais

Nesta secção são apresentados os tempos que a aplicação demorou a efetuar as diversas operações disponíveis a serem realizadas sobre as credenciais pessoais do utilizador. Primeiramente, a ação de criar a credencial. O tempo apresentado em seguida reflete apenas a duração da operação, desde que o botão de adicionar credencial é pressionado, até que a aplicação garante que os dados foram devidamente armazenados localmente e colocados no Servidor de Autenticação e Armazenamento, devidamente protegidos. O tempo de execução desta operação apresenta uma média 237.5 ± 16.9 ms. No segundo cenário, que remete para a atualização das credenciais, as ações executadas são idênticas às da criação de credenciais, mas, apenas atualiza-se algo que já existe. O tempo de execução desta operação apresentou uma média de 347.5 ± 40.4 ms. Por último, este cenário remete para apagar a informação de determinada credencial. Nesta ação, é contabilizado o tempo desde que o botão de apagar a credencial é selecionado, até que a credencial seja completamente removida. Esta operação foi concluída com uma média de 411.8 ± 21.4 ms.

6.4.5 Operações Sobre a Conta

Nesta secção, são apresentados os tempos para a realização das três operações possíveis na conta do utilizador: entrar, criar e sair da conta. A operação de entrada foi realizada sempre com o mesmo utilizador, resultando num tempo médio de 1404.6 ± 43.4 ms. A operação de sair da conta teve um tempo médio de 32.4 ± 3.8 ms, tendo sido sempre realizada com a mesma conta. Finalmente, a criação de conta foi testada com dez contas novas, apresentando uma duração média de 5255.4 ± 163.7 ms. Após a análise dos tempos de execução, concluiu-se que, de forma geral, as tarefas são rápidas a executar e que o seu tempo de execução não afeta a usabilidade da aplicação.

6.4.6 Conclusão dos Resultados

Os resultados apresentados indicam que o tempo de execução das operações não afeta a usabilidade da aplicação, mesmo com o aumento do número de credenciais e a presença dos mecanismos de segurança implementados no sistema.

6.5 Sumário

Neste capítulo, relatámos os testes realizados ao nosso sistema, tanto em termos de desempenho quanto com o público-alvo. Nos testes de desempenho, apresentámos o tempo que a aplicação demora a realizar as principais operações, nomeadamente a validação das credenciais, a rotatividade das chaves, e as operações sobre as credenciais e os dados da conta. Concluímos que a aplicação é notavelmente rápida nas operações que envolvem a interação direta com o utilizador. Embora as tarefas relacionadas com validações e rotatividade das chaves possam, em alguns casos, parecer mais demoradas, elas não comprometem a usabilidade, uma vez que estes processos ocorrem de forma imperceptível. Na avaliação com o público-alvo, analisámos a sua relação com a tecnologia, constatando que, embora os idosos reconheçam o impacto positivo da tecnologia nas suas vidas, muitos ainda não se sentem completamente à vontade no seu uso. No entanto, demonstraram interesse em como a tecnologia pode beneficiá-los. Observámos também que esta faixa etária carece frequentemente de proteção *online*, muitas vezes devido à falta de orientação. Apesar disso, conseguiram usar a aplicação com sucesso (SUS 81.3) e apreciaram as suas funcionalidades.

Capítulo 7

Conclusão e trabalho futuro

Neste trabalho, desenvolvemos um sistema destinado a ajudar os idosos a protegerem-se no mundo *online*, com o suporte dos seus cuidadores informais e integrando as metodologias necessárias para garantir a segurança dos utilizadores. Apesar de haver sempre espaço para melhorias, a avaliação com os idosos revelou um resultado médio de 81.3 no SUS, indicando que a plataforma foi considerada fácil de utilizar pelo público-alvo. Nas secções seguintes, sumarizamos o que foi discutido em cada capítulo, apresentamos as principais contribuições e limitações do nosso trabalho, e concluímos com sugestões para trabalhos futuros.

7.1 Sumário

No [Capítulo 1](#) introduzimos o nosso trabalho, onde apresentámos as diversas motivações que nos levaram ao desenvolvimento deste projeto, seguidas dos principais objetivos estipulados, sendo o principal o desenvolvimento de um gestor de palavras-passe focado na faixa etária mais avançada. Finalizámos o capítulo com a apresentação das principais contribuições deste projeto.

No [Capítulo 2](#) apresentámos o trabalho relacionado com a autenticação para os idosos. Descrevemos os tipos de métodos de autenticação existentes e alguns métodos de autenticação onde os idosos poderiam ser possíveis beneficiários, realizando comparações entre eles. Também explicámos o que é um gestor de palavras-passe, evidenciando o motivo de ser a solução mais indicada para esta faixa etária, e apresentámos alguns trabalhos relacionados com gestor de palavras-passe, onde os idosos também poderiam ser beneficiados. Concluímos este capítulo com uma explicação e análise do algoritmo SS, bastante importante no nosso sistema.

No [Capítulo 3](#) apresentámos os requisitos que foram estabelecidos, divididos em dois grupos distintos: requisitos funcionais e não funcionais.

No [Capítulo 4](#) detalhámos o desenho da solução implementada, começando pela descrição da arquitetura completa do sistema e dos seus componentes. Apresentámos também o modelo adversário estabelecido e os mecanismos de segurança incluídos na nossa solução. Este capítulo termina com a descrição das diversas operações construídas no sistema.

No [Capítulo 5](#) apresentámos detalhes da implementação, incluindo as tecnologias escolhidas para os diversos componentes do sistema e os motivos dessas escolhas. Também abordámos a

tecnologia de criptografia utilizada. Dado que, a implementação da interface e a segurança são fundamentais, explicámos as decisões de *design* e os principais fluxos que o utilizador deve seguir nas aplicações para as diversas tarefas disponíveis.

No [Capítulo 6](#) apresentámos as avaliações realizadas no nosso sistema. Começámos pela avaliação de desempenho, onde apresentámos os tempos médios e o desvio padrão necessários para a aplicação executar determinadas ações. Concluímos com as avaliações realizadas junto da faixa etária mais idosa, tanto as avaliações heurísticas como a avaliação final com o público alvo.

