CENTRO PAULA SOUZA

ETEC PROFESSOR ADHEMAR BATISTA HEMÉRITAS

Curso Técnico em Informática para Internet

Caio Mateus Fernandes Barbosa

Cauã Makoto Tanaka Sanches

Gabriel da Silva Melo

Guilherme dos Santos Pissarro

Italo de Lima Barbosa

Wendel Binotto Júnior

SEGURANÇA CIBERNÉTICA

SÃO PAULO

2025

Caio Mateus Fernandes Barbosa

Cauã Makoto Tanaka Sanches

Gabriel da Silva Melo

Guilherme dos Santos Pissarro

Italo de Lima Barbosa

Wendel Binotto Júnior

SEGURANÇA CIBERNÉTICA

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática para Internet da Etec Prof. Adhemar Batista Heméritas, orientado pelo Prof. Alexandre Aguiar como requisito parcial para obtenção do título de Curso Técnico em Informática para Internet.

SÃO PAULO

2025

Agradecimentos

Gostaria de expressar minha sincera gratidão a todas as pessoas que contribuíram para a realização deste trabalho.

Agradeço também aos meus orientadores Felipe Martins e Alexandre Aguiar, por suas orientações, paciência e pelas valiosas contribuições que enriqueceram este trabalho. Seu conhecimento e dedicação foram fundamentais para o desenvolvimento deste projeto.

Aos meus amigos e colegas de curso, um muito obrigado pelo auxílio, apoio mútuo e pelos momentos de descontração que tornaram a trajetória acadêmica mais agradável e menos solitária.

Um agradecimento especial aos professores da Etec Adhemar Batista Heméritas, que, com suas aulas e ensinamentos, me proporcionaram uma base sólida de conhecimentos e me prepararam para enfrentar os desafios deste trabalho.

Enfim, agradeço a todos que, de alguma forma, contribuíram para o sucesso desta etapa, seja com conselhos, palavras de incentivo ou suporte emocional. A colaboração de cada um foi essencial para a conclusão deste TCC.

Muito obrigado a todos!

Epígrafe

“A criptografia funciona. Sistemas de criptografia forte, quando implementados corretamente, são uma das poucas coisas nas quais você pode realmente confiar.”

Edward Snowden

RESUMO

O trabalho tem como tema central a segurança cibernética e busca conscientizar os usuários, especialmente jovens, sobre os riscos do ambiente digital e as práticas necessárias para garantir maior proteção de dados. O objetivo principal foi o desenvolvimento do site VanguardaSeg, uma plataforma educativa que reúne informações claras e acessíveis, recursos visuais modernos e interatividade por meio de quizzes, permitindo que o aprendizado ocorra de maneira prática e envolvente. A metodologia utilizada combinou pesquisa bibliográfica, análise de artigos científicos, pesquisa de campo com usuários e aplicação de metodologias ágeis, organizadas com o Trello e o modelo 5W2H. O processo de criação envolveu a prototipação no Figma, a programação em HTML, CSS e JavaScript no Visual Studio Code e a hospedagem no GitHub. O design foi planejado para transmitir modernidade e clareza, com paleta de cores em tons de roxo e azul, além da inclusão de recursos de acessibilidade, como narração no quiz para pessoas com baixa visão. Os resultados mostraram que, embora muitos usuários demonstrem conhecimento básico de segurança digital e adotem medidas como autenticação de dois fatores, ainda prevalecem práticas inseguras, como a repetição de senhas e o uso descuidado de redes públicas. As considerações finais destacam que o projeto contribui para a formação de usuários mais conscientes e preparados, promovendo a educação digital, a autonomia no uso seguro da internet e a valorização da segurança como parte essencial da vida cotidiana.

Palavras-chave: Segurança Cibernética. Educação Digital. Site. Prototipação. Acessibilidade Digital.

ABSTRACT

The project's central theme is cybersecurity, aiming to raise awareness among users, particularly young people, about the risks of the digital environment and the practices required to ensure stronger data protection. Its main objective was the development of the VanguardaSeg website, an educational platform that integrates clear and accessible information, modern visual resources, and interactive quizzes, enabling learning in a practical and engaging way. The methodology combined bibliographic research, analysis of scientific articles, field research with users, and the application of agile practices, organized through Trello and the 5W2H model. The development process included prototyping in Figma, programming in HTML, CSS, and JavaScript with Visual Studio Code, and hosting on GitHub. The design was conceived to convey modernity and clarity, with a purple and blue color palette, complemented by accessibility features such as quiz narration for people with low vision. The results indicated that, although many users demonstrate basic knowledge of digital security and adopt measures like two-factor authentication, unsafe habits remain prevalent, such as password reuse and careless use of public networks. The final considerations emphasize that the project contributes to developing more aware and better-prepared users, fostering digital literacy, autonomy in safe internet use, and the recognition of security as an essential aspect of everyday life.

Keywords: Cybersecurity. Digital Education. Website. Prototyping. Digital Accessibility.

Lista de imagens

Lista de gráficos

Lista de abreviaturas e siglas

Lista em ordem alfabética das abreviaturas e siglas utilizadas no texto, seguidas das palavras ou expressões correspondentes grafadas por extenso.

ABNT – Associação Brasileira de Normas Técnicas

CSS – Cascading Style Sheets

HTML – Hypertext Markup Language

JS – JavaScript

LGPD – Lei Geral de Proteção de Dados

PNSC – Política Nacional de Segurança Cibernética

TCC – Trabalho de Conclusão de Curso

UI – User Interface (*Interface do Usuário*)

UX – User Experience (*Experiência do Usuário*)

VS Code – Visual Studio Code

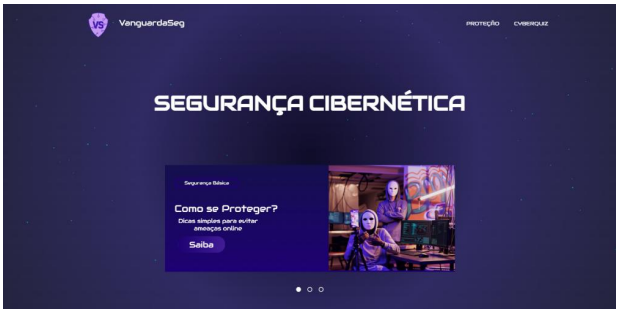
SUMÁRIO

1. INTRODUÇÃO

A segurança digital refere-se ao conjunto de práticas, tecnologias e comportamentos voltados à proteção de dados, sistemas e informações. Com o aumento da digitalização de serviços, transações financeiras, comunicações e dados pessoais, a preocupação com a segurança online tornou-se essencial. A exposição a ameaças como vazamento de dados, roubo de identidade, ataques cibernéticos e fraudes digitais afeta tanto usuários comuns quanto empresas de todos os portes, exigindo atenção constante e atualização de medidas preventivas. Diante do crescente uso da internet e da digitalização de serviços, a segurança digital tornou-se um tema de extrema relevância para a sociedade. Através deste projeto, foi possível desenvolver uma solução informativa e acessível com o objetivo de conscientizar os alunos sobre os riscos do ambiente virtual e apresentar práticas simples e eficazes de proteção.

Este trabalho tem como objetivo informar os alunos sobre a importância da segurança digital e apresentar práticas simples, porém eficazes, que podem ser aplicadas no dia a dia para aumentar a proteção online. O desenvolvimento ocorreu em etapas, utilizando diversas ferramentas tecnológicas. Primeiramente, será utilizada a plataforma Figma para criar os protótipos do site, facilitando o planejamento visual e a estruturação das informações. Em seguida, o site será construído com personalizações em HTML, CSS e JS para maior funcionalidade. Para garantir a correção gramatical e a clareza dos textos, utilizou-se o ChatGPT. A apresentação final do projeto será feita por meio da plataforma Canva, com slides explicativos e edição de vídeo com tópicos realizados no desenvolvimento do trabalho.

Imagem 1 – Página Inicial



Fonte: (Italo, 2025)

1.1 JUSTIFICATIVA

O tema segurança digital foi escolhido pelo grupo por sua crescente relevância no cotidiano das pessoas, especialmente dos jovens, que utilizam a internet como principal meio de estudo, comunicação e lazer. Trata-se de um assunto atual e essencial, que possui forte caráter educacional ao contribuir para a formação de usuários mais conscientes e preparados para lidar com os desafios do ambiente online.

Este projeto propõe o desenvolvimento de um site educativo e interativo, que sirva como apoio no processo de aprendizagem, apresentando conceitos fundamentais de segurança digital de forma simples e prática, além de orientar sobre como aplicá-los no dia a dia. A iniciativa do site busca despertar o senso crítico e incentivar o uso responsável da tecnologia, reforçando que a segurança é parte indispensável da vida digital.

A confiabilidade e a atualidade das informações serão asseguradas por meio de pesquisa bibliográfica em fontes especializadas, garantindo que o conteúdo esteja alinhado às boas práticas e aos princípios da educação digital.

1.2 ANÁLISE DE PESQUISA

O artigo escrito pela doutora em engenharia de software Flávia Brito aborda o crescimento alarmante dos incidentes de segurança cibernética no Brasil e os principais desafios para o fortalecimento da proteção digital no país. A pesquisa evidencia que o aumento de ataques, como phishing e fraudes financeiras, está relacionado à falta de investimentos governamentais, à escassez de profissionais qualificados e à ausência de uma cultura consolidada de segurança digital entre empresas e cidadãos. Embora a Lei Geral de Proteção de Dados (LGPD) represente um avanço significativo, muitas organizações ainda não estão plenamente adequadas às suas exigências, o que mantém vulnerabilidades estruturais e operacionais no sistema de defesa cibernética nacional. Ao analisar o contexto atual, o estudo evidencia um cenário de fragilidade institucional e orçamentária, com recursos insuficientes para garantir uma infraestrutura digital robusta. Some-se a isso o déficit de mais de 400 mil profissionais na área de segurança da informação, o que agrava a dependência tecnológica e compromete a resposta a incidentes de grande escala.

. A autora reforça que a mitigação desses riscos depende de ações conjuntas entre governo, setor privado e sociedade civil, sustentadas por políticas públicas integradas e programas contínuos de capacitação. Na conclusão, o texto destaca que a segurança cibernética deve ser tratada como tema estratégico para a economia e para a confiança social. A criação de um plano nacional de cibersegurança, somada a investimentos em educação digital e conscientização pública, é apontada como essencial para um futuro digital mais seguro. Sem compromisso político duradouro, o Brasil permanece vulnerável ao avanço das ameaças cibernéticas e às transformações digitais globais. O artigo está disponível na plataforma ABES[1].Também foi utilizado o uso de metodologias ágeis como parte do processo da abordagem de pesquisa. A ferramenta Trello foi usada para organização e visualização das tarefas, utilizando o método Kanban para acompanhamento do trabalho em tempo real. Igualmente, foi aplicado o modelo 5W2H para estruturar planos de ação, identificar as responsabilidades e definir estratégias de melhoria, promovendo uma abordagem fácil e interativa ao longo do estudo.

