UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE SISTEMAS DE INFORMAÇÃO

EMARIELLE ALMEIDA PRADO

I7SAFE - APLICATIVO PARA AUXILIAR O APRENDIZADO EM SEGURANÇA DA INFORMAÇÃO

Itacoatiara – Amazonas

2023

EMARIELLE ALMEIDA PRADO

I7SAFE - APLICATIVO PARA AUXILIAR O APRENDIZADO EM SEGURANÇA DA INFORMAÇÃO

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Sistemas de Informação.

ORIENTADOR: PROF. ESP.ALTERNEI DE SOUZA BRITO

Itacoatiara – Amazonas

2023

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Prado, Emarielle Almeida
P896i I7safe - aplicativo para auxiliar o aprendizado em segurança da informação / Emarielle Almeida Prado . 2023
41 f.: il. color; 31 cm.

Orientador: Alternei de Souza Brito
TCC de Graduação (Sistemas de Informação) - Universidade Federal do Amazonas.

1. Aprendizado. 2. Segurança da Informação. 3. Proteção de Dados. 4. Mobile Learning. 5. Desenvolvimento Movél. I. Brito, Alternei de Souza. II. Universidade Federal do Amazonas III. Título

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Curso de Sistemas de Informação - ICET

FOLHA DE APROVAÇÃO

EMARIELLE ALMEIDA PRADO

I7SAFE - APLICATIVO PARA AUXILIAR O APRENDIZADO EM SEGURANÇA DA INFORMAÇÃO

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Sistemas de Informação.

Aprovada em 27 de outubro de 2023

BANCA EXAMINADORA

Prof. Esp. Alternei de Souza Brito
Universidade Federal do Amazonas

Prof. Me. Christophe Saint-Christie de Lima Xavier
Universidade Federal do Amazonas

Prof. Me. Euler Vieira da Silva
Instituto Federal do Amazonas

Folha de Aprovação assinada pela Profa. Dra. Odette Mestrinho Passos, responsável pela disciplina ITS031 - Trabalho de Conclusão de Curso do Curso de Sistemas de Informação (Período: 2023.1), onde atesta a defesa do aluno e a presença dos membros da banca examinadora.

Documento assinado eletronicamente por **Odette Mestrinho Passos**, **Professor do Magistério Superior**, em 06/11/2023, às 09:43, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alternei de Souza Brito**, **Professor do Magistério Superior**, em 06/11/2023, às 09:49, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Christophe Saint-Christie de Lima Xavier**, **Professor do Magistério Superior**, em 06/11/2023, às 10:03, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1774958** e o código CRC **46462158**.

Rua Nossa Senhora do Rosário - Bairro Tiradentes nº 3836 - Telefone: (92) (92) 99318-2549
CEP 69103-128 Itacoatiara/AM - ccsiicet@ufam.edu.br

AGRADECIMENTOS

Primeiramente, gostaria de expressar minha profunda gratidão a Deus, cuja graça e orientação foram a luz que me guiou ao longo desta jornada acadêmica e durante a realização deste Trabalho de Conclusão de Curso.

Agradeço de coração a Alternei Brito, meu orientador, cuja dedicação, sabedoria e paciência foram fundamentais para o desenvolvimento deste trabalho.

Minha família merece uma profunda gratidão por seu constante apoio, amor incondicional, proteção e encorajamento. Agradeço a Deus pela bênção de tê-los ao meu lado, especialmente a minha filha, Angélica Vitória, por ser a minha força, meu companheiro de vida Vinícius Graça por toda ajuda durante esse processo, cujas palavras de incentivo e suporte foram fundamentais em todos os momentos.

Ao meu amigo Raimundo Carlos que se tornou um irmão durante toda a graduação, irmã Emanuelle Almeida Prado e colegas Selma Leal, Sidney Guerreiro, Jarlessandra Beniz, que compartilharam risos, desafios e conquistas ao longo desta jornada, meu sincero agradecimento. Todos foram essências nessa caminhada, só tenho a agradecer pela amizade e companheirismo de cada um.

Com gratidão,

Emarielle Almeida Prado

I7SAFE - APLICATIVO PARA AUXILIAR O APRENDIZADO EM SEGURANÇA DA INFORMAÇÃO

Emarielle A. Prado, Alternei de S. Brito

Instituto de Ciências Exatas e Tecnologia – Universidade Federal do Amazonas (ICET/UFAM) – Itacoatiara – Amazonas – Brasil

almeidaemarielle@gmail.com, alternei@ufam.edu.br

Resumo. *Com o crescimento de dispositivos conectados, torna-se necessário diversos cuidados com as informações que são enviadas e coletadas na internet, principalmente relacionadas à privacidade do usuário. Os ataques cibernéticos são efetuados de diversas formas e os usuários precisam ter conhecimento para evitar ou lidar com tais problemas. O aprendizado por meio de dispositivos móveis tem desencadeado transformações significativas nos hábitos da sociedade moderna. Nesse contexto, o objetivo deste trabalho é apresentar o aplicativo móvel I7Safe, projetado para auxiliar os usuários na compreensão de conceitos relacionados à Segurança da Informação. A metodologia consiste, primeiramente, em um levantamento bibliográfico, de forma a compor a fundamentação teórica e definir a proposta inicial. A partir disso, foi realizada a construção do aplicativo, baseada no Modelo Incremental. Por fim, foi realizada uma avaliação de usabilidade para verificar o estado de aceitação de uso do aplicativo. Os resultados mostraram a aceitação do aplicativo em aspectos de usabilidade, desempenho e relevância no conteúdo, e também o desejo de ser utilizado pelos usuários que participaram do processo de teste.*

1. Introdução

Na atualidade, uma variedade de dispositivos conectados desempenha funções de coleta, transmissão, armazenamento e compartilhamento de dados, muitos dos quais são de natureza pessoal e até mesmo íntima. O uso cada vez mais difundido desses dispositivos no mercado implica na necessidade premente de considerar os riscos que eles podem representar para a privacidade e a segurança dos usuários (Magrani, 2018).

Conforme dados do IBGE (2021), a pesquisa de Tecnologia da Informação e Comunicação (TIC) apontou que entre 2018 e 2019, a proporção de residências com acesso à internet aumentou. No entanto, de acordo com Castro (2021), esse aumento significativo na conectividade também trouxe consigo um aumento alarmante nos casos de golpes e fraudes digitais.

Segundo informações fornecidas pela renomada empresa de segurança digital Kaspersky, os ataques cibernéticos vêm crescendo consideravelmente em decorrência do aumento da digitalização. Adicionalmente, aproximadamente 69 empresas brasileiras enfrentam ataques que resultaram em vazamento e sequestro de dados durante o primeiro semestre de 2021. Esse cenário ressalta a urgência da conscientização e da proteção na esfera digital (Redação, 2022).

Para Conceição, Medeiros e Medeiros (2018), as pessoas frequentemente representam o elo mais vulnerável nas organizações, muitas vezes devido à falta de compreensão quanto ao real valor da informação. Uma estratégia eficaz para abordar essa fragilidade é a conscientização, juntamente com o fornecimento de treinamentos que permitam às pessoas identificarem riscos e ameaças. Essa abordagem não apenas dificulta as tentativas de coleta de dados por parte de indivíduos mal-intencionados, mas também ajuda a preparar a sociedade para lidar com desafios persistentes, como a engenharia social, para a qual recursos eficazes ainda são escassos. Uma das maneiras inovadoras de promover essa conscientização é através do uso de dispositivos móveis, aproveitando a abordagem de aprendizado móvel (mobile learning).

O mobile learning (aprendizado por meio de dispositivos móveis) tem desencadeado transformações significativas nos hábitos cotidianos da sociedade moderna. Esse movimento é evidente nas mudanças observadas nas relações sociais, no ambiente de trabalho e, em particular, na educação e processo de aprendizado (Júnior, 2016). De acordo com Nichele e Schlemmer (2014), a utilização de dispositivos móveis oferece uma maior mobilidade e comodidade tanto para estudantes quanto para professores. Isso é possibilitado pelas interfaces de fácil utilização desses dispositivos, que abrem um leque de possibilidades e interações entre os envolvidos, sejam eles alunos, professores, dispositivos, aplicativos ou o próprio ambiente (incluindo o local geográfico onde os participantes se encontram).

Com base nesse contexto, a metodologia adotada para este trabalho foi definida em três etapas: na primeira etapa foi realizado um levantamento bibliográfico para compor a fundamentação teórica e definir uma proposta inicial. Na segunda etapa, foi realizada a construção de um aplicativo móvel, usando como base a utilização do modelo de processo incremental que consiste em uma sequência de atividades para criação de um produto essencial, sendo passível de atualização caso necessário. Na terceira etapa do projeto, foi realizado uma avaliação do aplicativo junto aos usuários para coleta de informações. Sendo aplicado um questionário com perguntas relacionadas a usabilidade do aplicativo e a relevância dos conteúdos exibidos.

O objetivo principal é propor uma aplicação móvel que auxilie no ensino-aprendizagem sobre Segurança da Informação (SI), de forma a contribuir para que os usuários aprimorem seus conhecimentos relacionados à segurança, permitindo que tenham o domínio do assunto e um nível de conhecimento mais amplo, possibilitando o reconhecimento de situações de vulnerabilidade, evitando ser vítimas de fraudes.

Podendo testar o conhecimento adquirido através de um quiz, após o estudo de um conteúdo.

O trabalho está organizado da seguinte maneira. A Seção 2 apresenta alguns conceitos básicos e discute os trabalhos relacionados. A Seção 3 apresenta o método de pesquisa utilizado enquanto a Seção 4 mostra os resultados e as discussões. A Seção 5 apresenta as conclusões e os trabalhos futuros.

2. Fundamentação Teórica

2.1. Conceitos Relacionados

2.1.1. Segurança da Informação

A segurança da informação é um campo que desempenha um papel crítico na proteção de dados, sistemas e informações contra ameaças cibernéticas. Três conceitos fundamentais orientam a segurança da informação: confidencialidade, integridade e disponibilidade.

A confidencialidade refere-se à restrição do acesso a informações sensíveis, garantindo que apenas pessoas autorizadas possam acessar dados ou recursos específicos. A integridade visa garantir que os dados não tenham sido modificados de maneira não autorizada, protegendo contra alterações indesejadas. Por fim, a disponibilidade assegura que as informações estejam acessíveis quando necessário, evitando interrupções indesejadas. Esses conceitos são os alicerces da segurança da informação, guiando as estratégias de proteção de dados em organizações e sistemas de TI (Hintzbergen, et al., 2018).

A segurança da informação é de suma importância para indivíduos, organizações e sociedade como um todo. Para os indivíduos, ela protege a privacidade e a segurança pessoal, garantindo que informações sensíveis, como dados financeiros e médicos, permaneçam confidenciais. Além disso, previne fraudes e roubos de identidade, promovendo a confiança ao compartilhar informações online (Fontes, 2017).

Para as organizações, a segurança da informação é fundamental para proteger a integridade dos dados empresariais, a propriedade intelectual e a reputação. A perda de confiança do público devido a violações de segurança pode resultar em perda de negócios. Em nível societal, a segurança da informação protege a infraestrutura crítica, como serviços de saúde, energia e transporte, contra interrupções graves. Também desempenha um papel na segurança nacional e na conformidade com regulamentações de proteção de dados (Lyra, 2015).

Há uma variedade de ameaças comuns à segurança da informação que podem comprometer a confidencialidade, integridade e disponibilidade dos dados. Entre essas

ameaças, encontramos malware, que inclui vírus, worms e trojans que podem infectar sistemas e roubar informações. O phishing, uma técnica de engenharia social, visa enganar os usuários para revelar informações confidenciais, como senhas e números de cartão de crédito (Lourenço, 2020).