Finalmente, no [Capítulo 7](#) apresentámos as nossas conclusões finais, sumariando todo o trabalho realizado, as contribuições e as suas limitações. Apresentámos também as perspetivas para o trabalho futuro a ser realizado numa próxima versão desta plataforma.

7.2 Contribuições e Limitações

A principal contribuição deste trabalho foi o desenvolvimento de um gestor de palavras-passe adaptado às necessidades da população idosa, tendo como prioridade a segurança. O sistema permite que os idosos gerem as suas credenciais de forma adequada e que cuidadores informais os possam auxiliar remotamente, armazenando também as suas próprias credenciais na mesma plataforma. Esta funcionalidade promove uma maior proximidade entre cuidadores e idosos, facilitando a proteção das informações. Protocolos de segurança como o *Secret Sharing* e o *Signal*, aliados a métodos de criptografia, armazenamento seguros e mecanismos de segurança tanto nas aplicações como nos servidores, garantem a recuperação das credenciais dos idosos e a proteção dos dados dos utilizadores. Outro contributo relevante foi a recolha de requisitos, com foco nos idosos. Este processo envolveu a revisão da literatura, avaliações heurísticas por um perito e interações diretas com os idosos. A abordagem de design centrada no utilizador permitiu identificar melhorias sugeridas tanto pelo perito como pelos idosos, implementadas através de prototipagem iterativa, resultando numa aplicação otimizada. O recrutamento de cuidadores informais facilitou o acesso aos idosos, que demonstraram interesse e reconheceram a importância do sistema.

Através de 26 interações distintas com os idosos, confirmámos que o sistema pode ser uma solução prática para esta população. Os idosos mostraram-se, na maioria dos casos, interessados na forma como o sistema poderia melhorar a sua segurança digital. Além disso, conseguimos sensibilizá-los para os riscos da proteção inadequada das suas credenciais, promovendo comportamentos mais seguros.

Ao longo do projeto, a obtenção de voluntários revelou-se um processo demorado e sensível. A desconfiança, característica desta faixa etária, constituiu um desafio, levando alguns a desistirem de participar. Esta hesitação foi, em parte, causada pelo desconforto em abordar temas de segurança digital, e, noutras casas, pela relutância dos cuidadores informais, que, por vezes, assumiam que os idosos não conseguiriam utilizar o sistema sem lhes proporcionar uma oportunidade de experimentá-lo. Outra limitação identificada durante os testes foi o facto destes terem sido realizados em dispositivos que não pertenciam aos próprios idosos. Embora tivessem a opção de

escolher o sistema operativo com o qual se sentiam mais familiarizados, o uso de dispositivos alheios gerou algum desconforto durante a interação com a aplicação. Por fim, dado que o sistema inclui duas aplicações (uma para os idosos e outra para os cuidadores), teria sido ideal que, durante os testes, os cuidadores estivessem presentes para observar a interação simultânea entre ambos. No entanto, devido a incompatibilidade de horários e à preferência por realizar os testes presencialmente, em locais onde os idosos se sentissem mais à vontade, essa interação conjunta não foi possível.

7.3 Trabalho Futuro

No futuro, um caminho promissor seria o desenvolvimento de uma extensão para *browsers*, permitindo que os utilizadores acedam e editem as suas credenciais diretamente a partir do navegador, sem a necessidade de recorrer a dispositivos móveis. Esta extensão teria como objetivo simplificar a gestão e o acesso às credenciais, proporcionando uma interface intuitiva e segura, semelhante à experiência oferecida pela aplicação móvel.

Paralelamente, o aprimoramento das funcionalidades de preenchimento automático de formulários, tanto em aplicações web como nas aplicações instaladas nos dispositivos móveis, seria uma forma de minimizar o esforço dos utilizadores ao preencher dados repetitivos, eliminando a necessidade de copiar e colar essas informações.

Outro possível desenvolvimento seria permitir a utilização da mesma conta em múltiplos dispositivos simultaneamente. Isso permitiria que os utilizadores acedessem às suas contas em diferentes plataformas e dispositivos, com sincronização de dados em tempo real. Esse aprimoramento exigiria a criação de mecanismos de segurança robustos para proteger os dados durante o processo de sincronização e armazenamento, além da implementação de métodos de autenticação flexíveis que garantissem a segurança sem comprometer a usabilidade.

Todas as funcionalidades e trabalhos futuros referidos, foram os mais importantes identificados ao longo do trabalho e das necessidades que foram surgindo. É importante e crucial que a continuidade do desenvolvimento do sistema continue a ser centrado no utilizador e priorizando a segurança, envolvendo sempre que possível os futuros utilizadores, tanto os idosos como os respetivos cuidadores.

Bibliografia

- [1] 1password: More than a password manager. <https://1password.com/>. Acedido em 30 de julho de 2024.
- [2] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? *European Workshop on Usable Security*, 2016.
- [3] Nora Alkaldi, Karen Renaud, and Lewis Mackenzie. Encouraging password manager adoption by meeting adopter self-determination needs. *Hawaii International Conference on System Sciences*, 2019.
- [4] William Sims Bainbridge. *Berkshire encyclopedia of human-computer interaction*, volume 1. Berkshire Publishing Group LLC, 2004.
- [5] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):1–41, 2012.
- [6] Bitwarden: Open source password management. <https://bitwarden.com/>. Acedido em 30 de julho de 2024.
- [7] G. R. Blakley. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on*, pages 313–313. IEEE Computer Society, 1979.
- [8] Oliver Burmeister. Websites for seniors: Cognitive accessibility. *International Journal of Emerging Technologies and Society*, 8(2):99–113, 2010.
- [9] Bradley Camburn, Vimal Viswanathan, Julie Linsey, David Anderson, Daniel Jensen, Richard Crawford, Kevin Otto, and Kristin Wood. Design prototyping methods: state of the art in strategies, techniques, and guidelines. *Design Science*, 3:e13, 2017.
- [10] Carolina Carreira, Joao F Ferreira, and Alexandra Mendes. Towards improving the usability of password managers. In *InFORUM*, 2021.
- [11] Ke Chen and Alan Chan. Gerontechnology acceptance by elderly hong kong chinese: A senior technology acceptance model (stam). *Ergonomics*, 57, 03 2014.
- [12] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, volume 15, pages 1–16, 2006.