Por fim, realizou-se uma pesquisa bibliográfica com o objetivo de embasar teoricamente o estudo, reunindo conceitos e fundamentos sobre metodologias ágeis, produtividade em equipes e gestão de projetos. Foram consultados artigos científicos e materiais técnicos publicados em bases confiáveis, que serviram como referência para contextualizar os dados coletados e sustentar as análises e conclusões da pesquisa.

Para um maior embasamento dos conteúdos e informações, o grupo optou por não só usar artigos científicos e materiais técnicos, mas também ao suporte de ferramentas de inteligência artificial, como o ChatGPT e o Gemini, para geração de imagens e na correção ortográfica.

1.4.1 Cronograma

Um cronograma é uma ferramenta utilizada para organização, planejamento e acompanhamento das tarefas em andamento. Ele apresenta as atividades que precisam ser realizadas, as datas de andamento de cada tarefa com seus respectivos meses. No contexto do projeto, o cronograma foi utilizado para demarcar cada fase do projeto, garantindo que cada parte, como documentação, prototipação, entre outras, sejam realizadas a tempo.

Foi elaborado um cronograma com o objetivo de organizar as tarefas de maneira clara, garantindo que todas as etapas do projeto fossem realizadas de forma planejada e colaborativa. A realização do cronograma permitiu acompanhar o desenvolvimento do projeto.

Quadro 1 – Cronograma realizado para divisão das tarefas 1º semestre

ATIVIDADES	JAN	FEV	MAR	ABR	MAI	JUN
Organização		**X**	**X**			
Documentação			**X**	**X**	**X**	**X**
Prototipação site			**X**	**X**	**X**	**X**
Trello				**X**	**X**	
Pesquisa de campo				**X**	**X**	
Apresentação				**X**		
Desenvolvimento do site					**X**	**X**

Fonte: (Cauã, 2025)

Quadro 2 – Cronograma realizado para divisão das tarefas 2º semestre

ATIVIDADES	JUL	AGO	SET	OUT	NOV	DEZ
Documentação		X	X	X	X	
Trello		X	X	X	X	
Apresentação		X				X
Criação de conteúdo		X	X	X	X	
Desenvolvimento do site		X	X	X	X	
Vídeo		X	X	X	X	

Fonte: (Cauã, 2025)

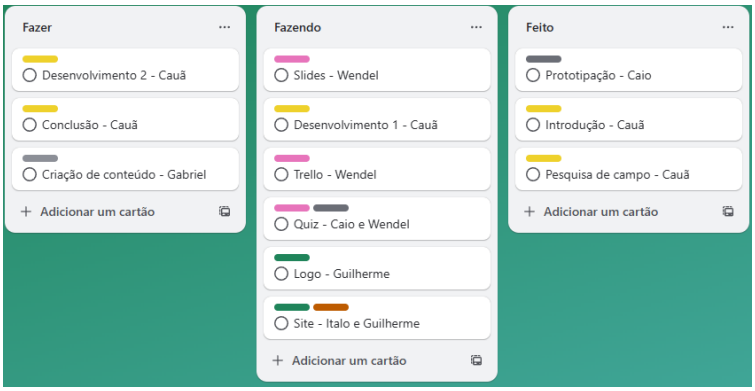
1.4.2 Metodologia Ágil

A metodologia ágil é um conjunto de ações e princípios voltados para tornar o desenvolvimento de projetos, especialmente de softwares, mais dinâmico, flexível e colaborativo. Ela surgiu como uma resposta aos modelos tradicionais, considerados lentos, que dificultavam a adaptação às mudanças ao longo do processo. Criada no início dos anos 2000, essa metodologia tem como propósito principal a entrega de valor de forma contínua. Dessa forma, a metodologia ágil foi feita para aumentar a eficiência, reduzir riscos e garantir que o fim do projeto esteja alinhado com as expectativas dos usuários.

A metodologia ágil foi adotada pela equipe devido à sua capacidade de proporcionar flexibilidade, colaboração e entrega contínua de valor. Ela possibilita que a equipe se adapte rapidamente a mudanças nos requisitos e nas prioridades, atendendo de forma eficaz para alunos. Ao organizar o trabalho em ciclos curtos (sprints), facilita o acompanhamento do progresso, a detecção precoce de problemas e a entrega constante de resultados. Além disso, a metodologia ágil favorece uma comunicação constante entre os membros da equipe, assegurando o alinhamento e permitindo ajustes durante o processo. Esses benefícios contribuem para um aumento na produtividade, maior satisfação dos usuários e melhores resultados ao longo do tempo.

Na metodologia ágil, utilizamos o Trello como ferramenta de gerenciamento de projetos e tarefas. Baseado no método Kanban, o Trello permite organizar e visualizar o andamento das atividades por meio de quadros visuais. Essa ferramenta foi essencial para a estruturação e o acompanhamento das tarefas do nosso trabalho.

Imagem 2 – Uso do Trello



Fonte: (Wendel, 2025)

O método Kanban utilizado no Trello é uma metodologia visual para o gerenciamento de tarefas em projetos, permitindo uma organização clara das etapas por meio de quadros, listas e cartões. Essa abordagem facilitou a visualização do andamento do projeto, possibilitando identificar o que já foi concluído, o que está em progresso e o que ainda precisa ser desenvolvido.

A ferramenta 5W2H é uma metodologia de planejamento amplamente aplicada em ambientes organizacionais para estruturar ações, processos e projetos. Seu nome deriva das iniciais das perguntas fundamentais em inglês: What, Why, Where, When, Who, How e How much, correspondentes a "O que", "Por que", "Onde", "Quando", "Quem", "Como" e "Quanto".

O principal objetivo do 5W2H é garantir clareza e objetividade no planejamento, definindo etapas, prazos, responsáveis e recursos necessários para execução. Ao responder às sete perguntas, torna-se possível detalhar ações, motivação, local de aplicação, responsáveis, prazos, métodos e custos envolvidos.

De aplicação simples e flexível, o 5W2H pode ser adaptado a diversos tipos de projeto, auxiliando decisões, planejamento estratégico e melhoria contínua. Também contribui para uma comunicação mais clara entre equipes e facilita o acompanhamento de resultados.

Quadro 3 – 5W2H

O quê	**Por quê?**	**Onde**	**Quando**	**Quem**	**Como**	**Quanto custou**
O que será feito?	Por que Será feito	Onde será feito	Quando será feito	Por quem será feito?	Como será feito	Quanto custará?
Site sobre a segurança digital	Para informar os alunos e finalizar o trabalho de conclusão de curso	Etec/Casa	Fevereiro de 2025 a dezembro de 2025	6 integrantes	Através de plataformas tecnológicas	Gratuito

Fonte: (Cauã, 2025)

O uso do 5W2H foi essencial para que o grupo pudesse organizar o planejamento da pesquisa de forma clara, pois a metodologia permite definir exatamente o que será feito. Essa organização torna o desenvolvimento mais eficiente e coerente do projeto.

2. DESENVOLVIMENTO

O referencial teórico do trabalho reúne conceitos, inspirações e pesquisas que fundamentam o projeto “VanguardaSeg”, voltado à conscientização sobre segurança cibernética. Ele aborda desde a construção da identidade visual, com a logo representando proteção e tecnologia, até referências de design retiradas de sites renomados, que orientaram a criação de protótipos modernos e interativos. Também apresenta a importância da experiência e da interface do usuário, destacando a necessidade de tornar o aprendizado acessível, dinâmico e envolvente para jovens. Além disso, inclui dados de pesquisa de campo que revelam o nível de conhecimento e vulnerabilidades dos usuários em relação à segurança digital, reforçando a relevância de práticas educativas. Dessa forma, o referencial teórico integra bases científicas, referências visuais e análises práticas, servindo como alicerce para o desenvolvimento do site e para a eficácia da proposta de conscientização.

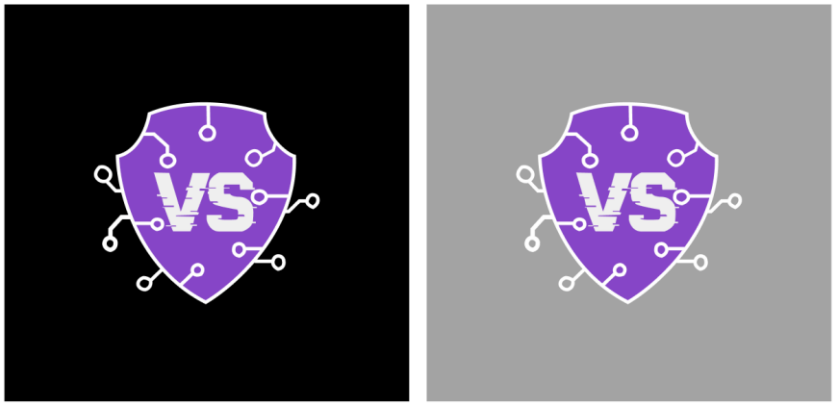
2.1 Referencial Teórico

O grupo recorreu a artigos científicos, materiais técnicos e ao suporte de ferramentas de inteligência artificial, a fim de garantir fundamentação teórica consistente e alinhada às práticas atuais.

2.1.1 Logotipo

O desenvolvimento da logo do projeto VanguardaSeg foi pensado para transmitir, de forma visual e objetiva, a essência do tema central: a segurança cibernética. O escudo foi escolhido como elemento principal por simbolizar proteção e defesa, reforçando a ideia de segurança digital. No interior do escudo, a sigla “VS” remete diretamente ao nome do projeto, destacando sua identidade. Além disso, foram adicionados circuitos eletrônicos conectados ao redor do escudo, representando a tecnologia e o ambiente virtual no qual a segurança é aplicada, as letras “bugadas” que aparecem na logo tem como objetivo simbolizar a vulnerabilidade e instabilidade do digital, remetendo a possíveis falhas em sistemas. A escolha da cor roxa buscou transmitir inovação, modernidade e criatividade, enquanto os detalhes em branco garantiram contraste e legibilidade em diferentes contextos visuais. Dessa forma, a logo cumpre um papel não apenas estético, mas também comunicativo, reforçando a proposta do projeto e aproximando o público de sua identidade visual.

Imagem 3 – Logotipo



Fonte: (Guilherme, 2025)

A seção do relatório foi desenvolvida com base em referências visuais e interativas de sites notáveis no cenário tecnológico e de design. As inspirações foram extraídas de três fontes principais, cada uma contribuindo com elementos distintos para a experiência final.