A engenharia social envolve a manipulação psicológica para obter informações confidenciais, muitas vezes por meio de ações enganosas. Os ataques de força bruta são tentativas repetidas de adivinhar senhas, explorando vulnerabilidades na autenticação. Além disso, os ataques de negação de serviço (DoS) sobrecarregam sistemas ou redes, tornando-os inacessíveis. Compreender essas ameaças é essencial para implementar medidas eficazes de segurança da informação (Silva *et.al* 2016).

Para proteger dados e sistemas contra ameaças cibernéticas, várias medidas de segurança comuns são empregadas. A criptografia é uma técnica que transforma informações em um formato ilegível, protegendo os dados durante o armazenamento e a transmissão. A autenticação verifica a identidade dos usuários, geralmente por meio de senhas, autenticação de dois fatores ou biometria. A autorização controla o acesso a recursos com base em permissões definidas, garantindo que apenas usuários autorizados possam realizar ações específicas. Firewalls filtram o tráfego de rede, bloqueando ameaças e protegendo a infraestrutura de TI (Cabral e Caprino, 2015). Essas medidas de segurança são parte integrante da proteção de dados e sistemas em ambientes digitais e podem ser aplicadas em diversos contextos, incluindo aplicativos móveis e sistemas de TI.

2.1.2. Desenvolvimento de Aplicativos Móveis

O desenvolvimento de aplicativos móveis é um campo em constante crescimento, impulsionado pelo aumento do uso de dispositivos móveis, como smartphones e tablets. As principais plataformas móveis incluem iOS, desenvolvido pela Apple, e Android, desenvolvido pelo Google. Cada plataforma possui suas próprias linguagens de programação, como Swift para iOS, Java e Kotlin para Android (Cruz e Pretucelli 2017).

O ciclo de vida do desenvolvimento de aplicativos móveis envolve várias etapas, desde a concepção e design até o desenvolvimento, testes, implantação e manutenção. Durante o processo de desenvolvimento, é importante considerar fatores como o desempenho, a segurança e a usabilidade do aplicativo (Gomes, 2017).

As boas práticas de desenvolvimento de aplicativos móveis incluem a criação de uma arquitetura sólida para o aplicativo, a otimização do desempenho para garantir que ele seja responsivo e eficiente, e a criação de interfaces de usuário amigáveis e intuitivas para proporcionar uma experiência positiva ao usuário (Guimarães e Tavares, 2014).

2.1.3. Segurança em Aplicativos Móveis

Os aplicativos móveis estão sujeitos a ameaças e desafios específicos de segurança. Devido à sua natureza portátil e à capacidade de acesso a informações pessoais e sensíveis, eles são alvos de ataques. Algumas das técnicas de segurança comuns em aplicativos móveis incluem autenticação de dois fatores, que adiciona uma camada extra de segurança, e o armazenamento seguro de senhas para evitar vazamentos de informações de login (Six, 2012).

Também é essencial garantir atualizações regulares de segurança para corrigir vulnerabilidades à medida que são descobertas. Diretrizes de segurança, como as definidas pelo Projeto de Segurança de Aplicações Web Abertas (OWASP), oferecem orientações detalhadas sobre as melhores práticas de segurança em aplicativos móveis, desde a prevenção de injeção de SQL até a proteção contra ataques de negação de serviço (Silva, 2022).

2.1.4. Abordagem de Usabilidade

A usabilidade desempenha um papel crítico na eficácia de um aplicativo móvel de segurança da informação. A usabilidade refere-se à facilidade de uso e à experiência do usuário ao interagir com o aplicativo. Para garantir que os usuários adotem e confiem no aplicativo, é fundamental seguir princípios de design de interfaces de usuário amigável (Batista, 2018).

Isso inclui criar uma interface intuitiva, onde as funções e recursos do aplicativo sejam facilmente compreensíveis para o usuário. Além disso, os elementos de design devem ser consistentes e seguir as diretrizes da plataforma móvel específica, seja iOS ou Android, para garantir que o aplicativo se integre de maneira harmoniosa no ambiente do dispositivo (Neto, Filho e Almeida, 2019).

Testes de usabilidade são essenciais durante o desenvolvimento do aplicativo, permitindo que os desenvolvedores identifiquem problemas de usabilidade e façam melhorias antes do lançamento. Envolvimento dos usuários, por meio de feedback e pesquisa, é fundamental para entender suas necessidades e preferências, resultando em um aplicativo mais eficaz e atraente (Mercês e Araújo, 2023).

2.1.5. Legislação e Conformidade

À medida que a sociedade digital cresce e as preocupações com a privacidade e segurança de dados aumentam, várias regulamentações e leis foram promulgadas em níveis nacionais e internacionais para proteger os direitos dos indivíduos e garantir a segurança da informação. Essas regulamentações têm um impacto significativo no

desenvolvimento de aplicativos móveis de segurança da informação, uma vez que os aplicativos frequentemente lidam com dados pessoais e sensíveis (Neves *et al.,* 2021).

Um exemplo notável é o Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor na União Europeia em maio de 2018. O GDPR estabelece regras rigorosas sobre a coleta, o processamento e a proteção de dados pessoais e se aplica a organizações em todo o mundo que tratam informações de cidadãos da UE. Os aplicativos móveis que lidam com dados pessoais de usuários da UE devem cumprir o GDPR, o que inclui a obtenção de consentimento explícito para a coleta de dados e a implementação de medidas de segurança adequadas (Magalhães e Pereira, 2020).

No Brasil, a Lei Geral de Proteção de Dados (LGPD), inspirada no GDPR, entrou em vigor em setembro de 2020. Ela estabelece princípios e diretrizes semelhantes para o tratamento de dados pessoais, garantindo a privacidade e a segurança das informações dos cidadãos brasileiros. Qualquer aplicativo móvel que colete dados de cidadãos brasileiros deve aderir às disposições da LGPD (Sabino, 2020).

É fundamental que desenvolvedores de aplicativos móveis de segurança da informação estejam cientes das regulamentações relevantes em sua região e garantam que seus aplicativos estejam em conformidade. Isso envolve a implementação de recursos de segurança, como a criptografia de dados, a adoção de políticas de privacidade transparentes e a obtenção de consentimento de usuário apropriado. Além disso, a conformidade contínua e a atualização dos aplicativos para atender às mudanças na legislação são essenciais para garantir a segurança e a privacidade dos usuários.

2.2. Trabalhos Relacionados

2.2.1. Rocha *et al*. (2022)

Rocha *et al*. (2022), apresenta uma pesquisa e análise sobre o nível de popularização das iniciativas para a educação digital e segurança da informação na internet, com o objetivo de analisar as iniciativas Cert.br, Segura Net e ICANN, devido ao seu foco na educação digital, no qual suas plataformas disponibilizam recursos educacionais de ensino/aprendizagem.

Para atingir tal objetivo foi utilizado a estratégia quantitativa para comparar o impacto das iniciativas nas redes sociais e sites oficiais e a estratégia qualitativa para comparar missão, financiamento e serviços englobando, áreas e público alvo. Por meio do estudo das plataformas e meios de divulgação, foi realizada uma comparação, a partir do levantamento de tráfego de seus respectivos sites, redes sociais e serviços desenvolvidos.

Como resultado da análise realizada pelos autores, é possível perceber que o ICANN se destaca dos demais, por ser voltado ao público mundial com base em serviços

de DNS. Por esse motivo, seu tráfego de rede é tão superior às outras iniciativas, visto que é conhecido mundialmente por sua importância na segurança e estabilidade das redes. Apesar do ICANN se destacar mundialmente, tanto o Cert.br quanto o SeguraNet se destacam nacionalmente, representados por Brasil e Portugal, respectivamente.

As iniciativas têm como missão contribuir para formação dos usuários sobre segurança na internet, uma vez que atuam em diferentes cenários, como educação, no caso do ICANN e SeguraNet, e no tratamento de incidentes em redes de conexão no Brasil, com o Cert.Br.

Para contribuir e melhorar os resultados a respeito dos aspectos de segurança na internet, o aplicativo I7Safe pode incorporar em seu conteúdo o direcionamento para as plataformas analisadas neste trabalho, bem como proporcionar ao usuário um acompanhamento de seu aprendizado com o quiz disponibilizado no aplicativo.

2.2.2. Carvalho, Reis e Alves (2017)

O trabalho de Carvalho, Reis e Alves (2017) teve o objetivo de reunir dados para demonstrar a necessidade da formação e conscientização de docentes, discentes e toda a comunidade escolar no que tange às noções básicas sobre Segurança da Informação e os principais fatores de riscos aos quais os usuários estão sujeitos, ao desempenharem suas atividades cotidianas a partir de dispositivos conectados em rede.

A metodologia adotada neste trabalho seguiu uma abordagem não experimental, e sim por um levantamento realizado por questionários online para sua elaboração e execução. Aos participantes da pesquisa foi aplicado um questionário com questões de múltipla escolha, onde puderam ser avaliados o conhecimento dos participantes, e como estes podem lidar com situações de riscos, como fraudes de antecipação de recursos, rastreamento de atividades, falsificação de e-mails, Cyberbullying, entre outros. Os dados coletados a partir dos questionários foram analisados estatisticamente para identificar os riscos menos frequentes, estimar o conhecimento do público em relação a cada vulnerabilidade avaliada, além de fundamentar o tratamento mais adequado em cada caso.

Como resultado, a pesquisa demonstrou que professores e alunos do Ensino Médio, e também do Ensino Superior estão expostos a diversas vulnerabilidades perigosas quando de suas atividades online, ficando clara a necessidade de um entendimento maior e capacidade das pessoas em lidar com situações de tais como: senhas fracas, troca de informações íntimas, fraudes de antecipação, entre outras. Dessa forma, o trabalho propôs ações educativas para o tratamento dos fatores de maior risco, como disciplinas, treinamentos, elaboração de materiais diversos e capacitação para professores e alunos.

Este trabalho foi aplicado no contexto educacional em uma escola de ensino médio, de forma que foi trabalho exclusivamente na pesquisa e na proposição de soluções

para o mesmo público alvo. O I7Safe é um aplicativo que será destinado a todos os usuários da internet, independente do ambiente ou idade, utilizando de informações atualizadas para gerar conhecimento e auxiliar os usuários na prevenção de problemas relacionados à segurança da informação.

2.2.3. Silva e Guarda (2019)

Silva e Guarda (2019) propuseram uma metodologia e objetos de aprendizagem utilizando as premissas da aprendizagem criativa, para ensinar alunos do ensino fundamental em conceitos de criptografia, a partir de conceitos de lógica de programação no jogo digital educacional Run Marco. O objetivo da aplicação da metodologia é desenvolver habilidades de abstração, decomposição, coleta de dados e construção de algoritmos. Para minimizar dúvidas em relação aos assuntos abordados, foram realizadas aulas preparatórias com os alunos, onde foram inseridos conceitos fundamentais de lógica de programação.

Para aplicação da dinâmica, os participantes foram divididos em grupos para escolher as fases do jogo que iriam resolver para descobrir a chave de criptografia de mensagens codificadas. A técnica utilizada para implementação da atividade foi a Cifra de César, na qual cada letra do alfabeto é substituída por um número inteiro. Dessa forma, os participantes puderam interagir e seguir as regras do jogo para resolver o problema, e utilizaram os conceitos aprendidos para propor a solução.

Os resultados obtidos demonstraram a maturidade da turma durante as análises para desenvolver as fases do jogo Run Marco e que, para descobrir a chave de criptografia, era necessário concentração da equipe para evitar erros nos cálculos. Outro fator, foi a utilização de estruturas complexas para a solução do problema, indicando o melhoramento do rendimento da turma a partir da exposição dos conteúdos aplicados previamente. Dessa forma, a abordagem utilizada contribui para a motivação dos alunos em aprender os conteúdos da área de computação, precisamente em criptografia.