- [13] Gradeigh D Clark and Janne Lindqvist. Engineering gesture-based authentication systems. *IEEE Pervasive Computing*, 14(1):18–25, 2015.
- [14] Contrast finder. <https://app.contrast-finder.org/>. Acedido em 12 de agosto de 2024.
- [15] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L Jean Camp, and Lesa Huber. Towards implementing inclusive authentication technologies for older adults. *Who Are You*, 2019.
- [16] Dashlane: The security-first password manager. <https://dashlane.com/>. Acedido em 30 de julho de 2024.
- [17] Jonas Ellefsen and Weiqin Chen. Privacy and data security in everyday online services for older adults. In *Proceedings of the 10th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion*, pages 203–207, 2022.
- [18] Susan L Gatto and Sunghee H Tak. Computer, internet, and e-mail use among older adults: Benefits and barriers. *Educational Gerontology*, 34(9):800–811, 2008.
- [19] Shirley Gaw and Edward W Felten. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*, pages 44–55, 2006.
- [20] Marcia Gibson, Karen Renaud, Marc Conrad, and Carsten Maple. Musipass: authenticating me softly with”my”song. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 85–100, 2009.
- [21] Google firebase. <https://firebase.google.com/>. Acedido em 30 de julho de 2024.
- [22] Peter Gregor, Alan F Newell, and Mary Zajicek. Designing for dynamic diversity: interfaces for older people. In *Proceedings of the fifth international ACM conference on Assistive technologies*, pages 151–156, 2002.
- [23] Onur Hakbilen, Piraveen Perinparajan, Michael Eikeland, and Nils Ulltveit-Moe. Safepass-presenting a convenient, portable and secure password manager. In *ICISSP*, pages 292–303, 2018.
- [24] Kalpana Hundlani. *A Parent-Child Password Manager*. PhD thesis, Carleton University, 2016.
- [25] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K Reiter, and Aviel Rubin. The design and analysis of graphical passwords. In *8th USENIX Security Symposium (USENIX Security 99)*, 1999.

- [26] Aušrius Juozapavičius, Agnė Brilingaitė, Linas Bukauskas, and Ricardo Gregorio Lugo. Age and gender impact on password hygiene. *Applied Sciences*, 12(2):894, 2022.
- [27] Dongsong Zhang Kanlun Wang, Lina Zhou. Biometrics-based mobile user authentication for the elderly: Accessibility, performance, and method design. In *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pages 1–6. IEEE, 2017.
- [28] Lina Zhou Kanlun Wang and Dongsong Zhang. Biometrics-based mobile user authentication for the elderly: Accessibility, performance, and method design. *International Journal of Human–Computer Interaction*, 40(9):2153–2167, 2024.
- [29] Ehud Karnin, Jonathan Greene, and Martin Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.
- [30] Keeper security: Password & secrets management. <https://keepersecurity.com/>. Acedido em 30 de julho de 2024.
- [31] Marc Alexander Kowtko. Biometric authentication for older adults. In *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, pages 1–6. IEEE, 2014.
- [32] Leona Lassak, † ElleenPan, Blase Ur, ‡ MaximilianGolla, Recruitment Website, and Disclaimer Demographics. Why aren't we using passkeys? obstacles companies face deploying fido2 passwordless authentication. In *33rd USENIX Security Symposium (USENIX Security 24)*, 2024.
- [33] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C Van Oorschot. Tapas: design, implementation, and usability evaluation of a password manager. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 89–98, 2012.
- [34] Measuring usability with the system usability scale (sus). <https://measuringu.com/sus/>. Acedido em 30 de julho de 2024.
- [35] Burak Merdenyan and Helen Petrie. Generational differences in password management behaviour. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32*, pages 1–10, 2018.
- [36] Benjamin Morrison, Lynne Coventry, and Pam Briggs. How do older adults feel about engaging with cyber-security? *Human Behavior and Emerging Technologies*, 3(5):1033–1049, 2021.
- [37] Deborah Nelson and Kim-Phuong L Vu. Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior*, 26(4):705–715, 2010.
- [38] Nordpass: Securely store, manage & autofill passwords. <https://nordpass.com/>. Acedido em 30 de julho de 2024.