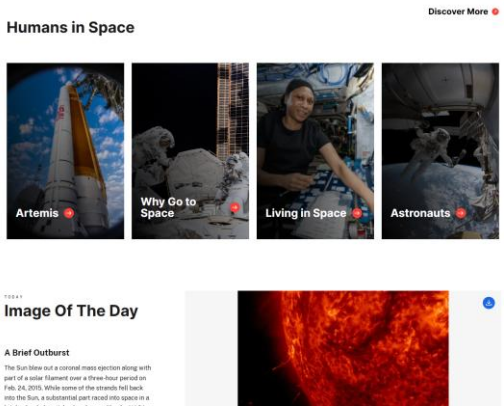
Chirpley: Foi utilizada como inspiração, em especial as três imagens sobrepostas e o tópico ao lado que introduz o conteúdo da página.

Imagem 4 – Inspirações 1, 2025

Fonte: (Chirpley, 2025)

NASA: Por fim, a NASA forneceu a base para uma abordagem mais minimalista e focada em dados. O design do site da agência espacial inspira-se na clareza e na organização para apresentar informações complexas de maneira elegante e intuitiva, priorizando a legibilidade e a estrutura limpa. Essa referência reforçou a importância de reduzir elementos visuais excessivos, destacando apenas o que é essencial para o usuário. Além disso, o uso equilibrado de cores, espaço e tipografia serviu como modelo para construir uma interface objetiva, funcional e visualmente moderna.

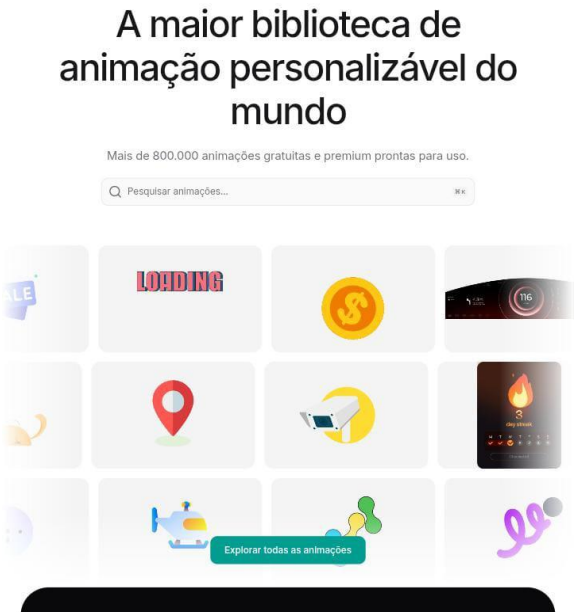
Imagem 5 – Inspirações 2, 2025



Fonte: (Nasa, 2025)

LottieFiles: O site LottieFiles apresenta uma estrutura em que o tema é introduzido por um título e, em seguida, exposto em um carrossel. Essa estrutura foi utilizada como inspiração na página “Cuidado com os golpes”.

Imagem 6 – Inspirações 3, 2025



Fonte: (LottieFilies, 2025)

2.1.3 Protótipos

O grupo deu início à parte técnica com a criação de seis protótipos, cada um com características diferentes, após uma análise do grupo e dos orientadores, foi escolhido o protótipo um, pois ele se destacou por atender melhor as propostas do projeto, e com um design inovador e tecnológico.

2.1.3.1 Protótipo 1

Este protótipo, desenvolvido por Caio Mateus, teve como objetivo principal melhorar a interatividade do usuário, utilizando informações objetivas e concisas para evitar textos longos e cansativos. Além disso, o aluno buscou criar um protótipo moderno, incorporando efeitos visuais e cores que transmitissem a ideia de tecnologia.

Imagem 7 – Protótipo 1.1

Fonte: (Caio, 2025)

Imagem 8 – Protótipo 1.2

Fonte: (Caio, 2025)

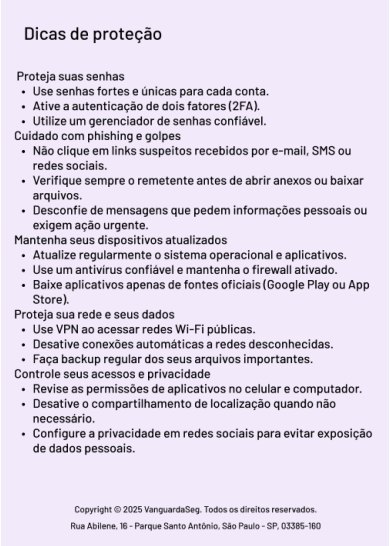
2.1.3.2 Protótipo 2

O protótipo de Cauã Makoto Tanaka Sanches apresenta informações sobre segurança cibernética de forma simples e direta, com dicas práticas para auxiliar os usuários na proteção contra malwares. Para tornar o aprendizado mais envolvente, será disponibilizado um quiz para que os usuários possam testar seus conhecimentos. No rodapé, estarão disponíveis informações de contato para aqueles que desejarem saber mais ou tirar dúvidas. A paleta de cores escolhida combina tons de roxo e azul, transmitindo criatividade, confiança e segurança. Além disso, branco, cinza e preto serão utilizados para adicionar detalhes e realçar o design.

Imagem 9 – Protótipo 2.1

Fonte: (Cauã, 2025)

Imagem 10 – Protótipo 2.2

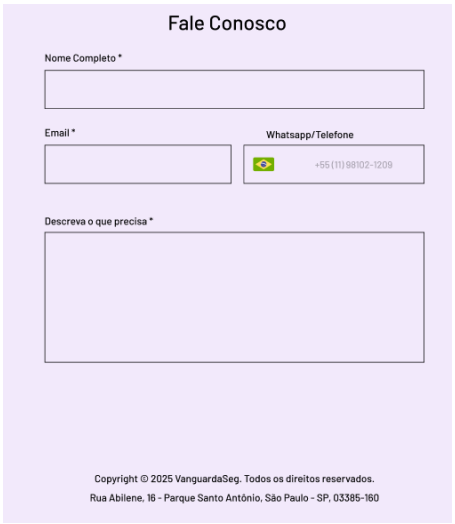


Fonte: (Cauã, 2025)

Imagem 11 – Protótipo 2.3

Fonte: (Cauã, 2025)

Imagem 12 – Protótipo 2.4



Fonte: (Cauã, 2025)

2.1.3.3 Protótipo 3

O protótipo desenvolvido por Guilherme Pissarro tem como objetivo apresentar um visual agradável e simples. Além disso, trata-se de um site intuitivo e informativo sobre segurança cibernética, que explica conceitos relacionados ao tema, oferece dicas de proteção e disponibiliza um quiz para que os usuários possam testar seus conhecimentos.

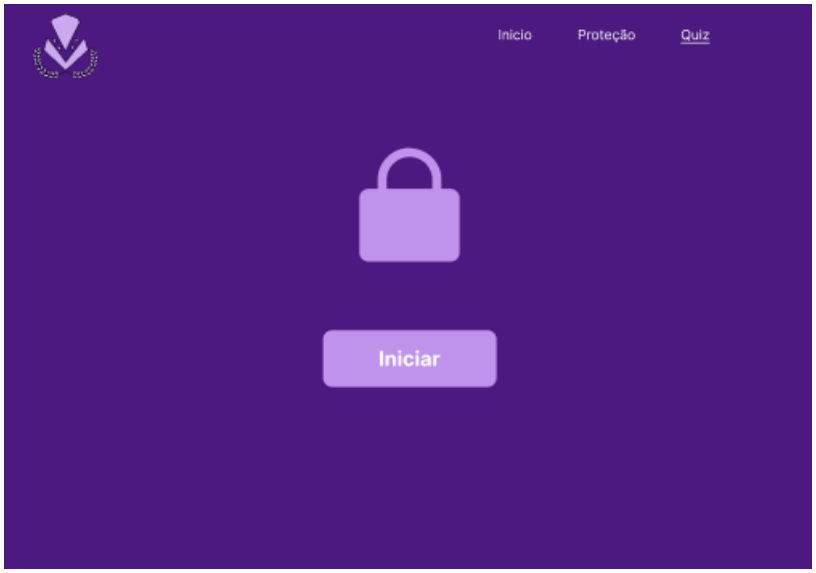
Imagem 13 – Protótipo 3.1

Fonte: (Guilherme, 2025)

Imagem 14 – Protótipo 3.2

Fonte: (Guilherme, 2025)

Imagem 15 – Protótipo 3.3



Fonte: (Guilherme, 2025)

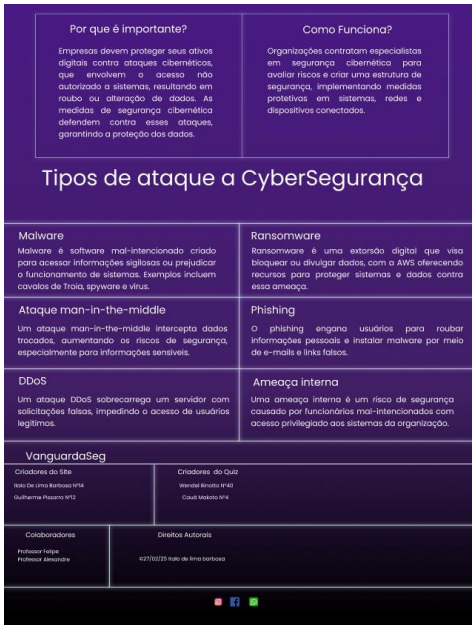
2.1.3.4 Protótipo 4

O protótipo desenvolvido por Italo de Lima Barbosa tem como principal objetivo proporcionar facilidade de uso aos usuários, por meio de um site com interface intuitiva e informativa. Além disso, a escolha das cores contribui para um design moderno e atrativo, reforçando a ideia inicial do projeto.

Imagem 16 – Protótipo 4.1

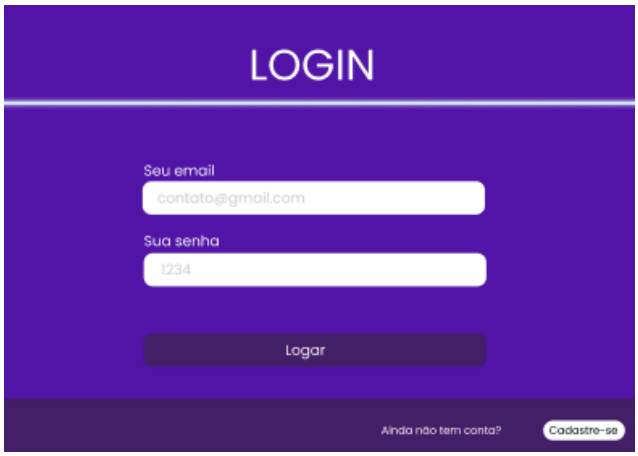
Fonte: (Italo, 2025)

Imagem 17 – Protótipo 4.2



Fonte: (Italo, 2025)

Imagem 18 – Protótipo 4.3



Fonte: (Italo, 2025)

Imagem 19 – Protótipo 4.4

Fonte: (Italo, 2025)

2.1.3.5 Protótipo 5

O protótipo desenvolvido por Wendel tem como principal objetivo facilitar o uso pelos usuários. Além disso, trata-se de um site intuitivo e informativo sobre segurança cibernética, que explica conceitos relacionados ao tema, oferece dicas de proteção e disponibiliza um quiz para que os usuários possam testar seus conhecimentos.