Por se tratar de um tema relacionado à segurança da informação, a abordagem utilizada desperta o interesse dos alunos em conhecer técnicas que podem ajudar na prevenção de riscos, mesmo os participantes estando ainda no ensino fundamental. Nesse sentido, torna-se possível aos estudantes, no futuro, que sejam capazes de construir modelos mentais para abstrações computacionais e formalizados em linguagens de programação.

O I7Safe, diferentemente deste trabalho, proporciona o conhecimento em diversas áreas da Segurança da Informação e não somente em criptografia e também disponibiliza em sua própria plataforma um quiz para que o usuário acompanhe seu aprendizado.

2.2.4. Santos, Araújo e França (2019)

Santos, Araújo e França (2019) apresentam um protótipo de aplicativo móvel por meio de gamificação, como ferramenta de auxílio no setor de recursos humanos de empresas, visando reduzir os impactos negativos causados pela transformação digital, promovendo o engajamento de usuários em busca de aprendizado, para uso consciente das tecnologias. No ambiente empresarial, torna-se necessário educar os colaboradores para o uso adequado das ferramentas tecnológicas.

O protótipo do aplicativo Safegame foi desenvolvido baseando-se em elementos comuns de design de jogos como, com um ranking baseado na pontuação dos jogadores, jogos de perguntas e respostas para testar o conhecimento dos colaboradores. As perguntas deste jogo serão selecionadas de um banco de questões já cadastrado no aplicativo. A ideia do jogo é baseada na gamificação, de forma que proporcione recompensa aos usuários que conseguem marcar as questões corretas.

O trabalho foi desenvolvido como um protótipo de aplicação web, como um estudo de novas tecnologias e aprofundamento em técnicas já conhecidas. O desenvolvimento se apoiou não apenas em uma tecnologia versátil, atrativa e de rápida prototipação de ideias como as utilizadas – Vue JS e, mas também a construção do projeto foi realizada tendo como um dos pilares a técnica de gamificação, explorando a área de segurança da informação.

O I7Safe possui características equivalentes com o Safegame, pois aborda os conceitos baseados em gamificação e segurança da informação. O I7Safe é um aplicativo móvel explorado pelo público em geral, com uma abordagem baseada em pontuação, na qual o usuário assume um nível de conhecimento e segurança da informação.

3. Procedimentos Metodológicos

A metodologia utilizada neste trabalho está dividida em três etapas fundamentais, sendo:

- **Levantamento bibliográfico**: esta primeira etapa é essencial para embasar o desenvolvimento teórico do trabalho de pesquisa. Foram realizadas pesquisas bibliográficas em sites que tratam sobre Segurança da Informação, artigos científicos em anais de eventos acadêmicos e eventos de pesquisa e tecnologia, monografias; trabalhos de conclusão de cursos, dissertações e teses em repositórios de universidades públicas e privadas, busca em livros acadêmicos virtuais e na biblioteca do Instituto Ciências Exatas e Tecnologia. Na visão de Pizzani et al (2012), o levantamento bibliográfico é entendido como uma revisão da literatura em que norteia teoricamente o trabalho científico, sendo que este pode ser pesquisado através de livros, periódicos, artigos de jornais, sites da Internet entre outras fontes.

- **Desenvolvimento do software:** para a segunda etapa, fez-se o uso do modelo incremental para a implementação no desenvolvimento de software. De acordo com Pressman et al (2002), o modelo incremental é uma metodologia ágil que tem por objetivo fazer a divisão do projeto de desenvolvimento em partes completas e pode ser construída de forma sequencial. As ações para a construção do sistema seguiram da seguinte forma:
    a) **Levantamento de Requisitos**: foi realizado um formulário com questões para obtenção de requisitos para desenvolver a aplicação.
    b) **Modelagem**: documentação que vai esclarecer o que a ferramenta irá fazer através dos requisitos solicitados. Para a criação dos diagramas UML (Unified Modeling Language) de caso de uso, classes, sequência e atividade, será utilizado a ferramenta Astah uml;
    c) **Arquitetura**: foram identificados os componentes estruturais da aplicação e o relacionamento entre eles. Foram utilizados os softwares Microsoft Office Powerpoint e Canva para elaboração da figura da arquitetura;
    d) **Banco de Dados**: foi rompida a integração da aplicação com o Firebase para a gestão do banco de dados. Dado que o Firebase é uma solução de banco de dados NoSQL, foi apresentada uma representação visual abrangente de toda a arquitetura do banco de dados para uma compreensão mais clara.
    e) **Implementação**: a implementação do aplicativo foi realizada em Kotlin, utilizando o framework Android Studio e integrando o Firebase como o banco de dados. O desenvolvimento se concentrou na criação de uma interface de usuário intuitiva e eficiente, de acordo com os requisitos levantados;
- **Avaliação:** na terceira etapa do projeto, realizou-se uma avaliação do aplicativo junto aos usuários para coleta de informações. Para isso, foi disponibilizado um questionário com perguntas relacionadas a usabilidade do aplicativo e a relevância dos conteúdos disponibilizado no mesmo.

4. Resultados e Discussões

4.1. Projeto do Aplicativo I7Safe

4.1.1. Levantamento dos Requisitos

No processo de comunicação, a etapa de levantamento de requisitos é essencial na engenharia de software. O propósito é compreender as expectativas dos diversos stakeholders em relação ao software a ser desenvolvido (Pressman e Maxim, 2016).

4.1.1.2. Análise do Levantamento de Requisitos

No formulário utilizado para a coleta de requisitos do desenvolvimento da aplicação, obtivemos um total de oitenta e sete respostas. Com base nesses resultados, observou-se que 18% das respostas provêm de indivíduos com idades entre 18 e 21 anos, enquanto 60% das respostas são de pessoas cujas idades variam de 22 a 30 anos.

Dentre todos os participantes da pesquisa, mais de 50% dos entrevistados completaram o Ensino Médio. Cerca de 49% dos participantes afirmaram não possuir conhecimento prévio sobre Segurança da Informação (SI). Notavelmente, 80,5% dos entrevistados relataram ter pessoalmente sofrido ou conhecido alguém que tenha sido vítima de golpes na internet. Além disso, 93,1% das pessoas entrevistadas expressaram seu interesse em aprimorar seus conhecimentos em segurança da informação, e impressionantes 97,7% consideram que uma aplicação com essa finalidade seria benéfica em seu dia a dia.

4.1.1.3. Requisitos Funcionais e Não Funcionais

Os requisitos podem ser categorizados em requisitos funcionais e requisitos não-funcionais. Os requisitos funcionais visam atender às necessidades práticas do usuário do sistema, descrevendo as funções que o sistema ou seus componentes devem desempenhar. Eles representam processos que utilizam entradas para produzir saídas. Por outro lado, os requisitos não-funcionais estabelecem restrições e critérios de desempenho que o software deve cumprir (Costa, 2018).

Portanto, para a primeira versão do sistema, foram definidos requisitos funcionais (RF) e requisitos não-funcionais (RNF), conforme detalhado nas Tabelas 1 e 2, respectivamente.

Tabela 1. Requisitos funcionais

Identificador	Descrição	Prioridade	Requisitos Relacionados
RF01	Fazer login	Essencial	[RNF002], [RN03]
RF02	Criar conta	Essencial	[RNF003]
RF03	Visualizar conteúdo	Essencial	[RNF005], [RN02]
RF04	Realizar quiz	Essencial	[RN05]
RF05	Visualizar resultado do quiz	Essencial	[RN04]

Tabela 2. Requisitos não-funcionais

Identificador	Descrição	Categoria	Prioridade	Requisitos Relacionados
RNF001	O sistema deve responder de forma rápida e eficiente às ações do usuário, garantindo que as páginas e os quizzes sejam concluídos sem atrasos perceptíveis	Desempenho	Essencial	
RNF002	As senhas dos usuários devem ser criptografadas	Segurança	Essencial	[RF01], [RF02]
RNF003	O sistema deve garantir que os dados dos usuários sejam armazenados com segurança e protegido contra acesso não autorizado	Segurança	Essencial	[RF01], [RF02]
RNF004	O sistema deverá estar disponível 24 horas por dia e 7 dias por semana	Disponibilidade	Essencial	
RNF005	O sistema deve ser fácil de usar, com uma interface de usuário intuitiva que permita aos usuários navegar facilmente pelos recursos do aplicativo	Usabilidade	Essencial	

As regras de negócio, de acordo com Guedes (2018), englobam políticas, diretrizes e condições definidas pela organização que devem ser observadas durante a implementação de uma funcionalidade. Portanto, a Tabela 3 contém as regras de negócio essenciais para a realização deste projeto.

Tabela 3. Requisitos não-funcionais

Identificador	Descrição	Prioridade	Requisitos Relacionados
[RN01]	Os usuários devem estar registrados e logados para acessar os conteúdos e o quiz	Essencial	[RF01], [RF02], [RF03], [RF04], [RF05]
[RN02]	O aplicativo deve exibir uma listagem de todos os assuntos nele contido	Essencial	[RF03]
[RN03]	O acesso do usuário ao sistema deverá ser feito por meio do seu e-mail e senha cadastrado	Essencial	[RF01], [RF02]
[RN04]	O quantitativo de erros e acertos do usuário no quiz só ficará disponível após todas as perguntas serem respondidas	Importante	[RF04], [RF05]

[RN05]	As perguntas do quiz devem estar diretamente relacionadas com o conteúdo selecionado	Essencial	[RF03], [RF04]

É relevante ressaltar que, em relação à priorização dos requisitos, foram estabelecidas as seguintes categorias:

- **Essencial**: esses requisitos são de suma importância, pois são indispensáveis para o funcionamento adequado do sistema. Sua implementação é prioritária, visto que o sistema não opera sem eles.
- **Importante**: nessa categoria, estão os requisitos que, embora não sejam essenciais, desempenham um papel relevante no desempenho satisfatório do sistema. Sua implementação é considerada importante para a qualidade geral do sistema.
- **Desejável**: requisitos classificados como desejáveis não afetam as funcionalidades básicas do sistema. Isso significa que o sistema pode operar de maneira satisfatória sem eles. A implementação desses requisitos pode ser considerada em versões subsequentes, caso não haja tempo disponível para sua inclusão na versão inicial.

4.1.2. Modelagem

4.1.2.1. Diagrama de Caso de Uso

Segundo Guedes (2018), com o intuído de apresentar o sistema de uma maneira simples aos usuários, o diagrama de casos de uso busca trazer uma ideia geral de como o sistema deve se comportar, pois tem como principal objetivo mostrar uma visão externa geral das funcionalidades, sem se preocupar com a questão de como tais funcionalidades serão implementadas. Considerando os requisitos coletados, o diagrama de caso de uso foi representado como demonstrado na Figura 1.

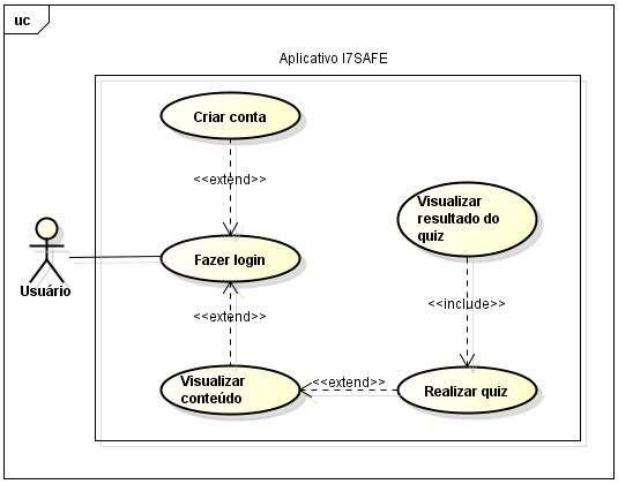


Figura 1. Diagrama de Caso de Uso

Para Guedes (2018) a documentação de casos de uso descreve por meio e linguagem simples, funções em linhas gerais do Caso de Uso, quais Atores interagem com o mesmo, quais etapas devem ser executadas pelo Ator e pelo sistema de forma que o que execute sua função, parâmetros que devem ser fornecidos e restrições e validações o Caso de Uso deve possuir. Dessa forma, na Tabela 4 e 5, respectivamente, são apresentadas a documentação de Caso de Uso "visualizar conteúdo" e "realizar quiz".