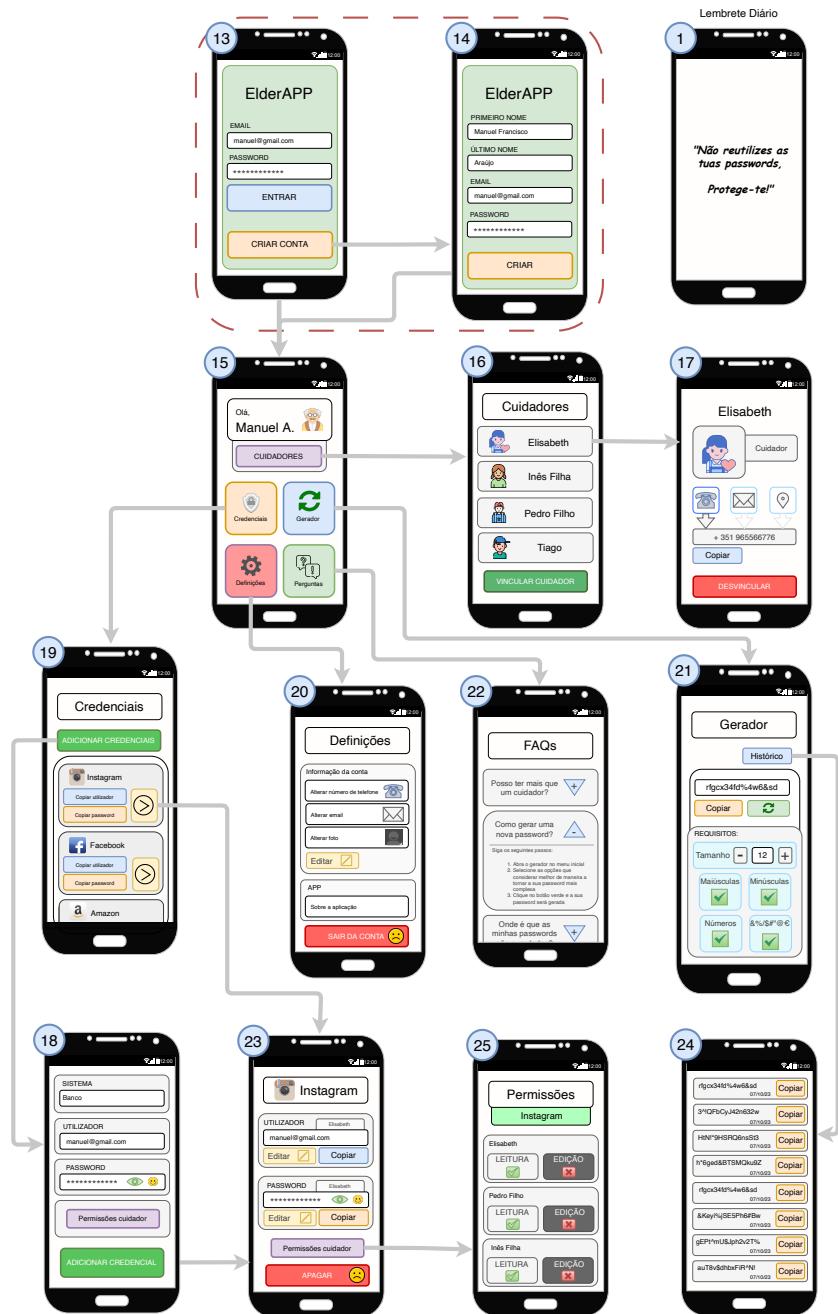
- [39] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. “it basically started using me:” an observational study of password manager usage. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–23, 2022.
- [40] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. Why older adults (don’t) use password managers. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 73–90, 2021.
- [41] React native. <https://reactnative.dev/>. Acedido em 30 de julho de 2024.
- [42] React native expo. <https://expo.dev/>. Acedido em 30 de julho de 2024.
- [43] Karen Renaud and Judith Ramsay. Now what was that password again? a more flexible way of identifying and authenticating our seniors. *Behaviour & Information Technology*, 26(4):309–322, 2007.
- [44] Karen Renaud, Kenneth C Scott-Brown, and Andrea Szymkowiak. Designing authentication with seniors in mind. *20th International Conference on Human-Computer Interaction with Mobile Devices and Service*, 2018.
- [45] Roboform: Next generation password manager. <https://roboform.com/>. Acedido em 30 de julho de 2024.
- [46] Bruce Schneier. Two-factor authentication: too little, too late. *Communications of the ACM*, 48(4):136, 2005.
- [47] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [48] 10 things to know about the single ease question (seq). <https://measuringu.com/seq10/>. Acedido em 30 de julho de 2024.
- [49] Lakshmidevi Sreeramareddy, Pewu Mulbah, and Jinjuan Heidi Feng. Investigating the use of gesture-based passwords by the seniors. In *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3*, pages 107–118. Springer, 2015.
- [50] Frank Stajano. Pico: No more passwords! In *International Workshop on Security Protocols*, pages 49–81. Springer, 2011.
- [51] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users’ perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760, 2016.
- [52] Kim-Phuong L Vu and Martina M Hills. The influence of password restrictions and mnemonics on the memory for passwords of older adults. In *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, pages 660–668. Springer, 2013.

- [53] Shikun Zhang, Sarah Pearman, Lujo Bauer, and Nicolas Christin. Why people (don't) use password managers effectively. In *SOUUPS@ USENIX Security Symposium*, 2019.