Imagem 20 – Protótipo 5.1

Fonte: (Wendel, 2025)

Imagem 21 – Protótipo 5.2

Fonte: (Wendel, 2025)

2.1.4 Criação de Conteúdo

Ao decorrer do desenvolvimento do projeto, o grupo buscou pesquisar diversas fontes para fundamentar e estruturar os conteúdos do site. Foram utilizados artigos científicos, como Segurança na Internet como parte da competência digital do cidadão[3], escrito por Raquel Barragán Sánchez, professora da Universidad de Sevilla, e a pesquisa Segurança cibernética no Brasil: desafios e necessidades urgentes de ação[1], desenvolvida pela doutora em engenharia de software Flávia Brito. Também foram utilizados alguns livros, como Segurança Digital na Educação[2], desenvolvido pela secretária-geral da Comissão de Direito Digital e Novas Tecnologias da OAB, Maria Zulmira de Brito, além de pesquisas em inteligência artificial e pesquisas bibliográficas, o que forneceu ao grupo uma base atualizada e sólida sobre o tema.

2.1.5 Criação de imagens

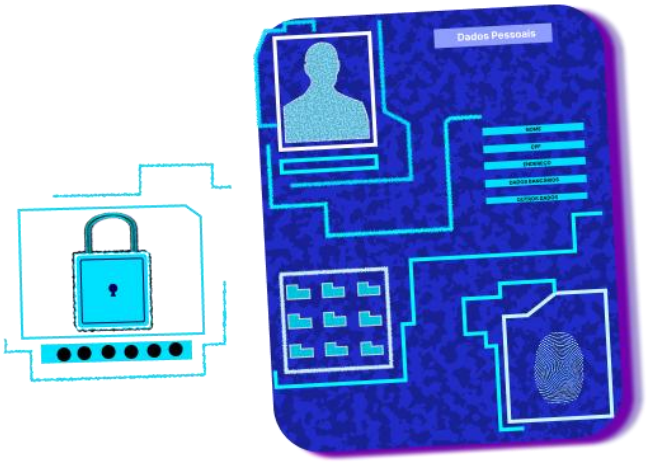
Para o desenvolvimento do projeto, o grupo utilizou a ferramenta digital Figma e o uso de algumas inteligências artificiais, como ChatGPT e o Gemini, para a criação e vetorização de imagens. O uso de inteligência artificial foi utilizado como inspirações para as criações de imagens coerentes com o tema do projeto. Já o Figma foi empregado no processo de vetorização.

Imagem 22 – Site 1

Fonte: (Gabriel, 2025)

Uma das imagens criadas foi uma ilustração da figura de um hacker, utilizando elementos como o capuz e a tela, que arremetem diretamente ao universo da segurança digital. Também foi pensado na escolha da paleta de cores, para reforçar a sensação de tecnologia e alerta, evidenciando os riscos do mundo digital.

Imagem 23 – Site 2



Fonte: (Gabriel, 2025)

A imagem feita retrata uma tabela digital com elementos como ícones e pastas interligadas por circuitos, simbolizando a estrutura de segurança e proteção de dados. O cadeado central representa a confidencialidade das informações, enquanto a paleta em tons de azul e roxo neon sugere confiança, tecnologia e vigilância constante. O design futurista dialoga com a identidade visual do projeto, reforçando a ideia de defesa cibernética frente a possíveis ameaças virtuais.

Imagem 24 – Site 3

Fonte: (Gabriel, 2025)

A imagem desenvolvida retrata uma figura encapuzada em um ambiente digital, cercada por circuitos e efeitos em neon, simbolizando a segurança cibernética. O personagem central representa o anonimato e a presença no meio tecnológico. Já para a paleta de cores foi optado por tons de roxo, azul e rosa neon, pois são cores que transmitem inovação, modernidade e um cenário futurista, alinhado com a ideia central do tema.

Imagem 25 – Site 4

Fonte: (Gemini.ia, 2025)

A imagem retrata uma figura encapuzada, com o rosto substituído por uma interface digital composta por ícones de cadeados, que sugerem diretamente a ideia de segurança e proteção de dados. Além do cenário tecnológico em tons de azul e rosa neon.

Imagem 26 – Site 5

Fonte: (Gemini.ia, 2025)

A imagem apresenta um envelope vermelho como foco principal, envolvido por elementos digitais como cadeados, textos e linhas gráficas, representando a proteção e a confidencialidade das informações. O fundo composto por uma superfície de circuitos em tons de azul e roxo neon reforçando a ideia de ambiente tecnológico e segurança digital.

Imagem 27 – Site 6

Fonte: (Gemini.ia, 2025)

A imagem representa um smartphone estilizado ao centro, de onde partem setas em múltiplas direções, simbolizando a disseminação rápida de informações. O ícone de corrente quebrada no centro do dispositivo representa o compartilhamento, enquanto os elementos gráficos externos, sugerem dúvidas e desinformação. E a utilização de azul e rosa neon para reforçar o ambiente digital e tecnológico.

Imagem 28 – Site 7

Fonte: (Gemini.ia, 2025)

A imagem apresenta um smartphone em destaque com um link exibido na tela e uma lupa sobreposta, acompanhada de um símbolo de “X”, indicando risco ou erro. As setas ao redor do dispositivo simbolizam a circulação rápida de conteúdos na internet, enquanto os códigos e linhas digitais reforçam o contexto tecnológico. A paleta em tons de azul e rosa neon sugere ambiente virtual e modernidade. A composição visual faz um alerta para o perigo de clicar em links falsos, transmitindo a ideia de ameaça, fraude e vulnerabilidade do usuário diante de páginas maliciosas e golpes online.

Imagem 29 – Site 8

Fonte: (Gemini.ia, 2025)

A imagem apresenta um smartphone em destaque exibindo uma interface de transferência, simbolizando operações financeiras digitais. Ao lado, o ícone de uma ampulheta com asas representa a ideia de pressa e urgência excessiva, enquanto as setas em volta do aparelho indicam velocidade e fluxo acelerado de informações. A paleta em tons de azul e rosa neon reforça o ambiente tecnológico e moderno. A composição sugere o alerta sobre transferências realizadas de forma impulsiva, destacando o risco de golpes e a necessidade de atenção antes de concluir operações financeiras no meio digital.

Imagem 30 – Site 9

Fonte: (Gemini.ia, 2025)

A imagem apresenta um smartphone exibindo um QR Code em destaque, sobreposto por um grande símbolo de “X”, indicando erro ou perigo. Ao redor, ícones de cadeado e ponto de interrogação reforçam a ideia de dúvida, risco e falta de segurança. As setas apontando para o código sugerem escaneamento imediato, enquanto o fundo com circuitos digitais enfatiza o contexto tecnológico. A paleta em tons de azul e rosa neon transmite modernidade e ambiente virtual. A composição visual tem como foco alertar o risco de escanear QR Codes sem verificação prévia, evidenciando a possibilidade de golpes e acesso a links maliciosos.

Imagem 31 – Site 10

Fonte: (Gemini.ia, 2025)

A imagem retrata um caixa eletrônico (ATM) em destaque, com uma pessoa utilizando o teclado enquanto outra mão se aproxima, sugerindo interferência externa. O triângulo com ponto de exclamação ao lado indica alerta e situação de risco iminente. As setas direcionadas reforçam a ideia de abordagem indevida, enquanto o fundo com circuitos digitais contextualiza o ambiente tecnológico. A paleta em tons de azul e rosa neon mantém a identidade visual futurista. A composição sugere o perigo de aceitar ajuda de desconhecidos em caixas eletrônicos, alertando para possíveis golpes e fraudes financeiras.

Imagem 32 – Site 11

Fonte: (Gemini.ia, 2025)

Uma das imagens criadas apresenta um smartphone em destaque, exibindo um alerta de erro associado ao uso de senhas repetidas, elemento central para representar práticas inseguras no ambiente digital. A ilustração utiliza uma paleta de cores vibrantes em neon, que remete ao universo tecnológico e reforça a sensação de atenção e risco. A mão segurando o dispositivo e os ícones de aviso contribuem para enfatizar a importância da adoção de boas práticas de segurança, evidenciando como escolhas simples, como a repetição de senhas, podem comprometer a proteção dos dados pessoais.

Imagem 33 – Site 12

Fonte: (Gemini.ia, 2025)

A imagem retrata um smartphone em destaque sendo invadido por uma figura encapuzada, simbolizando a ação de um hacker e a violação de segurança digital. Elementos como códigos, ícones de erro, cadeados e circuitos elétricos ao redor do aparelho reforçam a ideia de sistema comprometido e acesso não autorizado. As rachaduras e efeitos visuais no interior do celular sugerem danos e quebra de proteção. A paleta em tons de azul e rosa neon mantém o ambiente tecnológico e futurista. A composição visual indica o risco de ataques cibernéticos em dispositivos móveis, alertando para a vulnerabilidade dos dados pessoais diante de invasões virtuais.

Imagem 34 – Site 13

Fonte: (Gemini.ia, 2025)

Uma das imagens criadas apresenta ícones de perfis e interações digitais, evidenciando a prática de aceitar seguidores desconhecidos nas redes sociais. A composição utiliza linhas e símbolos neon que remetem ao ambiente tecnológico, reforçando a atmosfera de conectividade e alerta. Elementos como o ícone de aviso e o cadeado danificado destacam os riscos associados a essa ação, demonstrando como a exposição a estranhos pode comprometer a privacidade e a segurança online. A escolha da paleta de cores vibrantes acentua a sensação de atenção e cuidado necessária ao lidar com interações virtuais.

Imagem 35 – Site 14

Fonte: (Gemini.ia, 2025)

Uma das imagens criadas apresenta um balão de fala em destaque, marcado por um símbolo de alerta, representando o ato de postar opiniões polêmicas nas redes sociais. A composição utiliza ícones como expressões de desagrado, setas e um cadeado, que reforçam a sensação de tensão, repercussão e possível exposição decorrentes desse comportamento. A estética em neon, com cores vibrantes, remete ao universo tecnológico e enfatiza o clima de atenção e risco, ilustrando como conteúdos provocativos podem gerar conflitos, reações negativas e vulnerabilidades no ambiente digital.