Tabela 4. Documentação de Caso de Uso "Visualizar Conteúdo"

Diagrama de Caso de Uso	**I7SAFE**
Caso de Uso Geral	Visualizar conteúdo
Ator Principal	Usuário
Ator Secundário	-
Resumo	Este caso de uso descreve as etapas percorridas para o usuário visualizar os conteúdos contidos no aplicativo
Pré-Condições	O usuário deve estar autenticado no sistema
Pós-Condições	O usuário pode visualizar e fazer leitura do conteúdo selecionado
Fluxo Principal	
Ações do Ator	**Ações do Sistema**
1 - Acessa a tela home do aplicativo	

	2 - Lista os conteúdos contidos no aplicativo para o usuário
3 - Clica no conteúdo desejado	
	4 - Redirecionar usuário para a tela do conteúdo selecionado
Fluxo Alternativo	
-	-

Tabela 5. Documentação de Caso de Uso "Realizar Quiz"

Diagrama de Caso de Uso	**I7SAFE**
Caso de Uso Geral	Realizar quiz
Ator Principal	Usuário
Ator Secundário	-
Resumo	Este caso de uso descreve as etapas percorridas para o usuário ter acesso ao quiz do conteúdo selecionado
Pré-Condições	- O usuário deve estar autenticado no sistema - O usuário deve selecionar o assunto que deseja visualizar
Pós-Condições	O usuário respondeu às perguntas do quiz
Fluxo Principal	
Ações do Ator	**Ações do Sistema**
1 - Clicar na opção "Resolver Quiz"	
	2 - O sistema redireciona o usuário para a tela do quiz
	3 - Exibe as perguntas e opções de resposta do quiz
4 - Selecionar a resposta correta e clicar em "Responder" para cada pergunta exibida na tela de quiz	
Fluxo Alternativo	
-	-

4.1.2.2. Diagrama de Classe

Segundo Sommerville (2011), o diagrama de classes, tem o objetivo de mostrar as classes de objeto no sistema e as associações entre elas. Neste tipo de diagrama os elementos principais são caixas, que tem a finalidade de representar as classes e interfaces, essas caixas são divididas em três partes horizontais, sendo que, na primeira parte está o nome da classe, na segunda parte localiza-se seus atributos e na terceira e última parte do diagrama fica localizado às operações ou comportamentos da classe (Pressman e Maxim, 2016). Neste sentido, a Figura 2 mostra o diagrama de classes modelado de acordo com os requisitos.

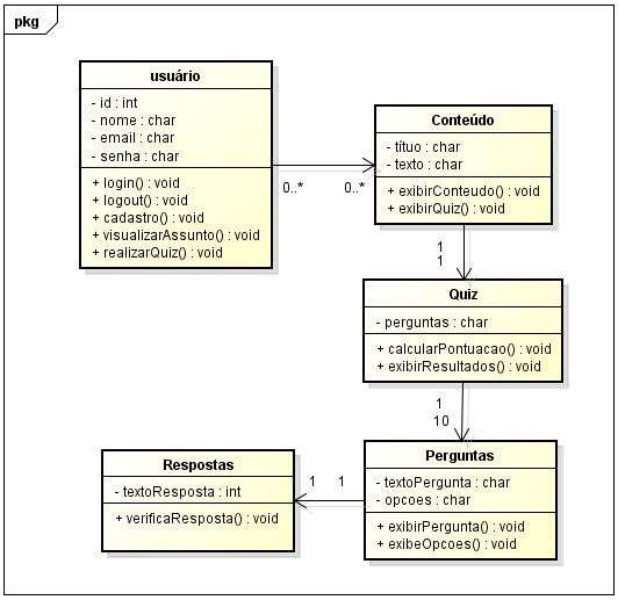


Figura 2. Diagrama de Classe

4.1.2.3. Diagramas de Sequência

O diagrama de sequência preocupa-se com a ordem temporal em que as mensagens são trocadas entre os objetos que estão envolvidos em um determinado processo. Este diagrama pode usar como base algumas características do diagrama de caso de uso e do diagrama de classes. Seu papel é ilustrar a ordem como as diferentes partes do sistema interagem (Guedes, 2018). Dessa forma, foram modelados os diagramas de sequência apresentados nas Figuras 3 e 4, respectivamente. Os demais Diagramas de Sequência podem ser observados no Apêndice A.

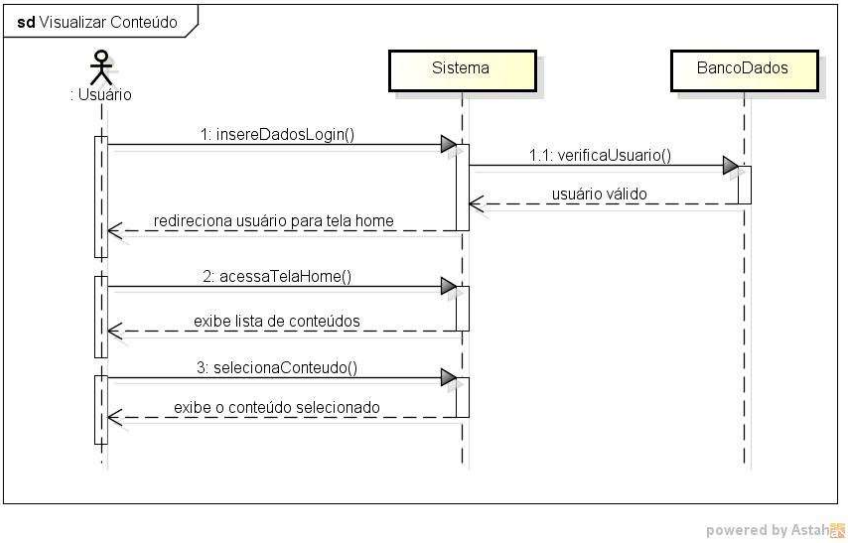


Figura 3. Diagrama de Sequência "Visualizar Conteúdo"

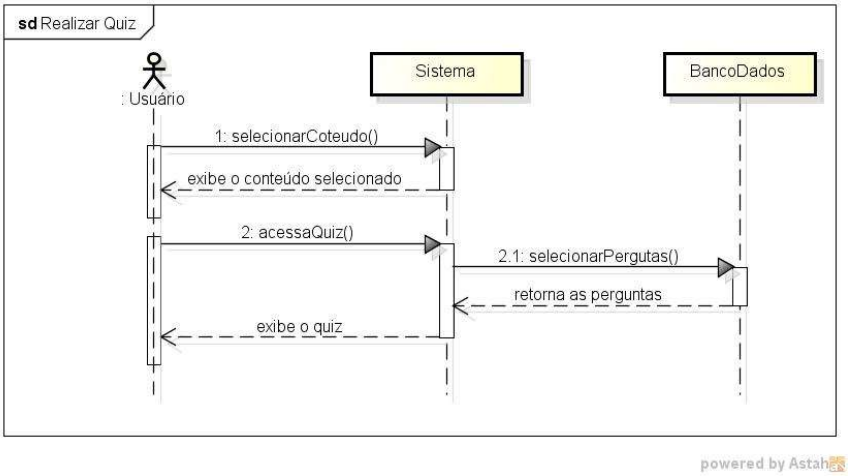


Figura 4. Diagrama de Sequência "Realizar Quiz"

4.1.2.4. Diagrama de Atividade

O diagrama de atividade é uma representação gráfica do fluxo de interação em um cenário específico, sua estrutura é semelhante a um fluxograma que mostra as atividades executadas por um sistema (Pressman e Maxim, 2016). Neste sentido, foram modelados os Diagramas de Atividades conforme mostra as Figuras 5 e 6, respectivamente. Os demais Diagramas de Atividades podem ser observados no Apêndice B.

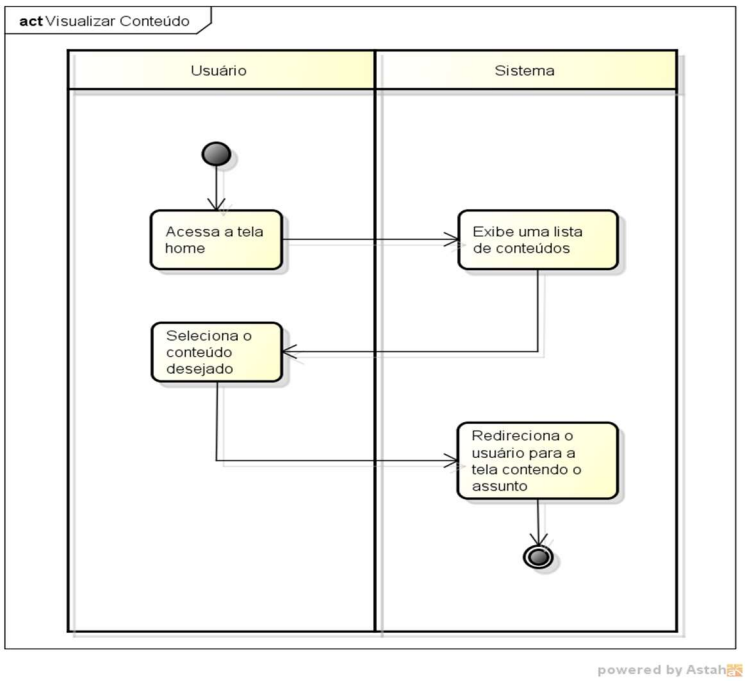


Figura 5. Diagrama de Atividade "Visualizar Conteúdo"

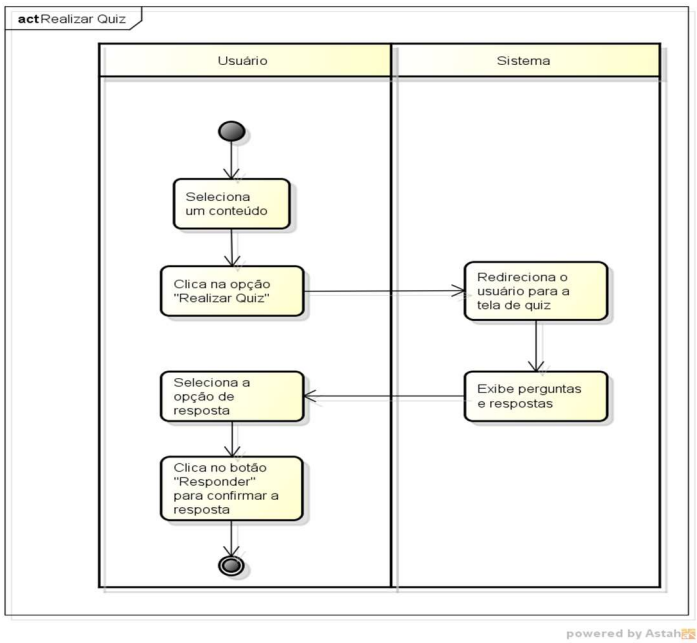


Figura 6. Diagrama de Atividade "Realizar Quiz"

4.1.2.5. Arquitetura

Na Figura 7, observa-se a estrutura da arquitetura do sistema.