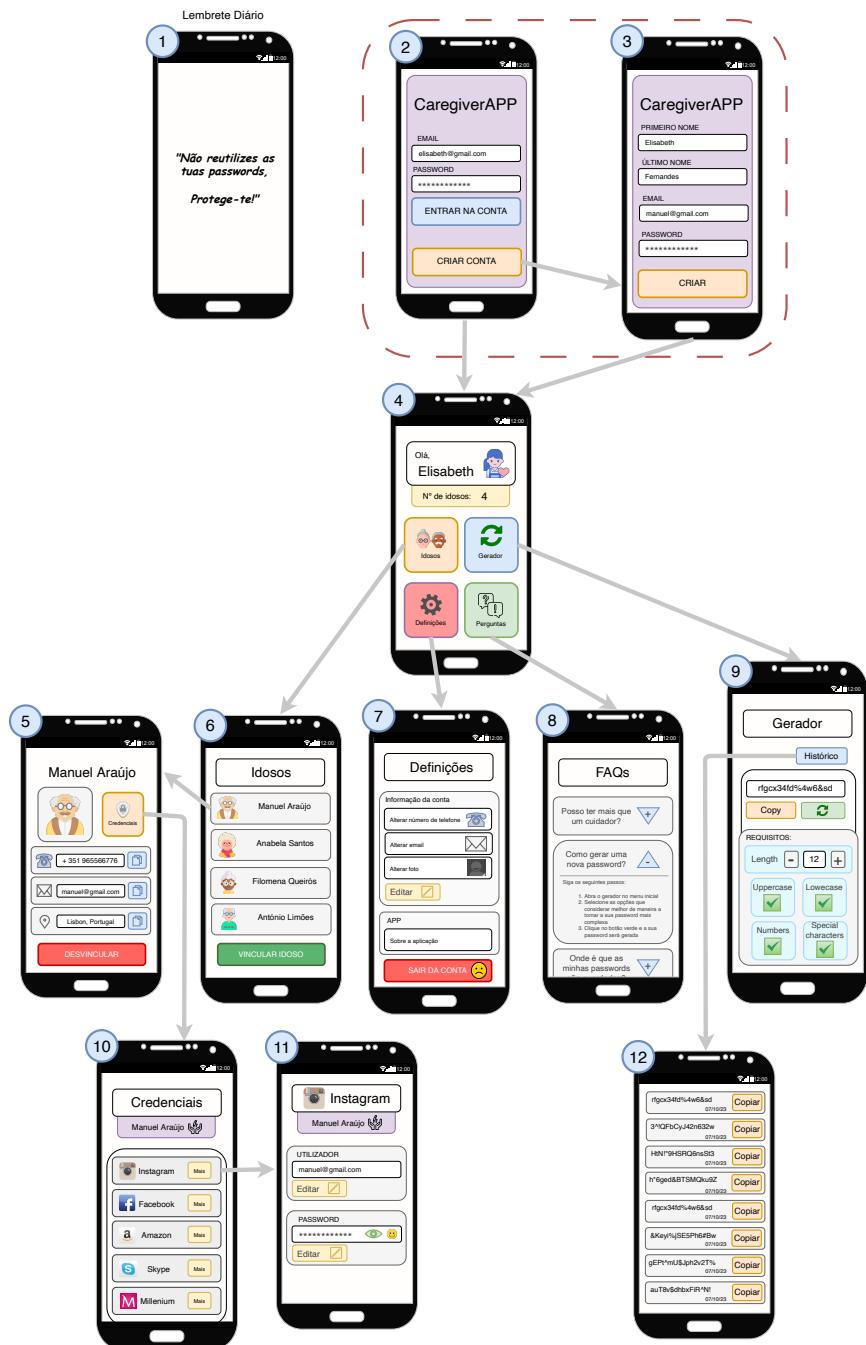
Apêndice A

Protótipo de alta fidelidade (idoso)



Apêndice B

Protótipo de alta fidelidade (cuidador)





Apêndice C

Guião experimental

Introdução / Objetivo

O presente questionário foi elaborado no âmbito da Dissertação de Mestrado em Engenharia Informática na Faculdade de Ciências da Universidade de Lisboa, cujo objetivo é desenvolver um gestor de credenciais destinado a pessoas idosas, permitindo-lhes salvaguardar de forma segura as suas credenciais de acesso. Além disso, o gestor de credenciais proposto facilitará o estabelecimento de relações com possíveis cuidadores informais, os quais poderão auxiliar na gestão e manutenção dessas credenciais. O objetivo deste questionário é avaliar o sistema desenvolvido, de forma a detectar possíveis melhorias e não avaliar os utilizadores voluntários durante esta fase.

Motivação

O que motivou o desenvolvimento deste sistema foi a observação de que muitos idosos recorrem a palavras-passe de fácil memorização e pelo facto das reutilizarem com alguma frequência. Estes comportamentos tornam as suas palavras-passe facilmente desvendáveis por potenciais atacantes online. Além disso, muitos idosos consideram as ameaças online um exagero, caindo na falácia de que "só acontece aos outros". Para além disso, possuem alguma dificuldade em lembrar as suas palavras-passe, e acabam por armazená-las em locais pouco seguros, como é o caso do papel. Existem aplicações, conhecidas como "gestores de palavras-passe", que poderiam ajudar, mas muitos idosos acham-nas confusas e difíceis de utilizar.

Consentimento

Agradecemos desde já o seu interesse e colaboração neste estudo. A sua participação é voluntária e pode desistir a qualquer momento. Todas as suas dúvidas serão devidamente esclarecidas pela equipa de investigação. Os dados recolhidos serão analisados de forma anónima, garantindo que nenhuma informação seja identificável. O áudio da sessão experimental será gravado para uma análise mais precisa posteriormente. Durante toda a sessão experimental, sinta-se à vontade para interromper caso possua algum comentário ou não entenda alguma informação que tenha sido transmitida. Ao prosseguir com este estudo, concorda em participar neste estudo e em permitir tanto a gravação da sessão experimental, bem como a captação de uma fotografia, que será utilizada pelo investigador no final do estudo como forma de agradecimento a todas as pessoas que contribuíram.

Questionário demográfico

1- Qual é o seu género?

- Feminino
- Masculino
- Outro

2- Qual é a sua idade?

3- Qual é o seu grau académico?

4- Possui alguma dificuldade visual?

- Nenhuma
- Hipermetropia (dificuldade em ver ao perto)
- Miopia (dificuldade em ver ao longe)
- Outro

5- Usa óculos? (Se não respondeu Nenhuma na anterior)

- Sim
- Não

6 - Há quantos anos utiliza um smartphone e/ou tablet?

- 0 (Agradece e termina o teste)
- Menos de um ano
- Entre 1 e 3 anos
- Entre 4 e 6 anos
- Mais de 7 anos

7- Como avalia o seu à vontade em utilizar o seu smartphone e/ou tablet?

- 1 (Pouco à vontade)
- 2
- 3
- 4
- 5 (Muito à vontade)

8- Quantas horas por dia utiliza o seu smartphone e/ou tablet?

- Menos de 1 hora
- Entre 1 e 3 horas
- Mais de 3 horas

9- Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Utilizar a tecnologia é uma boa ideia"?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

10 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Gosto da ideia de utilizar a tecnologia"?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

11 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Considero que a tecnologia pode trazer vantagens para a população com uma idade mais avançada"? Quais? (se a resposta for superior a 3)

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

12 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Considero que a tecnologia pode trazer desvantagens para a população com uma idade mais avançada."? Quais? (se a resposta for superior a 3)

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

13 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Considero a tecnologia algo útil no meu dia a dia."?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

14 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Gosto de explorar os benefícios que a tecnologia lhe pode trazer para o seu dia a dia."?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

15 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Considero que poderia ter mais habilidade a utilizar a tecnologia."?

- 1 (Discordo completamente)

- 2
- 3
- 4
- 5 (Concordo completamente)

16 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Conseguiria completar uma tarefa utilizando uma tecnologia se houvesse alguém para me demonstrar como realizá-la."?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

17 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Conseguiria completar uma tarefa utilizando uma tecnologia se houvesse um manual com os passos necessários."?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

18 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Sinto-me apreensivo relativamente à utilização da tecnologia."?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

19 - Numa escala de 1-5, quanto é que concorda com a seguinte afirmação: "Hesito em utilizar a tecnologia devido ao medo de realizar algo de errado."?