Imagem 36 – Site 15

Fonte: (Gemini.ia, 2025)

A imagem retrata um smartphone em destaque com uma interface de contatos, sobre a qual uma mão mecânica realiza a seleção de informações, simbolizando a extração indevida de dados. Ao redor do aparelho, ícones de cadeados e elementos gráficos conectados por circuitos indicam o contexto de segurança digital e invasão. A presença do título “Roubo de contato” reforça a ideia de furto de informações pessoais, como números e dados sensíveis. A paleta em tons de azul e rosa neon sugere um ambiente tecnológico e futurista. A composição visual faz um alerta para o risco do roubo de contatos, evidenciando a vulnerabilidade do usuário diante de acessos não autorizados e práticas maliciosas no meio digital.

Imagem 37 – Site 16

Fonte: (Gemini.ia, 2025)

A imagem apresenta um smartphone em destaque exibindo um valor elevado em vermelho, acompanhado de um ícone de carteira digital e um cadeado quebrado, simbolizando uma situação de dano financeiro grave. Os efeitos de partículas e circuitos ao redor do aparelho reforçam a ideia de colapso do sistema e falha na proteção dos dados. A interface luminosa em tons de azul e rosa neon sugere um ambiente tecnológico associado a transações digitais comprometidas. A composição visual comunica a noção de perda definitiva e impacto financeiro permanente, alertando para as consequências severas de golpes e falhas de segurança no meio virtual.

Imagem 38 – Site 17

Fonte: (Gemini.ia, 2025)

A imagem mostra um smartphone exibindo uma tela de pagamento no valor de R$ 1.500,00, com o botão “PAGAR” em evidência, indicando a finalização de uma transação financeira. Ao lado, a figura encapuzada com expressão sorridente representa o golpista, reforçando a ideia de fraude e manipulação do usuário. Ícones de alerta, cifrão e cadeados ao redor do aparelho evidenciam o contexto de risco e comprometimento da segurança. A paleta em tons neon de azul e rosa mantém o aspecto tecnológico e digital. A composição sugere um cenário de transferência indevida de valores, alertando para o envio de dinheiro a criminosos por meio de golpes virtuais e engenharia social.

Imagem 39 – Site 18

Fonte: (Gemini.ia, 2025)

A imagem apresenta um smartphone exibindo a mensagem “Saque inválido”, acompanhada de um ícone de erro, indicando a não autorização da operação. A interface mostra valores e opções de retirada, enquanto uma mão aponta para o botão de ação, sugerindo a tentativa do usuário em realizar a transação. Ícones de alerta, cadeados e setas ao redor do aparelho reforçam o contexto de risco, bloqueio e falha no processo financeiro. A paleta em tons de azul e rosa neon mantém o ambiente tecnológico e digital. A composição visual sugere a impossibilidade de conclusão do saque, alertando para problemas de segurança ou inconsistências na operação bancária.

Imagem 40 – Site 19

Fonte: (Gemini.ia, 2025)

A imagem mostra a representação de um dispositivo móvel conectado a uma rede Wi-Fi pública aberta, evidenciada por símbolos de sinal e cadeados que remetem à exposição e à ausência de proteção adequada. Ao lado, uma figura encapuzada simboliza a ação de cibercriminosos, com linhas digitais fluindo em direção ao aparelho, sugerindo interceptação de dados e possíveis tentativas de acesso indevido a informações sensíveis. Elementos como ícones de moedas, senhas e arquivos reforçam a ideia de vulnerabilidade e risco durante o uso de conexões não seguras. A estética em tons neon de azul e rosa cria um ambiente tecnológico e alerta para as ameaças virtuais associadas a essa prática, destacando a importância de cautela ao utilizar redes abertas.

Imagem 41 – Site 20

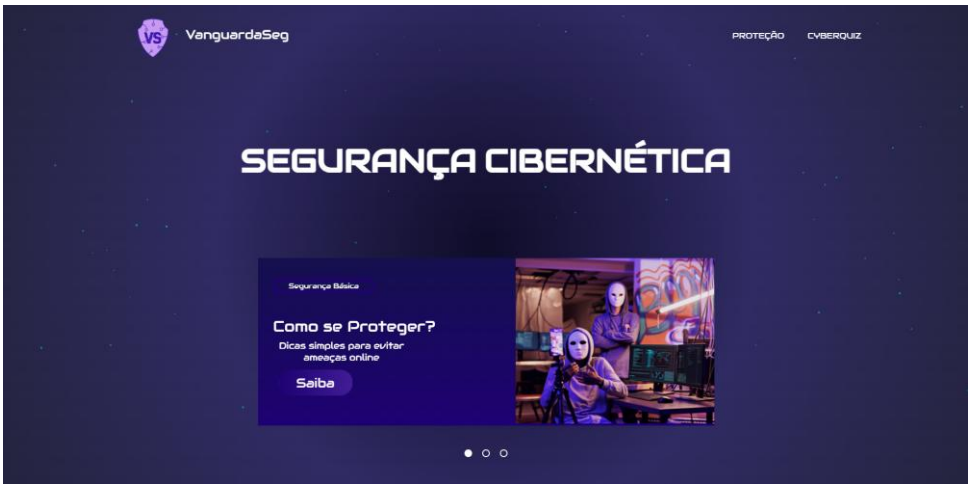
Fonte: (Gemini.ia, 2025)

A imagem retrata um smartphone em destaque exibindo indicadores negativos relacionados à reputação digital, como o ícone de “descurtida” e símbolos de alerta, sugerindo danos à credibilidade do usuário em ambientes virtuais. Elementos gráficos como cadeados, circuitos e notificações dispersas ao redor do aparelho reforçam a ideia de vulnerabilidade e consequências decorrentes de comportamentos ou incidentes que afetam a imagem pessoal ou profissional. A composição em tons neon de azul e rosa, associada ao cenário tecnológico, enfatiza o impacto que ações online podem gerar na percepção pública, transmitindo a noção de um ambiente crítico em que a reputação pode ser facilmente comprometida.

2.1.6 Interface de usuário

O desenvolvimento da interface de usuário do projeto foi orientado pela necessidade de tornar o conteúdo sobre segurança cibernética claro, atrativo e de fácil acesso ao público-alvo. Para isso, a organização visual foi planejada de forma a estabelecer hierarquia entre os elementos, destacando títulos, menus e informações principais em áreas estratégicas da tela. A escolha da paleta de cores, baseada em tons de roxo e azul, teve como objetivo transmitir modernidade, confiança e tecnologia, ao mesmo tempo em que o contraste com branco e outros tons vibrantes garantiu legibilidade e destaque aos elementos centrais. Além disso, foram utilizados ícones e ilustrações digitais que remetem a cadeados, escudos e navegadores, reforçando a temática da proteção de dados e facilitando a associação entre o conteúdo e sua aplicação prática. A navegação foi pensada de forma intuitiva, com menus posicionados na parte superior que permitem acesso rápido às principais seções, como “Home”, “Proteção” e “CyberQuiz”. Essa estrutura simples contribui para que o usuário encontre facilmente o que procura, sem sobrecarga de informações. Outro ponto essencial foi a adoção de elementos interativos, como passos explicativos e quizzes, que tornam o aprendizado mais dinâmico e envolvente. Por fim, a interface foi projetada para ser responsiva, garantindo que a experiência se mantenha consistente e acessível em diferentes dispositivos, desde computadores até smartphones. Dessa forma, a interface de usuário cumpre o papel de apoiar a proposta pedagógica do projeto, transformando a navegação em um processo educativo eficiente e agradável.

Imagem 42 – Interface



Fonte: (Italo, 2025)

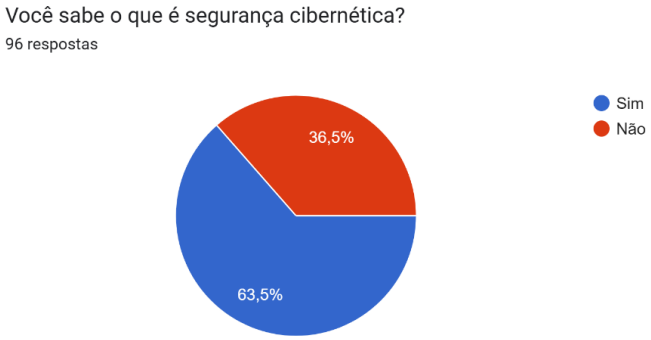
2.1.7 Experiência de usuário

O site do VanguardaSeg foi planejado para ser interativo, dinâmico e educativo, de modo a atender às necessidades de um público jovem, na faixa etária de 15 a 23 anos, que busca compreender e aplicar conceitos fundamentais de segurança cibernética em seu cotidiano. O site foi desenvolvido com foco em praticidade, permitindo que a navegação seja intuitiva e que os conteúdos sejam apresentados de forma clara, objetiva e atrativa. Para alcançar esse propósito, foram utilizados recursos visuais modernos, quizzes interativos e materiais informativos elaborados a partir de referências confiáveis, garantindo que o aprendizado ocorra de maneira envolvente e consistente. Além disso, a proposta pedagógica do projeto valoriza a autonomia do usuário, incentivando-o a explorar os conteúdos no próprio ritmo e a aplicar os conhecimentos adquiridos em situações reais do ambiente digital. Dessa forma, o VanguardaSeg não apenas dissemina informações sobre segurança cibernética, mas também contribui para a formação de usuários mais conscientes, críticos e preparados para enfrentar os riscos presentes no espaço virtual, reforçando o caráter social e educativo da iniciativa.

2.1.8 Pesquisa de Campo

Foi realizada uma pesquisa quantitativa contendo 12 perguntas relacionadas à área de segurança da informação, na qual foram obtidas 96 respostas que auxiliaram no desenvolvimento do projeto.

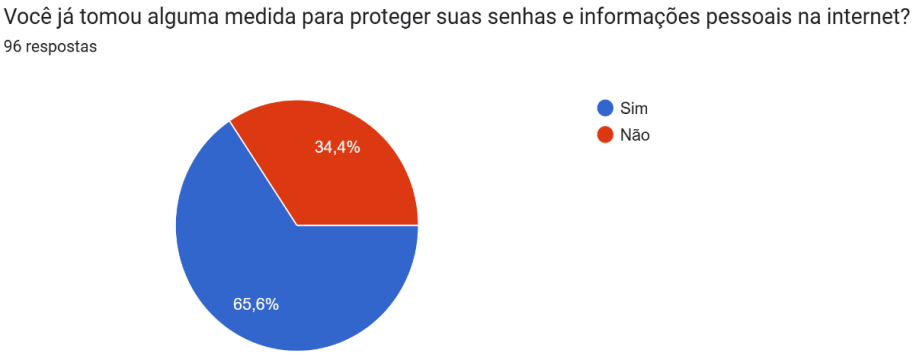
Gráfico 1 – Você sabe o que é segurança cibernética



Fonte: (Cauã, 2025)

Com base nas respostas obtidas, 63,5% dos participantes afirmaram saber o que é segurança cibernética, enquanto 36,5% disseram não conhecer o tema. Esse resultado demonstra que a maioria já possui alguma noção sobre o assunto, o que pode facilitar a adoção de práticas seguras no ambiente digital. No entanto, a parcela significativa que declarou não ter conhecimento evidencia a necessidade de ampliar ações de conscientização e educação digital, de modo a reduzir a vulnerabilidade frente a ameaças virtuais.