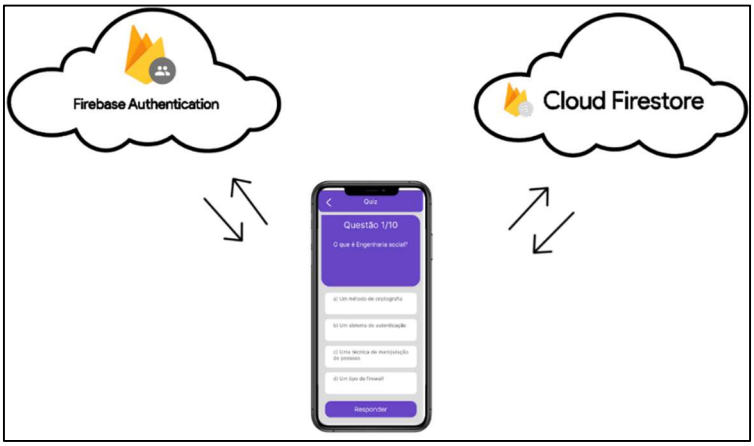


Figura 7. Arquitetura de software

4.1.2.6. Banco de Dados

Em relação ao banco de dados, foi utilizado o Firebase e por se tratar de um banco não relacional, sua estrutura é apresentada na Figura 8.

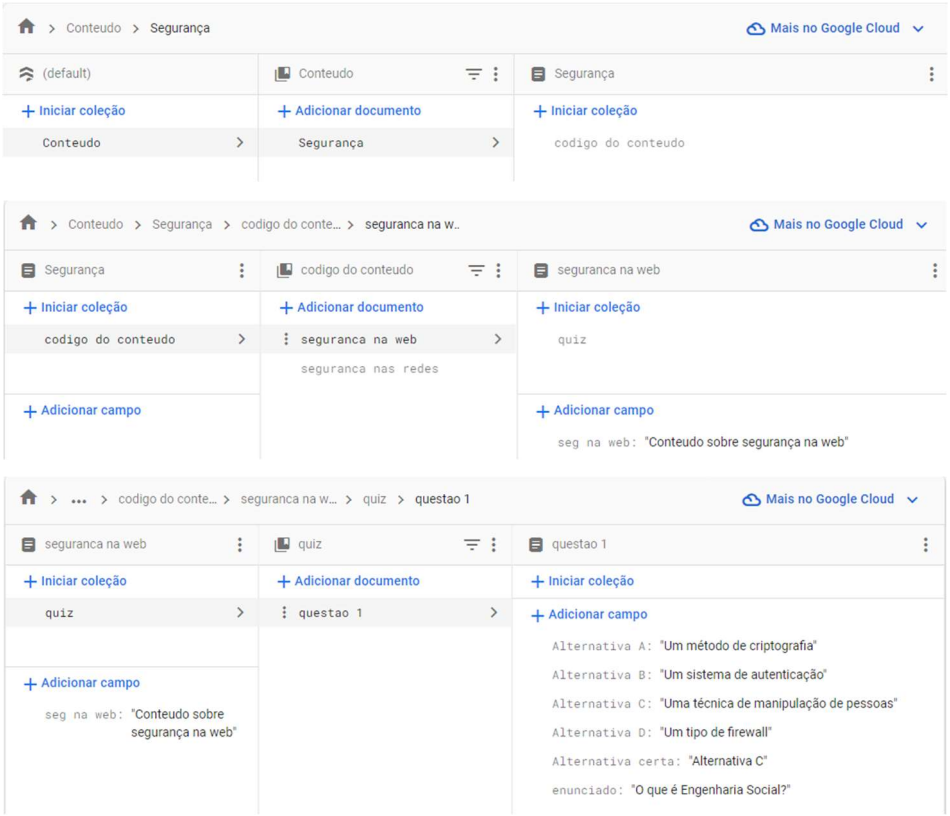


Figura 8. Estrutura do banco

4.2. Implementação do Aplicativo I7Safe

Nesta seção, serão apresentados os resultados do desenvolvimento do aplicativo I7Safe, como escopo dos tópicos relacionados ao levantamento de requisitos, modelagem do sistema e arquitetura do software. A seguir, serão exibidas as telas do software desenvolvido neste trabalho.

4.2.1. Telas do Aplicativo

Na Figura 9 (a) pode -se visualizar a interface de acesso da aplicação, na qual é exibida a tela de login, contendo dois campos interativos. Na figura 9 (b) permite o cadastro do usuário no aplicativo, onde o mesmo realiza o cadastro de seu e-mail e senha.

(a) **(b)**

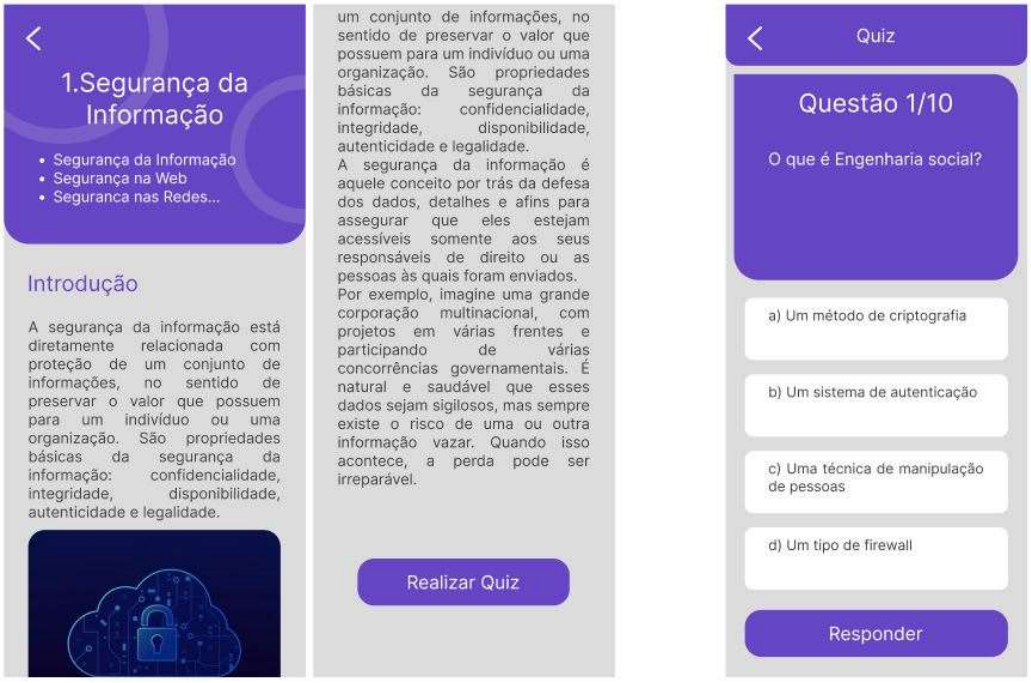
Figura 9. (a) Tela de Login e (b) Cadastro no App

Na Figura 10 (a), pode-se observar a interface inicial, onde o usuário pode realizar seu primeiro teste de conhecimento na aplicação. Na Figura 10 (b), temos a tela home onde pode-se visualizar a lista de conteúdos no aplicativo.

(a) **(b)**

Figura 10. (a) Tela inicial e (b) Home

Na Figura 11 (a) pode-se observar a interface de conteúdo da aplicação, onde o usuário visualiza conteúdo escolhido pelo mesmo. Na Figura 11 (b) contém a interface de quiz do conteúdo estudado.



(a) **(b)**

Figura 11. (a) Tela de conteúdo e (b) Quiz

4.2.2. Avaliação do Aplicativo I7Safe

A avaliação realizada no dia 23 de outubro de 2023, deu-se com pessoas de diversas idades e ocupação, sem a definição de um público específico, utilizando um smartphone contendo a aplicação em questão devidamente instalada, e teve como objetivo a aplicação de um questionário com questões para levantamento de dados de opinião dos usuários sobre usabilidade, desempenho e relevância do aplicativo.

4.2.2.1. Planejamento da Avaliação

• Definição dos Participantes

A seleção dos participantes não foi feita de forma específica, permitindo que o público em geral pudesse participar sem restrições ou critérios particulares.

• Definição da Instrumentação

Nesta etapa, foi desenvolvido um questionário para os participantes, contendo perguntas sobre os dados dos participantes (veja a Figura 13) e sobre a usabilidade e aceitação do aplicativo desenvolvido (veja a Figura 14). Antes de responder ao questionário, os participantes assinaram um termo de consentimento livre e esclarecido, como pode ser observado na Figura 12.

Avaliação: "I7Safe - Aplicativo para Auxiliar o Aprendizado em Segurança da Informação".

Prezado(a) Participante,

Meu nome é Emarielle Almeida Prado, estudante do curso de Sistema de Informação na Universidade Federal do Amazonas. Estou conduzindo uma avaliação do aplicativo de aprendizagem denominado I7Safe como parte do meu trabalho de conclusão de curso (TCC), sob a orientação do Prof. Alternei de Souza Brito. O objetivo deste estudo é apresentar uma proposta de um aplicativo alternativo para aprendizagem em Segurança da Informação

Sua participação é muito importante, pois ajudará na avaliação das funcionalidades implementadas na versão atual do software, bem como na análise da interface e outras características. As respostas fornecidas por você neste questionário serão utilizadas para aprimorar o software. O preenchimento do questionário deve levar aproximadamente de 5 a 10 minutos. Sua contribuição é fundamental para a conclusão deste trabalho.

Sua participação neste estudo é voluntária, e você pode desistir a qualquer momento. Sua identidade será mantida em total sigilo na divulgação dos resultados desta pesquisa. Todas as informações que possam identificá-lo(a) serão omitidas.

Antes de começar você precisa aceitar participar da pesquisa.

( ) Eu aceito participar

( ) Não aceito participar

Figura 12. Termo de consentimento livre e esclarecido

Dados do Participante

1. Qual sua idade?

Resposta:_____

2. Qual sua profissão?

Resposta:_____

3. Qual seu grau de escolaridade?

Resposta:_____

Figura 13. Questionário de perfil do participante

Formulário de Avaliação

4. As informações contidas no aplicativo são apresentadas de forma intuitiva e clara?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

5. O aplicativo I7Safe consegue ter clareza nos comandos facilitando sua utilização?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

6. Você acredita que as informações apresentadas no aplicativo irão ajudar no seu aprendizado?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

7. Foi fácil ganhar habilidade no uso do sistema?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

8. O sistema mostrou ter um bom tempo de execução?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

9. O público interessado teria algum tipo de limitação em utilizar o aplicativo?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

10. O aplicativo pode ser utilizado no dia a dia do público interessado, independentemente de ser no ambiente educacional?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

11. Você acredita que a aplicação I7Safe pode ser utilizado como ferramenta de apoio ao ensino-aprendizagem?

( ) Concordo Totalmente

( ) Concordo

( ) Neutro

( ) Discordo

( ) Discordo Totalmente

Figura 14. Formulário de avaliação do aplicativo

4.2.2.2. Resultado da Avaliação

Nesta seção, serão apresentados os resultados do questionário de avaliação (QA) conduzido durante a fase de avaliação do software. A pesquisa foi realizada no município de Itacoatiara, onde foram coletadas 13 respostas de usuários de vários perfis.

- **Perfil dos Participantes Avaliadores**

Conforme ilustrado na Figura 15, as respostas foram provenientes de usuários de diferentes faixas etárias, variando de 15 a 46 anos. Na figura 16, pode ser visualizado a

ocupação dos participantes, é interessante observar que possuem ocupações diversas e que 61,5% são estudantes.