- 1 (Discordo completamente)
- 2
- 3
- 4
- 5 (Concordo completamente)

20 - Alguma vez teve uma experiência negativa relacionada com o acesso não autorizado a uma das suas contas na internet?

- Sim
- Não

Não sei

21 - Considera-se um alvo fácil para pessoas mal intencionadas roubarem as suas informações pessoais no mundo online?

Sim

Não

Não sei

22 - A que é que costuma recorrer para memorizar as suas palavras-passe/pins?

Não memorizo de todo

Recorro a terceiros

Ao bloco de notas do telemóvel

A um caderno

À minha memória

Outro

23 - Recorre a alguém para lhe ajudar na gestão das suas palavras-passe/pins?

Sim

Não

24 - (Caso a resposta anterior seja sim). A quem recorre?

Filhos

Netos

Cônjuge

Amigos

Outro

25 - Sabe o que significa uma palavra-passe ser fraca/forte?

Sim

Não

< providenciar explicação ao idoso do que se considera uma palavra-passe ser fraca/forte >

26 - Considera as suas palavras-passe fortes?

Sim

Não

27 - Conhece algum método seguro para guardar as suas palavras-passe/pins? Quais? (Se sim)

Sim

Não

28 - Sabe o que é um gestor de palavras-passe?

- Sim
- Não

29 - Confiaria numa aplicação móvel, considerada segura, para armazenar as suas palavras-passe/pins?

- Sim
- Não
- Não tenho a certeza

Sessão experimental

Cada tarefa a ser realizada pelos idosos será avaliada com base em duas métricas: o tempo necessário para completar a tarefa e o número de cliques incorrectos durante a sua execução, sendo estas métricas calculadas e verificadas através tanto da gravação do audio como do ecrã do dispositivo que o utilizador se encontra a utilizar. Além disso, se um idoso demonstrar a intenção de clicar num botão incorreto e aguardar a confirmação do avaliador também será considerada como um clique errado. Depois de cada tarefa, o idoso irá avaliar a execução da tarefa recorrendo a uma escala SEQ (Single Ease Question).

Nota: Os idosos não serão informados de que o tempo e o número de cliques estão a ser avaliados, de modo a evitar que o nervosismo e o sentimento de estarem a ser avaliados acabe por afetar a avaliação. Em todas as tarefas, o utilizador parte do menu inicial da aplicação.

Tarefa 1: Registar na aplicação.

Para começar a utilizar a aplicação, é necessário registar-se na mesma. Utilize o nome “Pedro”, o email pedro1@gmail.com, o número de telefone 912345678 e a palavra-passe “teste123”.

“Acho que a tarefa foi fácil de executar”

DISCORDO COMPLETAMENTE 1 2 3 4 5 6 7 CONCORDO COMPLETAMENTE

Tarefa 2: Adicionar uma credencial.

Decidiu modificar a sua palavra-passe da conta do Facebook, mas quer garantir que ela é segura e que não se esquece da mesma, então decide utilizar a aplicação para adicionar uma credencial. Utilize o nome da plataforma “Facebook”, o URL “www.facebook.com”, o nome de utilizador “pedro”, e escolha uma palavra-passe forte.

"Acho que a tarefa foi fácil de executar"

DISCORDO COMPLETAMENTE 1 2 3 4 5 6 7 CONCORDO COMPLETAMENTE

Tarefa 3: Entrar na conta Facebook criada.

A sua aplicação do Facebook alertou-o que alguém tentou entrar na sua conta, por isso pediu-lhe que inserisse as suas credenciais novamente. Uma vez que possui esses dados guardados na aplicação, recorra aos mesmos para realizar login na sua conta do Facebook.

"Acho que a tarefa foi fácil de executar"

DISCORDO COMPLETAMENTE 1 2 3 4 5 6 7 CONCORDO COMPLETAMENTE

Tarefa 4: Atualizar uma credencial.

Visto que tentaram entrar na sua conta do facebook, sentiu a necessidade de alterar a sua palavra-passe por precaução. Realize essa alteração na aplicação.

"Acho que a tarefa foi fácil de executar"

DISCORDO COMPLETAMENTE 1 2 3 4 5 6 7 CONCORDO COMPLETAMENTE

Tarefa 5: Vincular um cuidador.

Uma vez que o seu neto é a pessoa que o ajuda na gestão das suas credenciais, convide-o para que ele seja o seu cuidador na aplicação, sendo o seu email: neto123@gmail.com.

"Acho que a tarefa foi fácil de executar"

DISCORDO COMPLETAMENTE 1 2 3 4 5 6 7 CONCORDO COMPLETAMENTE

Tarefa 6: Desvinculação do cuidador.

O seu neto está com muito trabalho e não o pode ajudar durante uns meses. Desvincule-se dele de modo a que ele deixe de ter acesso aos seus dados.

"Acho que a tarefa foi fácil de executar"

DISCORDO COMPLETAMENTE 1 2 3 4 5 6 7 CONCORDO COMPLETAMENTE

Questionário pós-teste

Este questionário tem como intuito concluir a opinião final dos idosos relativamente à aplicação que lhes foi apresentada. Para isso recorremos ao método SUS (System Usability Scale).

- **Eu penso que gostaria de usar este sistema com frequência.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Achei o sistema desnecessariamente complexo.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Achei o sistema fácil de usar.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Acredito que precisaria do apoio de um cuidador para conseguir utilizar este sistema.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Achei que as várias funções deste sistema estavam bem integradas.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Achei que havia demasiada inconsistência neste sistema.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Imagino que a maioria das pessoas aprenderia a usar este sistema com alguma facilidade.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Achei que o sistema era complicado de usar.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Senti-me confiante a usar o sistema.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

- **Precisei de aprender muitas coisas antes de conseguir começar a utilizar este sistema.**

DISCORDO COMPLETAMENTE 1 2 3 4 5 CONCORDO COMPLETAMENTE

Observações finais

Após a apresentação dos motivos e objetivos deste projeto, bem como a utilização da aplicação, possui algum comentário ou observação final que gostaria de transmitir para contribuir para a melhoria do sistema apresentado?