Gráfico 2 – Já tomou alguma medida para proteger senhas



Fonte: (Cauã, 2025)

De acordo com os dados levantados, 65,6% dos participantes afirmaram já ter tomado alguma medida para proteger suas senhas e informações pessoais na internet, enquanto 34,4% declararam não adotar esse tipo de precaução.

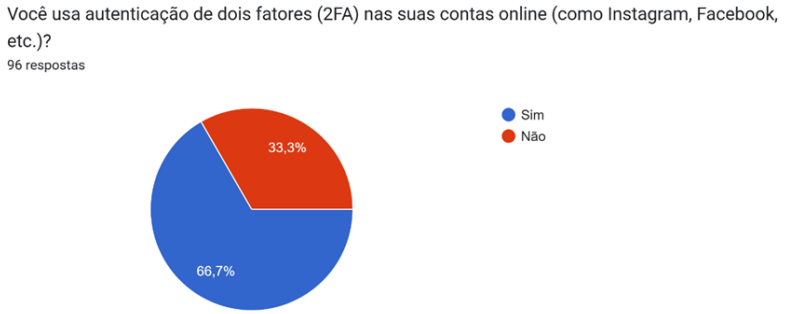
Esse resultado indica que a maioria dos usuários demonstra preocupação com a proteção de seus dados, adotando práticas de segurança digital. Porém, a quantidade significativa de pessoas que ainda não se protege ressalta a necessidade de ampliar a conscientização sobre os riscos online e incentivar hábitos mais seguros no uso da internet.

Gráfico 3 – Já aconteceu problemas como roubo de conta ou vírus

Fonte: (Cauã, 2025)

A partir das respostas analisadas, 58,3% dos participantes afirmaram já ter enfrentado algum problema na internet, como roubo de conta ou infecção por vírus, enquanto 41,7% disseram nunca ter passado por esse tipo de situação. Esse resultado mostra que uma parcela significativa dos usuários já foi vítima de ameaças digitais, o que evidencia a vulnerabilidade existente no ambiente online. Por outro lado, a porcentagem de pessoas que nunca enfrentou tais problemas indica que, embora os riscos sejam comuns, ainda há indivíduos que conseguem se manter protegidos, seja por meio de boas práticas ou por não terem sido diretamente expostos.

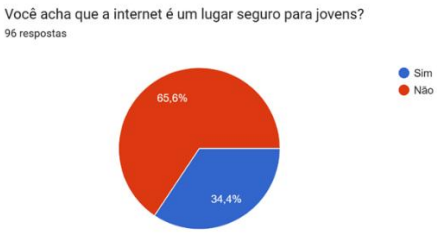
Gráfico 4 – Autenticação de dois fatores



Fonte: (Cauã, 2025)

A partir das respostas analisadas, 66,7% dos participantes afirmaram utilizar autenticação de dois fatores (2FA) em suas contas online, enquanto 33,3% disseram não adotar esse recurso de segurança. Esse resultado evidencia que a maioria dos usuários está atenta à importância de reforçar a proteção de suas contas, reduzindo o risco de invasões e roubos de informações. No entanto, ainda há uma parcela considerável que não utiliza essa medida, o que pode indicar falta de conhecimento sobre o recurso ou subestimação dos riscos, deixando suas contas mais vulneráveis a ataques cibernéticos.

Gráfico 5 – Acha que a internet é um lugar seguro



Fonte: (Cauã, 2025)

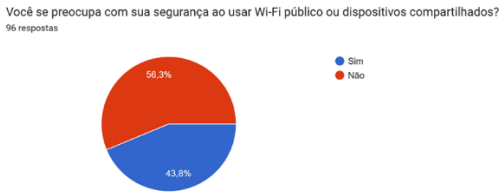
De acordo com os dados obtidos, 34,4% dos participantes consideram a internet um lugar seguro para jovens, enquanto 65,6% acreditam que não seja. Esse resultado evidencia uma percepção predominante de insegurança em relação ao ambiente digital, possivelmente associada a riscos como golpes, exposição a conteúdos impróprios ou falta de orientação adequada. Ainda assim, a parcela que acredita na segurança pode refletir confiança em ferramentas de proteção, monitoramento ou no uso responsável da internet, ressaltando a importância de promover conscientização e práticas seguras no espaço online.

Gráfico 6 – Já recebeu mensagem suspeita

Fonte: (Cauã, 2025)

Com base nas respostas obtidas, 62,5% dos participantes afirmaram já ter recebido algum e-mail ou mensagem suspeita solicitando informações pessoais ou financeiras, enquanto 37,5% disseram não ter passado por essa experiência. Esse resultado revela que a maioria já foi exposta a tentativas de golpes virtuais, como phishing, que representam uma ameaça significativa à segurança digital. Por outro lado, a parcela que nunca recebeu esse tipo de contato mostra que nem todos os usuários foram diretamente atingidos, mas ainda assim é fundamental que estejam atentos para identificar e evitar possíveis fraudes online.

Gráfico 7 – Se preocupa com segurança ao usar WI-FI público



Fonte: (Cauã, 2025)

Segundo os resultados apresentados, 43,8% dos participantes disseram se preocupar com sua segurança ao utilizar Wi-Fi público ou dispositivos compartilhados, enquanto 56,3% afirmaram não ter essa preocupação. Esse cenário indica que a maioria dos usuários ainda não percebe os riscos associados a essas práticas, como a possibilidade de roubo de dados ou invasões. Por outro lado, a parcela que demonstra cautela evidencia uma maior conscientização sobre os perigos do ambiente digital, destacando a necessidade de reforçar a educação em segurança cibernética para todos os usuários.

Gráfico 8 – Verificar se um site é seguro antes de inserir dados pessoais

Fonte: (Cauã, 2025)

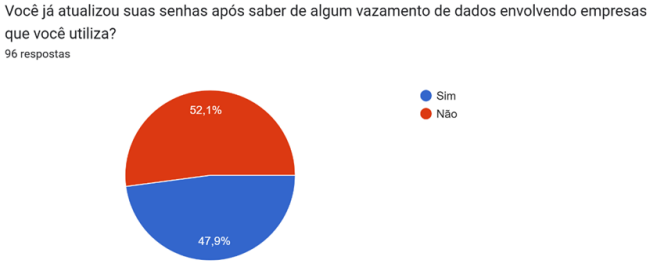
Os dados coletados mostram que 68,8% dos participantes costumam verificar se um site é seguro antes de inserir dados pessoais ou realizar compras online, enquanto 31,3% afirmaram não adotar esse cuidado. Esse resultado evidencia que a maioria dos usuários já tem consciência da importância de checar a confiabilidade das páginas acessadas, reduzindo os riscos de fraudes e golpes virtuais. No entanto, ainda existe uma parcela significativa que não realiza essa verificação, o que pode deixá-los mais vulneráveis a ataques cibernéticos e perdas financeiras.

Gráfico 9 – Utilizar senhas diferentes para cada uma de suas contas

Fonte: (Cauã, 2025)

De acordo com o levantamento, 40,6% dos participantes afirmaram utilizar senhas diferentes para cada uma de suas contas online, enquanto 59,4% disseram não adotar essa prática. Esse resultado mostra que a maioria ainda mantém o hábito de repetir senhas, o que aumenta os riscos de invasões em caso de vazamento de dados. Por outro lado, a parcela que utiliza combinações distintas demonstra maior preocupação com a segurança digital, reforçando a importância de boas práticas para proteger informações pessoais na internet.

Gráfico 10 – Atualizar senhas após um vazamento de dados



Fonte: (Cauã, 2025)

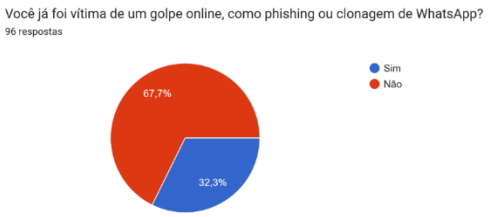
Os resultados apontam que 47,9% dos participantes já atualizaram suas senhas após tomar conhecimento de algum vazamento de dados envolvendo empresas que utilizam, enquanto 52,1% afirmaram não ter feito essa alteração. Esse cenário mostra que pouco menos da metade dos usuários adota medidas reativas de proteção diante de incidentes de segurança, o que reduz o risco de invasões e fraudes. Contudo, a maioria ainda não realiza essa prática, o que pode indicar falta de conscientização sobre a gravidade de vazamentos ou uma subestimação dos riscos relacionados à exposição de informações pessoais.

Gráfico 11 – Realização de backup

Fonte: (Cauã, 2025)

A pesquisa revela que 60,4% dos participantes realizam backup regular de seus dados importantes, como fotos e documentos, enquanto 39,6% afirmaram não adotar essa prática. Esse resultado indica que a maioria dos usuários já reconhece a importância de manter cópias de segurança para evitar perdas em caso de falhas, ataques cibernéticos ou exclusões acidentais. No entanto, a parcela que não realiza backups ainda representa um grupo vulnerável, evidenciando a necessidade de maior conscientização sobre a relevância dessa medida para a proteção das informações pessoais.

Gráfico 12 – Vítimas de clonagem



Fonte: (Cauã, 2025)

Com base nas respostas, 32,3% dos participantes afirmaram já ter sido vítimas de algum golpe online, como phishing ou clonagem de WhatsApp, enquanto 67,7% disseram não ter passado por esse tipo de situação. Esse dado revela que uma parcela considerável já sofreu diretamente com ataques virtuais, evidenciando os riscos frequentes presentes na internet. Por outro lado, a maioria que não enfrentou golpes até o momento reforça que, embora exista exposição, medidas de prevenção e conscientização podem reduzir a probabilidade de ser alvo desses crimes digitais.

A partir da análise das pesquisas, o grupo percebeu que, embora a maioria dos participantes demonstre certo conhecimento sobre segurança cibernética e adote algumas práticas de proteção, como a autenticação de dois fatores e a verificação da segurança de sites, ainda existem comportamentos que revelam vulnerabilidades significativas, como o uso de senhas repetidas e a falta de cuidado ao utilizar redes Wi-Fi públicas. Além disso, muitos já enfrentaram problemas relacionados a golpes virtuais e não consideram a internet um ambiente seguro para jovens, o que reforça a importância de ampliar a conscientização digital.

2.2 Referencial Técnico

O grupo realizou o site utilizando HTML, CSS e JS, com o objetivo de estruturar, estilizar e tornar interativa as páginas e conteúdos do site Vanguarda-Seg. o HTML foi empregado para estruturar o site, enquanto o CSS permitiu aplicar a identidade visual que foi desenvolvida no protótipo, por meio de cores, fontes, espaçamentos e elementos gráficos que reforçam a ideia do tema, já o JS foi importante para adicionar dinamismo, criando interações, animações e funcionalidades, como o quiz educativo.