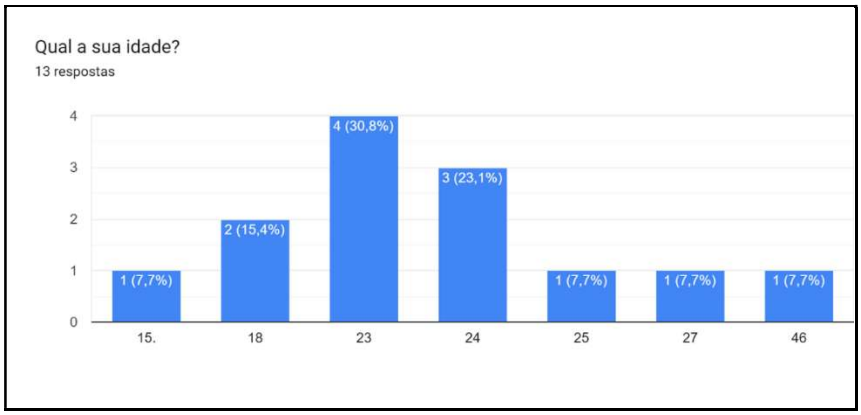


Figura 15. Formulário de avaliação do aplicativo

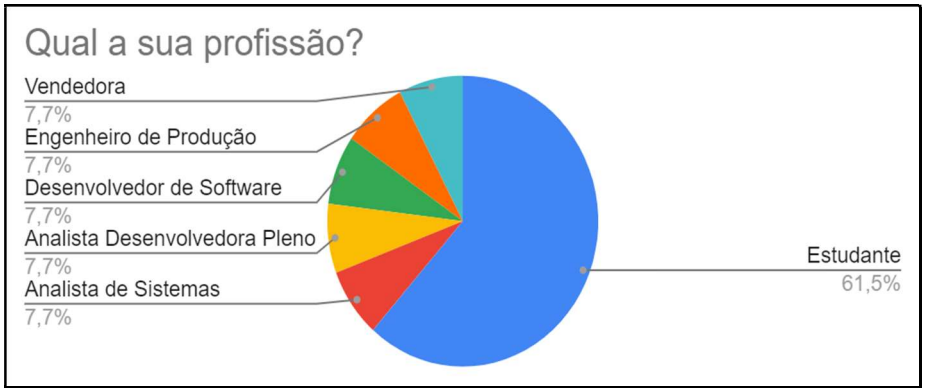


Figura 16. Formulário de avaliação do aplicativo

- **Formulário de Avaliação**

Conforme apresentado na Figura 17, tratando-se da clareza das informações apresentadas, percebeu-se que 69,2% dos participantes concordaram totalmente com a usabilidade do aplicativo. Além disso, 23,1% concordaram com esse atributo. Em contrapartida, 7,7% dos avaliadores discordaram em relação a esse aspecto.

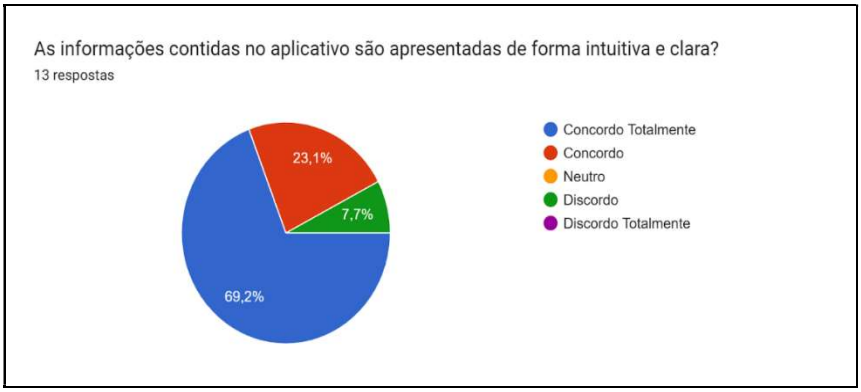


Figura 17. Formulário de avaliação do aplicativo

Ao examinar os comandos interativos, observou-se que 53,8% concordaram totalmente com a característica de clareza nos comandos do aplicativo. Além disso, 46,2% concordaram em relação a essa questão de pesquisa, conforme apresentado na Figura 18.

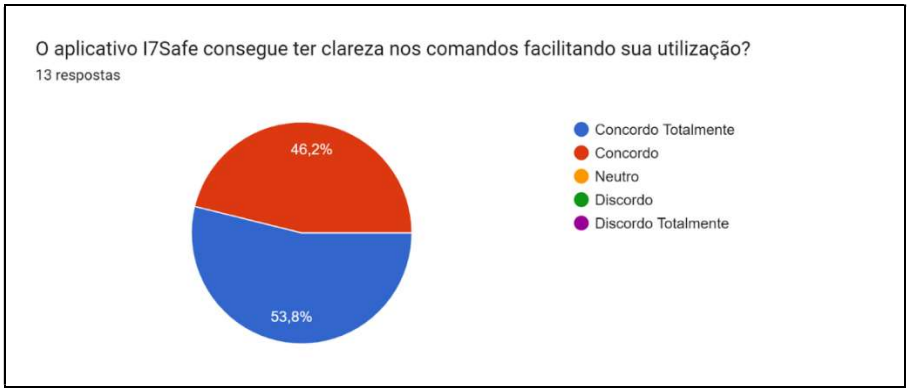


Figura 18. Formulário de avaliação do aplicativo

Quanto aos conteúdos apresentados, constatou-se que 61,5% concordaram totalmente que as informações serão úteis para o seu aprendizado, enquanto 38,5% concordaram com a questão de pesquisa, conforme demonstrado na Figura 19.

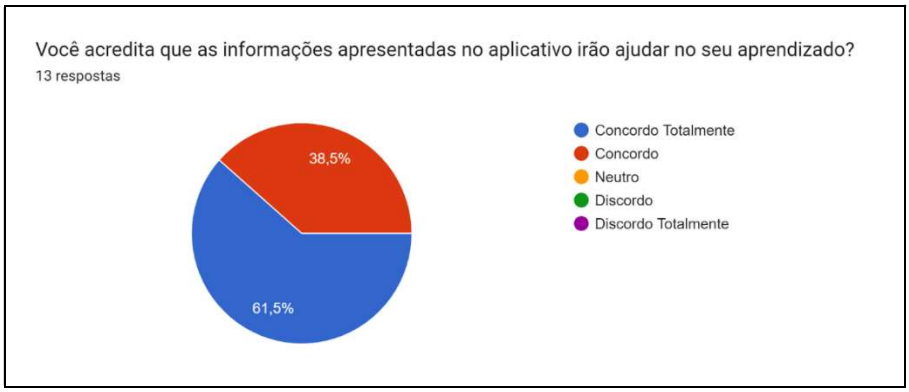


Figura 19. Formulário de avaliação do aplicativo

Quando se trata da facilidade em navegar na aplicação, constatou-se que 61,5% concordaram totalmente com essa característica, quando 38,5% concordaram com esse aspecto da pesquisa, conforme apresentado na Figura 20.

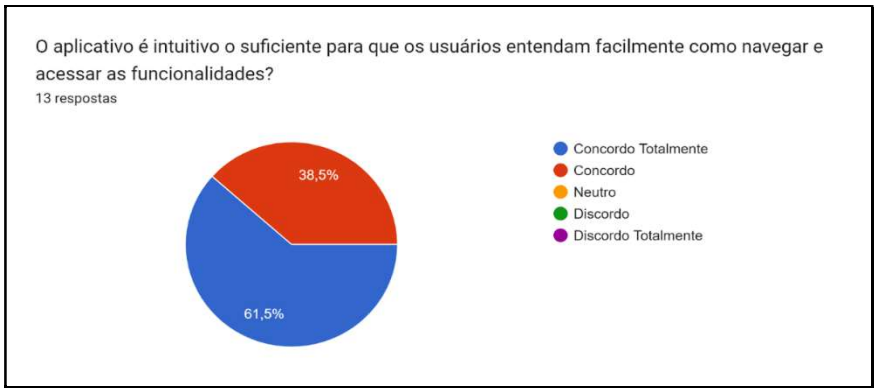


Figura 20. Formulário de avaliação do aplicativo

Conforme apresentado na Figura 21, tratando-se em tempo de execução, certificou-se que 69,2% concordaram que a aplicação possui um bom tempo de resposta, enquanto 23,1% concordaram totalmente e 7,7% mantêm posição neutra em relação à questão de pesquisa.

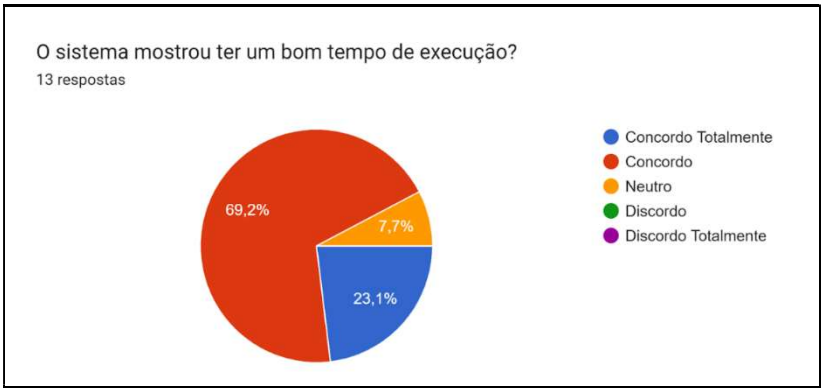


Figura 21. Formulário de avaliação do aplicativo

No que diz respeito ao aspecto de limitações ao uso da aplicação, percebe-se que 53,8% mantém uma posição neutra em questões as limitações de usabilidade, ao mesmo tempo que 38,5% discordaram sobre a questão de pesquisa e 7,7% concordaram com limitações ao uso do aplicativo, conforme apresentado na Figura 22.

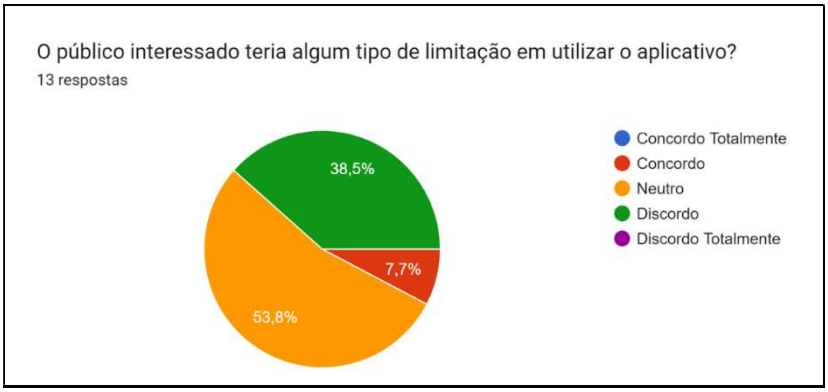


Figura 22. Formulário de avaliação do aplicativo

Conforme a Figura 23, tratando-se do interesse na utilização da aplicação fora do ambiente educacional, nota-se que 61,5% concordam com a utilização da aplicação, enquanto 38,5% concordam totalmente com a questão de pesquisa.

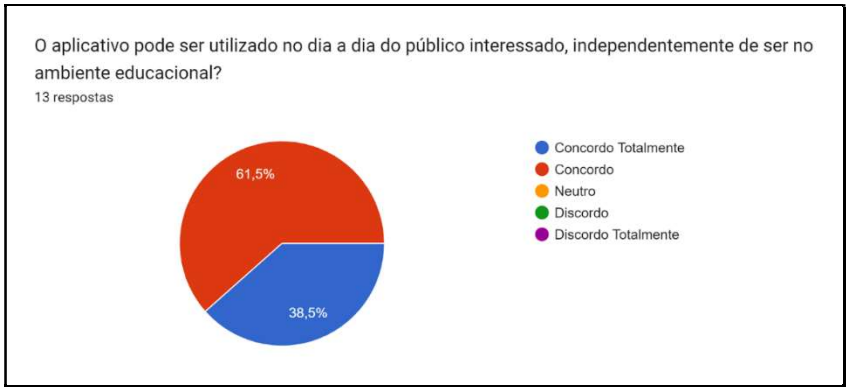


Figura 23. Formulário de avaliação do aplicativo

No contexto da aplicação como uma ferramenta de apoio ao ensino-aprendizagem, constatou-se que 84,6% dos participantes concordaram que acreditam na viabilidade da utilização da ferramenta para esse propósito e 15,4% concordaram com a questão de pesquisa, conforme demonstrada na Figura 24.