Agradecimentos

Apêndice D

Avaliação heurística

Avaliação Heurística

A avaliação abaixo foi feita com recurso às **heurísticas de Nielsen**:

- H2.1 – Tornar estado do sistema visível
- H2.2 – Correspondência entre o sistema e o mundo real
- H2.3 – Utilizador controla e exerce livre-arbítrio
- H2.4 – Consistência e adesão a normas
- H2.5 – Evitar erros
- H2.6 – Reconhecimento em vez de lembrança
- H2.7 – Flexibilidade e eficiência
- H2.8 – Desenho estético e minimalista
- H2.9 – Ajudar o utilizador a reconhecer, diagnosticar e recuperar de erros
- H2.10 – Dar ajuda e documentação

Cada problema de usabilidade foi classificado com um **grau de severidade** na seguinte escala:

- 0 – Não há consenso que seja problema de usabilidade
 - 1 – Problema estético apenas
 - 2 – Problema de usabilidade menor
 - 3 – Problema de usabilidade importante
 - 4 – Catastrofe de usabilidade
-

1) Problema: Efeito de carregamento (*loading*) desaparece aquando da criação da conta, antes de passar ao próximo ecrã, o que pode confundir o utilizador

Heurística: H2.5 – Evitar erros

Descrição: Efeito de carregamento (*loading*) desaparece aquando da criação da conta, antes de passar ao próximo ecrã. Isto pode confundir o utilizador, levando-o a pensar que tem de preencher o formulário de criação de conta novamente.

Correção: Fazer com que a duração do *loading* se estenda até que o ecrã principal esteja pronto a mostrar.

Severidade: 3

2) Problema: Em *Adicionar Credencial*, poderá não ser claro para que serve o ícone de varinha mágica.

Heurísticas: H2.2 – Correspondência entre o sistema e o mundo real; H2.10 – Dar ajuda e documentação

Descrição: Em *Adicionar Credencial*, poderá não ser claro que o ícone de varinha mágica serve para pré-preencher o formulário da credencial com a informação de plataformas conhecidas, uma vez que é pouco provável que seja um ícone familiar para um idoso ou alguém pouco rotinado com tecnologia.

Correção: Na primeira utilização da aplicação, mostrar uma forma de ajuda (ex: sobreposta ao ecrã, como nos tutoriais de jogos casuais) em que se mostre para que serve e como usar a varinha mágica para pré-preencher o formulário de criação de credencial.

Severidade: 2

3) Problema: Em *Adicionar Credencial*, o estado do ícone de mostrar/ocultar palavra-passe (“olho”) está ao contrário do resto da aplicação (e do que é habitual).

Heurística: H2.4 – Consistência e adesão a normas

Descrição: Em *Adicionar Credencial*, o ícone de mostrar/ocultar palavra-passe está em modo de “mostrar” quando a palavra-passe já está a ser mostrada e em modo de “ocultar” quando esta já se encontra oculta, contrariando a convenção de uso deste ícone, bem como o seu uso no resto da aplicação.

Correção: Manter o uso do ícone de mostrar/ocultar palavra-passe consistente ao longo da aplicação, mostrando o ícone de ocultar quando esta está a ser mostrada, e vice-versa (tal como já acontece no ecrã de criação de conta no gestor de passwords).

Severidade: 2

4) Problema: Em *Adicionar Credencial*, e em *Gerar nova*, o termo “Regenerar” poderá causar confusão.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: O termo “Regenerar” tem um significado diferente do que se pretende e pode causar confusão.

Correção: Substituir “Regenerar” por “Gerar nova palavra-passe”.

Severidade: 2

5) Problema: Em *Adicionar Credencial*, o modo como é feita a alternância entre diferentes opções de tipo de credencial (*Login* e *Cartão*) pode confundir o utilizador.

Heurísticas: H2.5 – Evitar erros; H2.4 – Consistência e adesão a normas

Descrição: Em *Adicionar Credencial*, não é claro que é possível alternar entre diferentes opções de tipo de credencial (*Login* e *Cartão*). A seta entre ambas as opções dá a entender tratar-se de uma sequência de passos. Além disso, ao clicar numa das opções por engano e voltar para a outra, o progresso do que foi preenchido desaparece.

Correção: Fornecer as duas opções num ecrã anterior ao formulário a preencher.

Severidade: 3

6) Problema: Em *Credenciais*, os símbolos para filtrar a lista por tipo de credencial podem não ser claros, especialmente o símbolo de infinito.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: A utilização do símbolo de infinito para designar todos os tipos de credencial, e do símbolo de pessoa para designar contas pode levar a que o utilizador não saiba que ali pode filtrar as credenciais por tipo. Em particular, o símbolo do infinito pode não ser reconhecido por idosos.

Correção: Ter uma lista pendente (*listbox*) com opções por escrito (ex: Filtrar > Login; Cartão), ou mostrar logo os vários tipos de credencial por cima da lista de credenciais.

Severidade: 3

7) Problema: Nas F.A.Q., o uso do termo “Passos” para designar o tutorial pode não ser claro.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: Nas F.A.Q., o uso do termo “Passos” para designar o tutorial de como usar a aplicação pode não ser claro.

Correção: Substituir “Passos” por “Tutorial” ou “Passo-a-passo”.

Severidade: 2

8) Problema: Nas F.A.Q., os vídeos demonstrativos conduzem à app do Youtube, o que pode confundir os utilizadores.

Heurísticas: H2.3 – Utilizador controla e exerce livre-arbítrio; H2.5 – Evitar erros

Descrição: Nas F.A.Q., os vídeos demonstrativos conduzem à app do Youtube, o que pode sobressaltar utilizadores menos experientes, ou fazê-los sentir-se obrigados a utilizar uma app externa que podem não ter ou querer usar.

Correção: Incluir os vídeos localmente à app, ou embeber os vídeos do Youtube sem implicar sair da aplicação.