Imagem 43 – Homepage 1

Fonte: (Cauã, 2025)

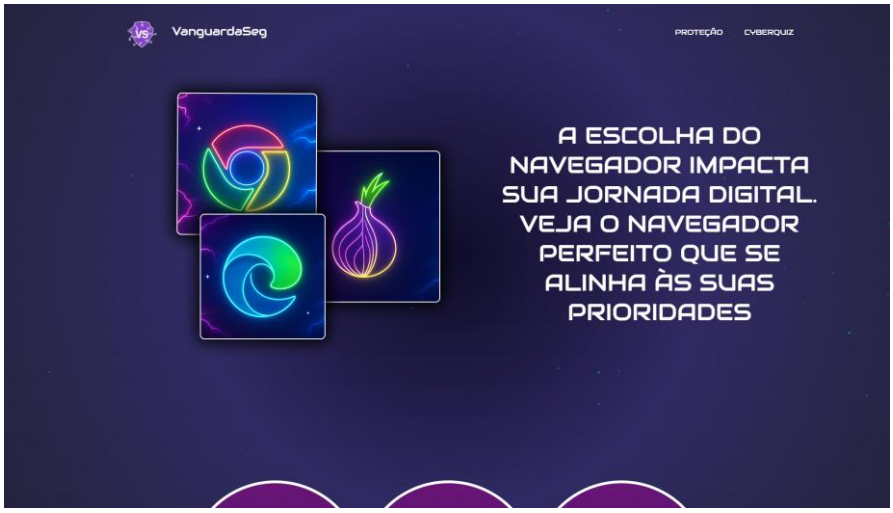
Imagem 44 – Homepage 2

Fonte: (Italo, 2025)

Imagem 45 – Homepage 3

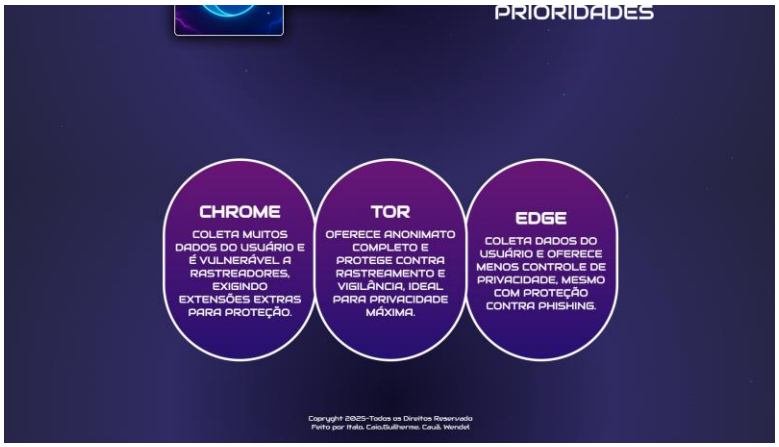
Fonte: (Italo, 2025)

Imagem 46 – Saiba mais 1



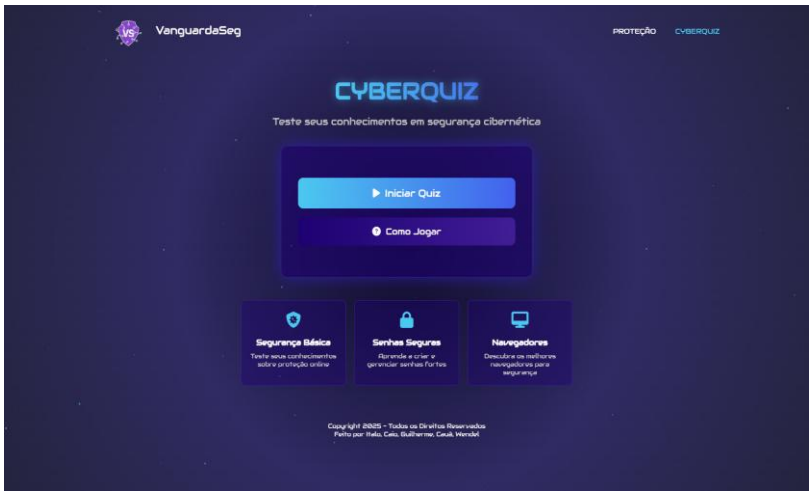
Fonte: (Italo, 2025)

Imagem 47 – Saiba mais 2



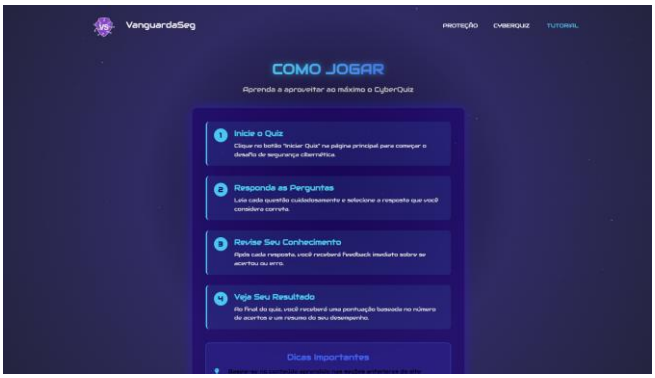
Fonte: (Italo, 2025)

Imagem 48 – Cyberquiz



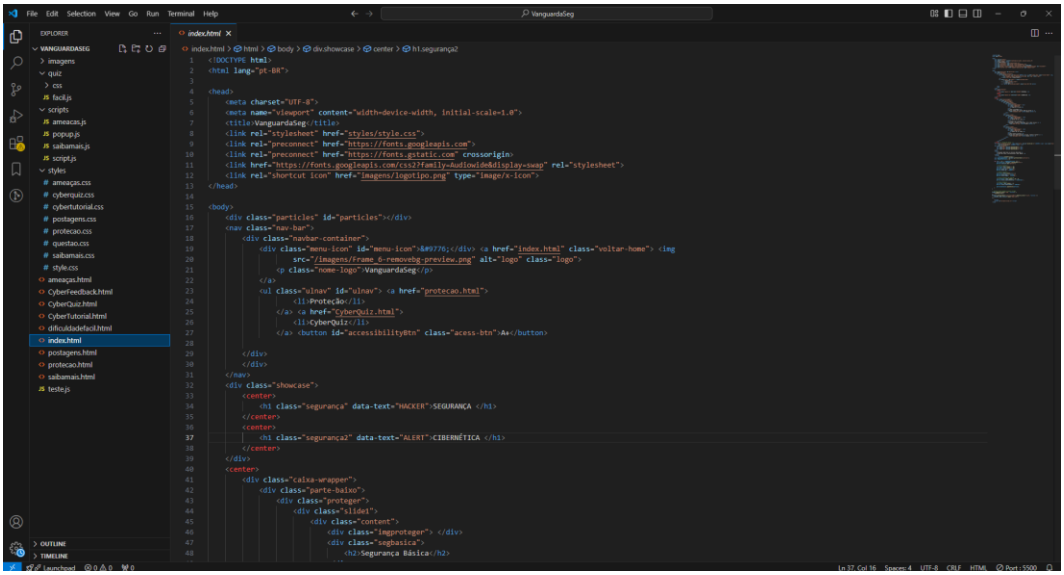
Fonte: (Italo, 2025)

Imagem 49 – Como jogar



Fonte: (Italo, 2025)

Imagem 50 – Códigos do site



Fonte: (Italo, 2025)

2.2.1 Ferramentas utilizadas

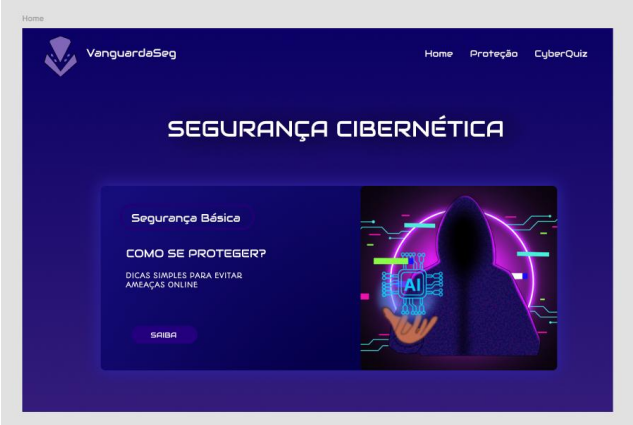
Durante o desenvolvimento deste trabalho de conclusão de curso, foram utilizadas duas ferramentas principais: Figma e VSCode. Cada uma desempenhou um papel fundamental em diferentes etapas do projeto, contribuindo para a organização, visualização e implementação da solução proposta.

2.2.2 Programação Front–End

O grupo deu início à fase de prototipação no Figma, criando os layouts e a identidade visual do site, definindo cores, ícones, elementos gráficos e a disposição das informações. Após a validação dos modelos, iniciou-se a programação front-end, utilizando HTML para estruturar o conteúdo, CSS para aplicar estilos visuais e JS para adicionar interatividade.

Figma – O Figma foi a ferramenta escolhida para a prototipagem da interface do usuário (UI). Como plataforma de design baseada na nuvem, permite criar protótipos navegáveis e simular a experiência do usuário antes da implementação. Nele foram desenvolvidos os layouts das telas, definindo o posicionamento de botões e demais elementos da interface. Essa visualização antecipada facilitou ajustes e validações com orientadores, além de servir como referência visual para o desenvolvimento do código.

Imagem 51 – Figma Prototipagem 1



Fonte: (Caio, 2025)

Imagem 52 – Figma Prototipagem 2

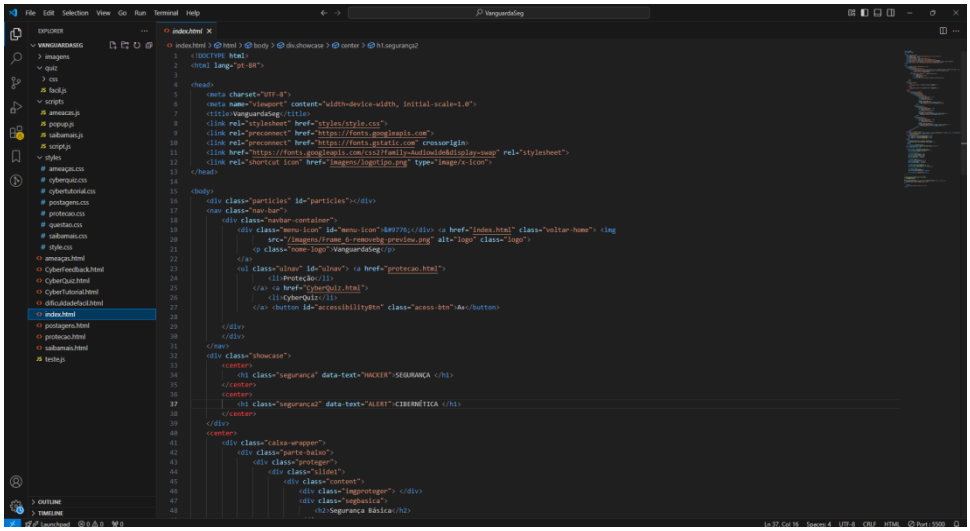
Fonte: (Caio, 2025)

Imagem 53 – Figma Prototipagem 3

Fonte: (Caio, 2025)

HTML: Utilizado para estruturar o conteúdo das páginas, definindo elementos como títulos, parágrafos, botões, formulários, imagens, entre outros.