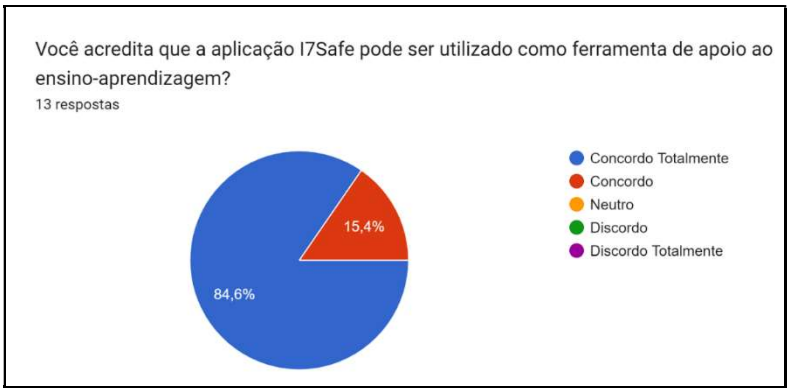


Figura 24. Formulário de avaliação do aplicativo

5. Conclusão

Neste estudo, realizou-se uma revisão bibliográfica abrangente para fundamentar a base teórica do trabalho, examinando pesquisas relacionadas que se concentram em estratégias relacionadas à importância do domínio do conhecimento em Segurança da Informação, e assim, foi desenvolvido uma proposta de uma aplicação mobile para auxiliar o aprendizado em Segurança da Informação, visando oferecer mais um recurso para que o usuário possa obter mais conhecimentos específicos sobre o tema. É importante ressaltar que os testes mais aprofundados ainda não foram realizados, mas os

testes iniciais foram feitos, afim de extrair feedbacks de usuários para que assim possam ser feitos ajustes no aplicativo.

Após a avaliação da aplicação com os usuários, foi constatado que a tecnologia implementada atendeu de maneira satisfatória às diretrizes propostas e aos requisitos do aplicativo sobre usabilidade, desempenho e relevância, tendo em vista que a aplicação continuará sofrendo alterações posteriormente, assim que realizado uma avaliação mais detalhada das suas funcionalidades e coletar mais feedbacks de usuários.

A limitação deste estudo diz respeito ao escopo da avaliação do aplicativo, que poderia ter beneficiado de um maior número de participantes. Isso permitiria uma coleta de dados mais ampla e, consequentemente, uma análise mais robusta para avaliar a verdadeira intenção dos usuários de utilizar o aplicativo ou não.

Como perspectivas de pesquisa futura, almeja-se a realização de um mapeamento mais aprofundado de determinados tópicos pertinentes à Segurança da Informação. Além disso, pretende-se investigar a viabilidade de incorporar funcionalidades de personalização que se adequem às necessidades individuais dos usuários, levando em consideração diversos níveis de conhecimento e experiência no campo da segurança da informação.

Referências

Batista, M. H. da S. (2018). **Uma abordagem para verificação de acessibilidade e usabilidade em aplicativos móveis**. Diss. Universidade de São Paulo.

Cabral, C. e Caprino, W. (2015). **Trilhas em segurança da informação: caminhos e ideias para a proteção de dados**. Brasport.

Carvalho, E. A.; Reis, T. e Alves, F. J. (2017). **Ensino de Noções Básicas de Segurança da Informação nas Escolas Brasileiras.** Anais do Workshop de Informática na Escola.

Castro, N. (2021**). Números de golpes pela internet quase triplicou em 2020, aponta ISP**.G1. Globo. Disponível em:Número de golpes pela internet quase triplicou em 2020, aponta ISP | Rio de Janeiro | G1. Acesso em: 10 de julho de 2022.

Cruz, V. S. e Pretucelli, E. E. (2017). **Tecnologias Web para o Desenvolvimento Mobile Nativo.**

Conceição, L.; Medeiros, M. e Medeiros, G. (2018). **Metodologia para Construção de Storyboard de Segurança da Informação como Guia de Engenharia Social para Capacitação de Colaboradores**. Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, v. 1, n. 1, p. 58-68.

Costa, E. C. da. (2018). **A importância da Engenharia de Requisitos no Processo de Desenvolvimento de Sistemas de Informação**. Revista Interface Tecnológica, v. 15, n. 1, p. 203-214.

Davis, F. (1989). **Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology**. MIS Quarterly, p. 319-340.

Fontes, E. L. G. (2017). **Segurança da informação**. Saraiva Educação SA.

Gomes, D. B. M. (2017). **Desenvolvimento de uma plataforma mobile com base Android**. Diss. Instituto Politecnico de Braganca (Portugal).

Guedes, G. (2018). **UML 2: Uma Abordagem Prática**. 3. ed. São Paulo: Novatec.

Guimarães, A. P. N. e Tavares, T. A. (2014). **Avaliação de Interfaces de Usuário voltada à Acessibilidade em Dispositivos Móveis: Boas práticas para experiência de usuário**. Anais Estendidos do XX Simpósio Brasileiro de Sistemas Multimídia e Web. SBC.

Hintzbergen, J., Hintzbergen, K., Smulders, A. e Baars, H. (2018). **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport.

IBGE. (2021). **Pesquisa de Tecnologia da Informação e Comunicação (TIC).**

Lyra, M. R. (2015). **Governança da segurança da informação**. Brasília: nd.

Magalhães, F. M. e Pereira, M. L. (2020). R**egulamento Geral de Proteção de Dados: Manual Prático.** 3ª Edição Revista e Ampliada. Vida Economica Editorial.

Mercês, L. S. das. e Araújo, T. M. U. de. (2023). **Técnicas para avaliação de usabilidade em aplicações de dispositivos móveis: uma revisão sistemática qualitativa da literatura.** Revista GEMInIS 14.1.

Magrani, E. (2018). **A Internet das Coisas**. 1ª. ed. rev. Rio de Janeiro: FVG Editora, p. 192.

Criação de Vantagens Competitivas: Revisão de Literatura. Revista Visão, v. 7, n. 1, p. 39-51.

Neto, L. A; Filho, S S. e Almeida, D. D. (2019**). Estudo de usabilidade entre aplicações nativas e multiplataforma no sistema Android**. Anais da X Escola Regional de Informática de Mato Grosso. SBC.

Neves, D. L. F.; Almeida, L. de; Pavani, G. C. e Sales, R. M. (2021). **A segurança da informação de encontro às conformidades da LGPD**. Revista Processando o Saber, 13, 186-198.

Nichele, A. G. e Schlemmer, E. (2014). **Aplicativos para o ensino e aprendizagem de Química**. Renote.

Pizzani, L. et al. (2012). **A arte da pesquisa bibliográfica na busca do conhecimento**. RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação, Campinas, SP, v. 10, n. 2, p. 54.

Pressman, R. e Maxim, B. (2002). **Engenharia de Software: uma abordagem profissional.** 5. ed.: AMGH.

Pressman, R. e Maxim, B. (2016**). Engenharia de Software: uma Abordagem Profissional.** [tradução: João Eduardo Nóbrega Tortello; revisão técnica: Reginaldo Arakaki, Julio Arakaki, Renato Manzan de Andrade]. 8. ed. Porto Alegre: AMGH.

Redação. (2022). **Brasil ocupa 12º lugar no ranking de vazamento de dados**. Próximo Nível. Disponível em: proximonivel.embratel.com.br/brasil-ocupa-12o-lugar-no-ranking-de-vazamento-de-dados/. Acesso em: 10 de julho de 2022.

Sabino, R. (2020). **Gestão da segurança da informação orientado a LGPD: impactos da implantação das mormas LGPD nos processos da ADM Sistemas LTDA**. Tecnologia em Gestão da Tecnologia da Informação-Unisul Virtual.

Santos, L. A. B.; Araújo, J. P. R. de; França, M. A. R. (2019). **Aprendizado de segurança da informação através de gamificação.** Universidade de Uberaba.

Silva, J. A. R. D. I. M.; Dias, Junior., J. R.; Vivaldini, L. A.; Nishiyama, L. G. P.; Silva, R. T. K. D. C.; Kamakome, R. K. e Matos, V. Z. P. D. (2016). **Engenharia social: segurança da informação.**

Silva, D. J. e Guarda, G. (2019). **Criptodata: Ensino de criptografia via computação desplugada.** Anais dos Workshops do Congresso Brasileiro de Informática na Educação.

Silva, L. O. (2022). **Testes de segurança em aplicações Android baseados na metodologia OWASP.**

Six, J. (2012). **Segurança de aplicativos android.** Novatec Editora.

Sommerville, I. (2011). **Engenharia de Software.** [tradução: Ivan Bosnic e Kalinka G. de O.Gonçalves; revisão técnica: Kechi Hirama]. 9. ed. São Paulo: Pearson Prentice Hall.

APÊNDICE A – DEMAIS DIAGRAMAS

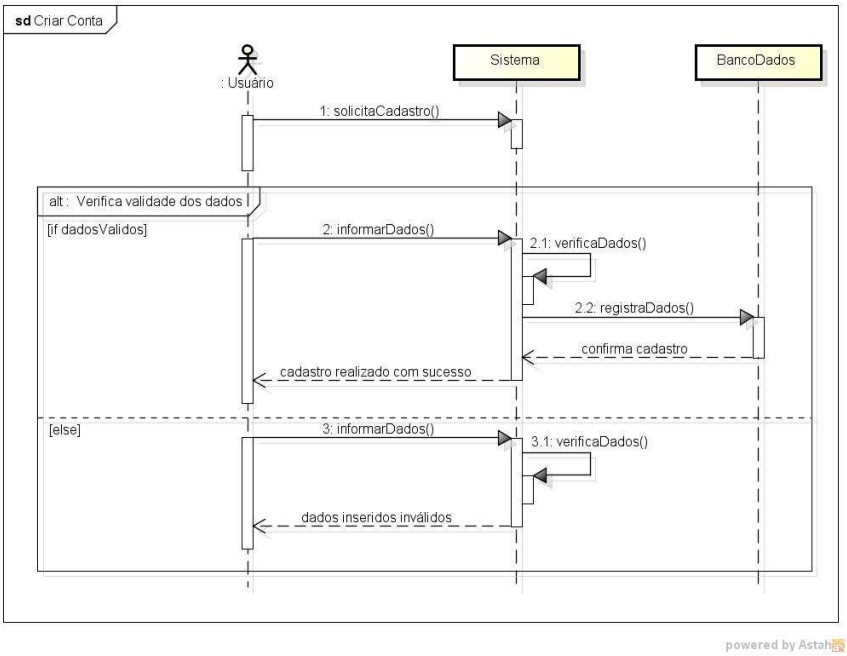


Figura 25. Diagrama de Sequência "Criar Conta"