Severidade: 3

9) Problema: O uso dos termos “Username” e “Password” ao longo da aplicação pode não ser claro.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: Ao longo da aplicação, há uma falta de correspondência entre os termos “Username” e “Password” e os termos que a maioria das plataformas usam quando estão no idioma português (ex: “nome de utilizador” e “palavra-passe”). Esta falta de correspondência pode ser um problema para utilizadores que não falem inglês e/ou que não estejam rotinados com tecnologia. Acresce o desafio de que algumas plataformas (ex: Facebook) referem diretamente e-mail ou número de telemóvel em vez de usar o termo “nome de utilizador”.

Correção: Utilizar os termos “nome de utilizador” e “palavra-passe” ao longo da aplicação, indicando e-mail ou nº de telemóvel como exemplos de nome de utilizador no caso das plataformas listadas para pré-preenchimento que usem esses termos (ex: Facebook).

Severidade: 2

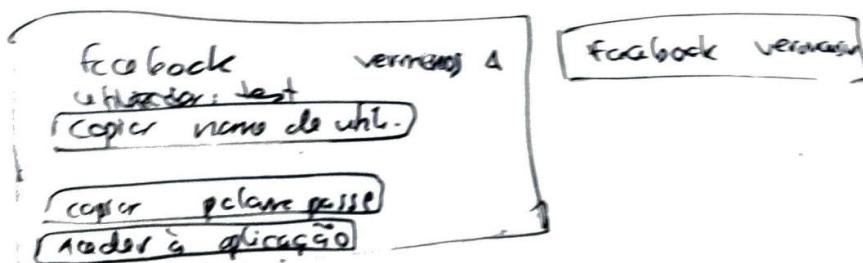
10) Problema: Em *Credenciais*, os termos “Ações” e “Navegar” não são claros, o que torna as principais funcionalidades da aplicação pouco acessíveis.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: Em *Credenciais*, não é claro que é através do botão “Ações” que poderão aceder às funcionalidades de copiar nome de utilizador e palavra-passe, bem como aceder à aplicação em que querem realizar o início de sessão.

Correção: Reorganizar as ações associadas a cada credencial de forma a facilitar o acesso às mesmas (ver imagem abaixo). Por exemplo, o botão “Ações” poderia ser substituído por um botão “Ver mais” de expandir a secção, e ao expandi-la, as opções de interação com aquela credencial ficariam logo visíveis. Adicionalmente, o termo “Navegar” poderia ser substituído por “Aceder à aplicação”.

Severidade: 3



11) Problema: Falta de ajuda relativamente ao processo de iniciar sessão numa aplicação externa.

Heurística: H2.10 – Dar ajuda e documentação

Descrição: Mesmo considerando uma possível reorganização das ações associadas às credenciais (ver Problema #10), o processo poderá não ser óbvio para utilizadores menos rotinados com tecnologia.

Correção: Na primeira utilização da aplicação, mostrar uma forma de ajuda (ex: sobreposta ao ecrã, como nos tutoriais de jogos casuais) em que se mostre como efetuar início de sessão numa plataforma externa.

Severidade: 3

12) Problema: No menu principal, os termos “Cuidadores”, “Credenciais”, e “Gerar nova” podem ser vagos.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: No menu principal, pode não ser claro a que tipo de funcionalidade os botões “Cuidadores”, “Credenciais” e “Gerar nova” se referem.

Correção: Substituir os termos em uso nesses botões por “Gerir Cuidadores”, “Gerir Credenciais” e “Gerar nova palavra-passe”, respectivamente.

Severidade: 0

13) Problema: Em *Cuidadores*, pode ser confuso haver um botão “Adicionar Cuidador 1” e botão “Adicionar Cuidador 2”.

Heurística: H2.2 – Correspondência entre o sistema e o mundo real

Descrição: Em *Cuidadores*, o uso dos termos “Cuidador 1” e “Cuidador 2” pode dar a entender que há inherentemente algum tipo de diferença de privilégios ou hierarquia entre ambos os cuidadores, quando na realidade qualquer um deles pode ter (ou não) os mesmos privilégios de acesso e edição das credenciais.

Correção: Substituir ambos os botões por um único botão “Adicionar cuidador”, e mostrar o botão apenas enquanto há menos do que 2 cuidadores vinculados.

Severidade: 2

14) Problema: Em *Cuidadores*, o estado atual da permissão para o cuidador alterar credenciais pode não ser claro.

Heurísticas: H2.1 – Tornar estado do sistema visível; H2.2 – Correspondência entre o sistema e o mundo real

Descrição: Em *Cuidadores*, o estado atual da permissão para o cuidador alterar credenciais é um único botão simples, o que não deixa claro se a permissão está a ser concedida ou não.

Correção: Em vez de um botão simples, usar um botão do tipo *switch/toggle* (interruptor).

Severidade: 2

15) Problema: No ecrã de edição de uma credencial, “Apagar login” e “Apagar cartão” é menos consistente e claro do que se fosse usado o termo “Apagar credencial” em ambos.

Heurísticas: H2.4 – Consistência e adesão a normas; H2.2 – Correspondência entre o sistema e o mundo real

Descrição: No ecrã de edição de uma credencial, são usados os termos “Apagar login” e “Apagar cartão” consoante o tipo de credencial, o que pode ser pouco claro no caso de “Apagar login” e não está consistente com as restantes ações possíveis sobre credenciais.

Correção: Utilizar o termo “Apagar credencial” em ambos os tipos de credencial.

Severidade: 0

16) Problema: Nas definições, o botão “Mais sobre a aplicação” conduz a uma página externa, o que pode confundir o utilizador.

Heurística: H2.5 – Evitar erros

Descrição: Nas definições, o botão “Mais sobre a aplicação” conduz a uma página externa onde se pode encontrar o repositório de código Github da aplicação. Dado que neste ainda não se encontra documentação sobre a aplicação, e que a mudança de aplicação pode confundir os utilizadores, este botão poderia ser dispensado.

Correção: Remover o botão “Mais sobre a aplicação”.

Severidade: 0

17) Problema: Nas F.A.Q., as perguntas estão alinhadas ao centro.

Heurística: H2.8 – Desenho estético e minimalista

Descrição: O alinhamento ao centro utilizado nas perguntas e respostas das F.A.Q. não é adequado para este tipo de conteúdo, tornando-o menos legível.

Correção: Alinhar perguntas e respostas à esquerda.

Severidade: 1