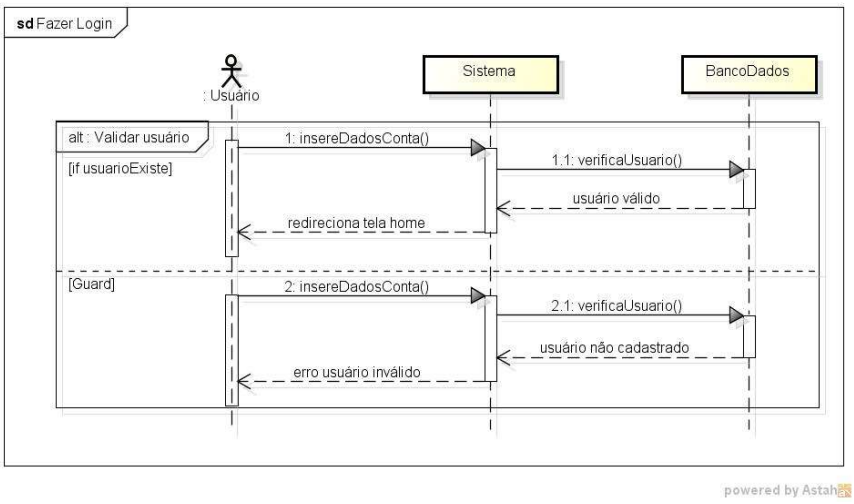


Figura 26. Diagrama de Sequência "Fazer Login"

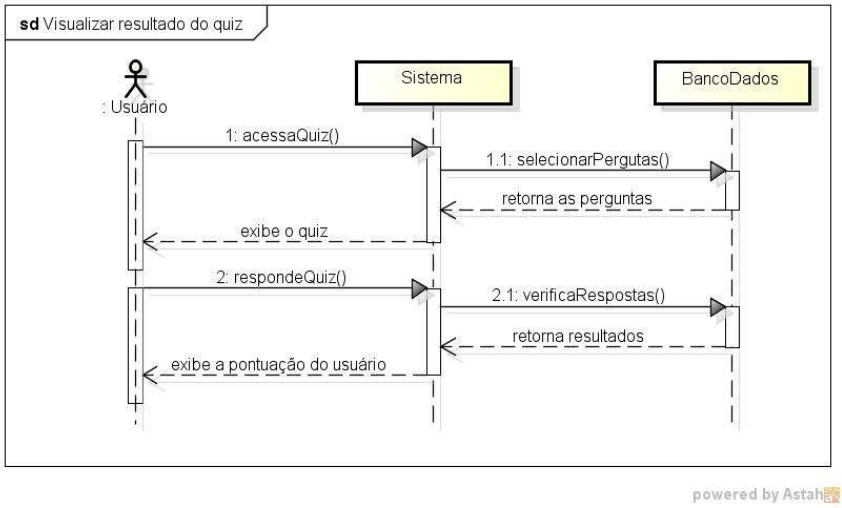


Figura 27. Diagrama de Sequência "Visualizar Resultado do Quiz"

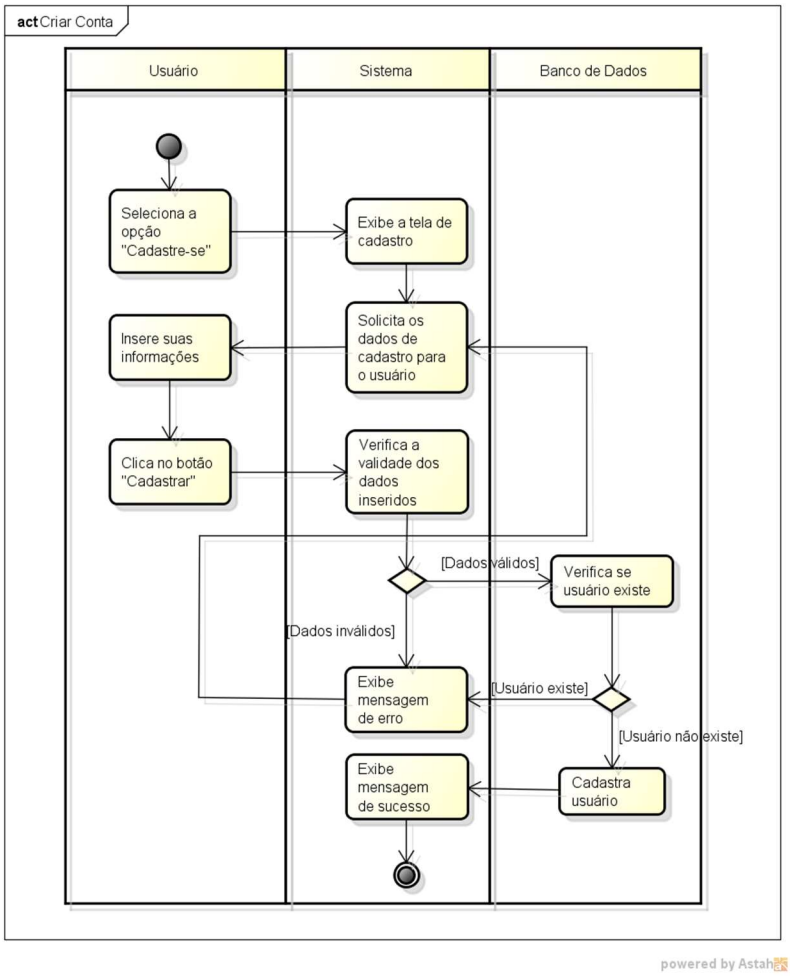


Figura 28. Diagrama de Atividade "Criar Conta"

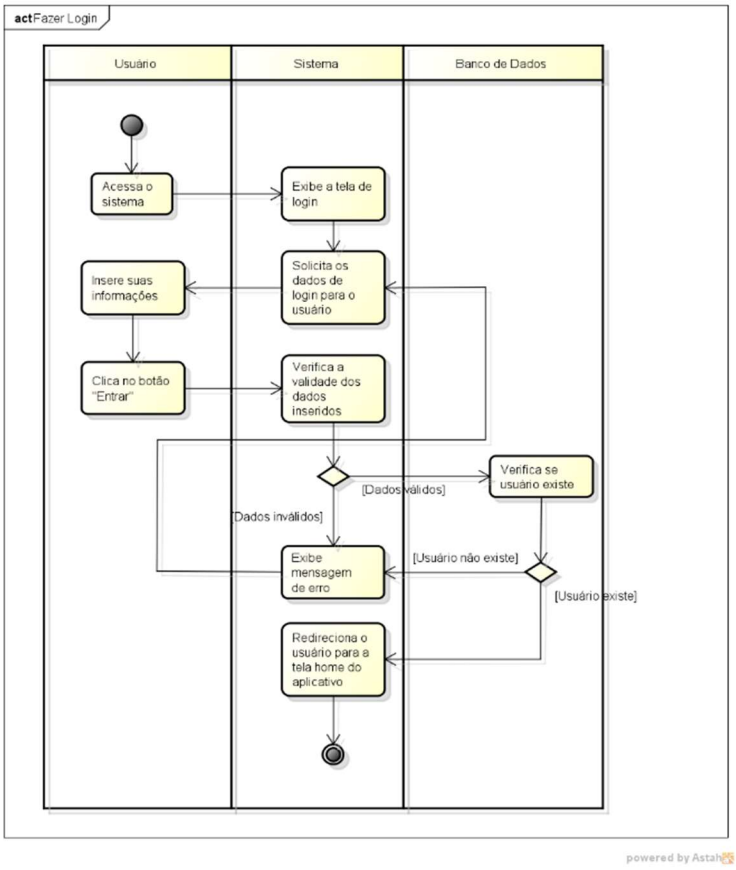


Figura 29. Diagrama de Atividade "Fazer Login"

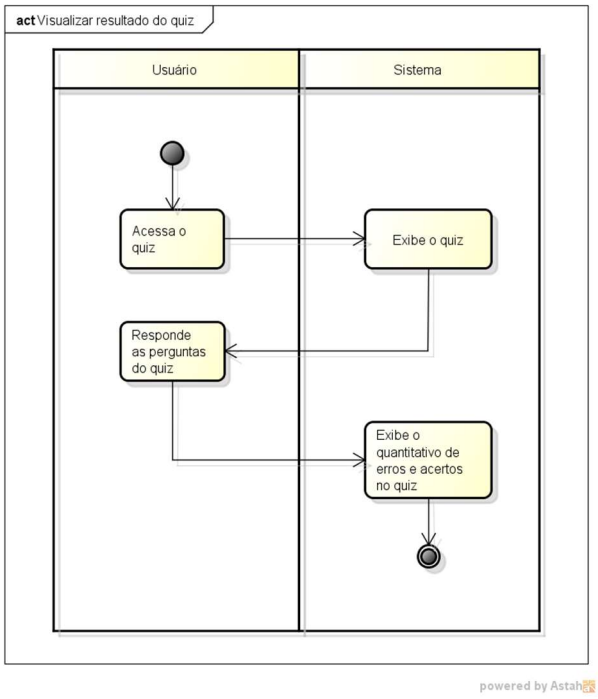


Figura 30. Diagrama de Atividade "Visualizar resultado do quiz"

APÊNDICE B – DEMAIS DOCUMENTAÇÕES DE CASO DE USO

Tabela 6. Documentação de Caso de Uso "Fazer Login"

Diagrama de Caso de Uso	**I7SAFE**
Caso de Uso Geral	Fazer login
Ator Principal	Usuário
Ator Secundário	-
Resumo	Este caso de uso descreve as etapas percorridas para o usuário fazer login no aplicativo
Pré-Condições	É necessário o usuário ter um cadastro no aplicativo
Pós-Condições	O usuário está autenticado e tem acesso ao conteúdo do aplicativo
Fluxo Principal	
Ações do Ator	**Ações do Sistema**
1 - Informa os dados para login	
	2 - Verifica se usuário possui cadastro no aplicativo
	3 - O aplicativo autentica o usuário
	4 - Redireciona o usuário para a tela home
Fluxo Alternativo	
	2.1 Exibe mensagem que o usuário não está cadastrado
2.2 Clica na opção "Cadastre-se"	
	2.3 Redireciona para a tela de cadastro
2.4 Informa os dados solicitados no cadastro	

	2.5 Verifica a validade dos dados
	2.6 Cadastra o usuário no banco de dados
	2.7 Exibe mensagem de sucesso no cadastro

Tabela 7. Documentação de Caso de Uso "Criar Conta"

Diagrama de Caso de Uso	**I7SAFE**
Caso de Uso Geral	Criar conta
Ator Principal	Usuário
Ator Secundário	-
Resumo	Este caso de uso descreve as etapas percorridas para o usuário criar uma conta no aplicativo
Pré-Condições	-
Pós-Condições	O usuário possuir uma conta no aplicativo
Fluxo Principal	
Ações do Ator	**Ações do Sistema**
1 - Acessa a tela de cadastro clicando na opção "Cadastre-se"	
	2 - Redireciona para a tela de cadastro
3 - Informa os dados solicitados no cadastro	
	4 - Verificar a validade dos dados
	5 - Cadastrar o usuário no banco de dados
	6 - Exibe mensagem de sucesso no cadastro
Fluxo alternativo	
-	-

Tabela 8. Documentação de Caso de Uso "Visualizar resultado do quiz"

Diagrama de Caso de Uso	**I7SAFE**
Caso de Uso Geral	Visualizar resultado do quiz
Ator Principal	Usuário
Ator Secundário	-
Resumo	Este caso de uso descreve as etapas percorridas para o usuário visualizar o quantitativo de erros e acertos no quiz realizado
Pré-Condições	- O usuário deve estar autenticado no sistema -O usuário deve selecionar assunto que deseja visualizar
Pós-Condições	O usuário tem acesso a tela contendo o resultado do quiz realizado
Fluxo Principal	
Ações do Ator	**Ações do Sistema**
1 - Clicar na opção "Resolver Quiz"	
	2 - O sistema redireciona o usuário para a tela do quiz
	3 - Exibe as perguntas e opções de resposta do quiz
4 - Selecionar a resposta correta e clicar em "Responder", repetir esse passo até que todas as perguntas exibidas na tela de quiz sejam respondidas	
	5 - Redirecionar o usuário para a tela contendo o quantitativo de erros e acertos no quiz
Fluxo Alternativo	
-	-