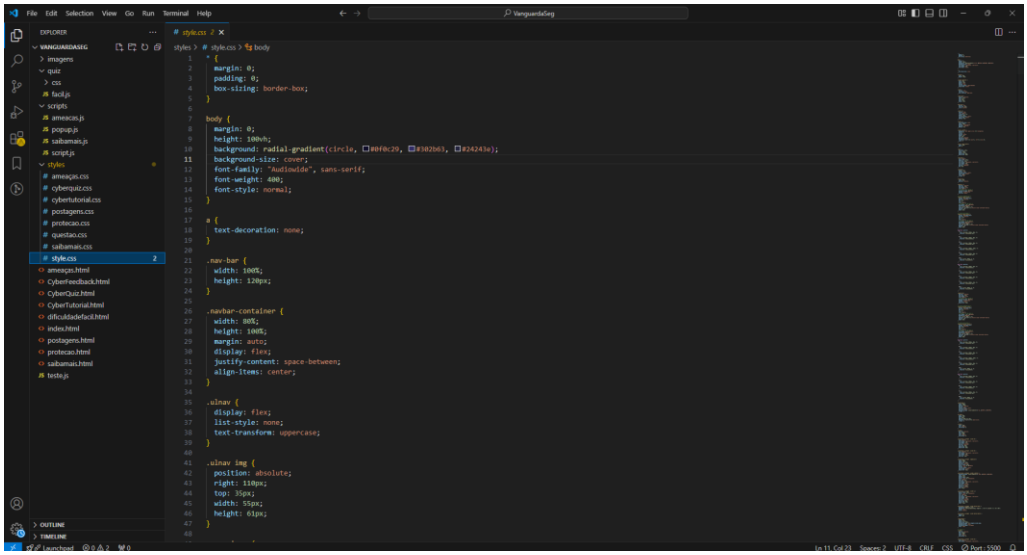
Imagem 54 – HTML Código



Fonte: (Caio, 2025)

CSS: Responsável pela estilização da aplicação, definindo cores, tamanhos, fontes, espaçamentos, alinhamentos e animações, de modo a tornar a interface mais atraente e alinhada com o protótipo criado no Figma.

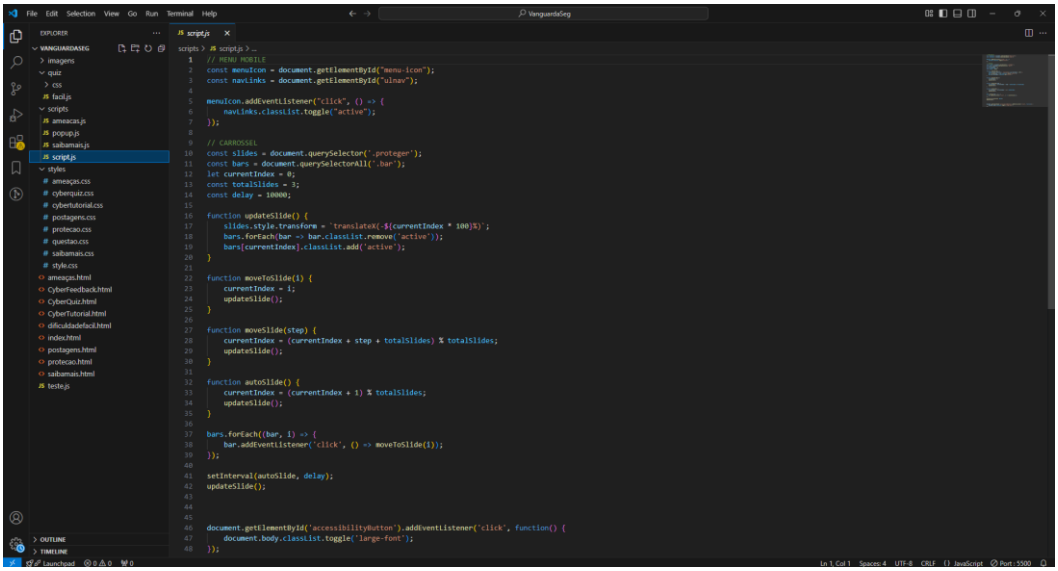
Imagem 55 – CSS Código



Fonte: (Caio, 2025)

JS: Utilizado para tornar as páginas interativas e dinâmicas, permitindo a manipulação de elementos HTML, criação de animações, tratamento de eventos como cliques e teclas pressionadas.

Imagem 56 – JS Código



Fonte: (Italo, 2025)

VSCode – Para a etapa de desenvolvimento, foi utilizado um editor de código-fonte que é amplamente adotado por desenvolvedores devido à sua leveza, extensibilidade e suporte a múltiplas linguagens. Foi feita toda a codificação do projeto, utilizando as linguagens HTML, CSS

2.2.3 Design do site

O processo de design do projeto foi desenvolvido com foco na clareza e na experiência do usuário, adotando uma identidade visual moderna e alinhada ao tema da segurança cibernética. As telas foram estruturadas para transmitir informações de forma objetiva, utilizando contrastes de cores em tons de roxo e azul, ícones representativos e elementos gráficos que reforçam a ideia de proteção e tecnologia. Além disso, a organização dos conteúdos em seções como Home, como se proteger e objetivo garante uma navegação intuitiva e didática, facilitando a compreensão do usuário e tornando a interação mais envolvente.

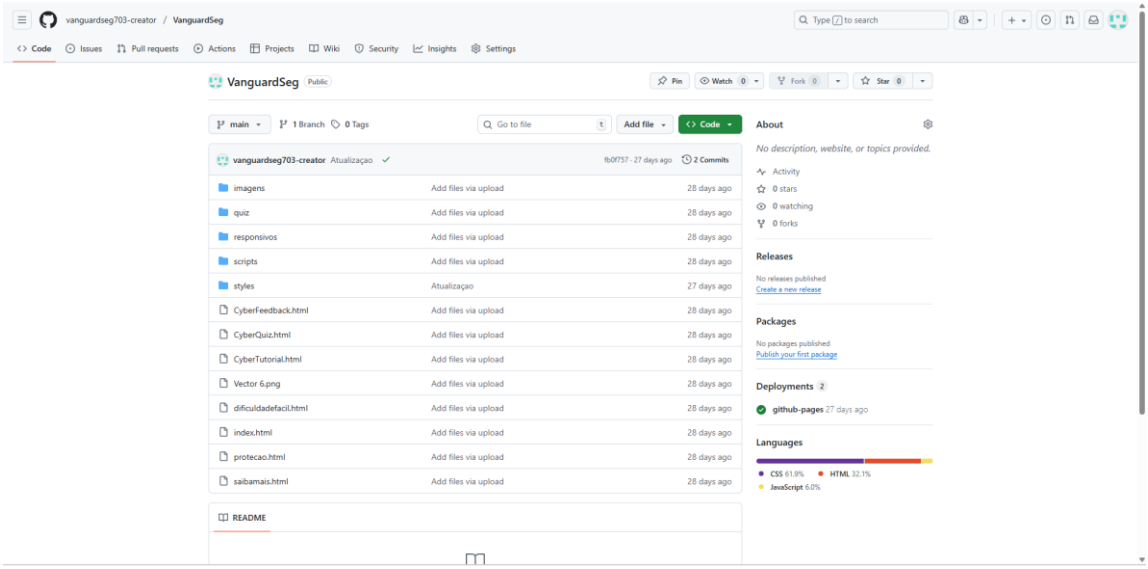
2.2.4 Acessibilidade digital

Com o objetivo de tornar o projeto mais inclusivo, o grupo implementou recursos de acessibilidade no site por meio de um zoom que amplia o tamanho da fonte, auxiliando pessoas com baixa visão. A iniciativa reforça a preocupação em promover igualdade de acesso às informações, garantindo que usuários com diferentes necessidades possam interagir com o conteúdo de forma autônoma e eficiente.

2.2.5 Hospedagem

O grupo utilizou o GitHub como plataforma de hospedagem do projeto, aproveitando suas funcionalidades para versionamento de código, organização dos arquivos e colaboração entre os integrantes. Essa escolha possibilitou maior controle sobre as atualizações, transparência no desenvolvimento e facilidade de acesso aos materiais produzidos, além de garantir segurança e confiabilidade no armazenamento.

Imagem 57 – Hospedagem



Fonte: (Caio, 2025)

3. CONSIDERAÇÕES FINAIS

Este trabalho explorou a experiência dos alunos na criação de um site educativo focado na conscientização sobre segurança digital. O desenvolvimento do VanguardaSeg permitiu que o grupo aplicasse, no projeto, os conhecimentos estudados ao longo do curso, juntamente com pesquisas, prototipação e programação, resultando em um site simples e educativos

Entretanto, reconhecemos a existência de algumas adversidades, como a variação no nível de conhecimento entre os desenvolvedores, o que pode influenciar a qualidade e o andamento da produção dos conteúdos do site. Para projetos futuros, seria pertinente explorar de forma mais aprofundada o uso de plataformas educativas como recurso de ensino e conscientização.

Portanto, o VanguardaSeg contribuiu para a conscientização da segurança digital, destacando como a cibersegurança é necessária para tornar o uso da internet mais seguro.

4. REFERÊNCIAS

BRITO, Flávia. **Segurança cibernética no Brasil: desafios e necessidades urgentes de ação, 2024**

Disponível em: https://abes.org.br/seguranca-cibernetica-no-brasil-desafios-e-necessidades-urgentes-de-acao/ Acesso em: 12 de out. 2025.

BRITO, Maria. **Segurança Digital na Educação: Normas e Boas Práticas para o Tratamento de Dados de Crianças e Adolescentes, 2025**

Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=N9hjE-QAAQBAJ&oi=fnd&pg=PT7&dq=livros+seguran%C3%A7a+digital&ots=Tv-a2lxt0X&sig=AtowF0-oxhq2GZdawXAEzCMDRk4&redir_esc=y#v=one-page&q=livros%20seguran%C3%A7a%20digital&f=false Acesso em: 19 de nov. 2025.

LANDIM, José. **Na trilha da segurança digital: protegendo o conhecimento, 2025**

Disponível em: https://periodicos.newsciencepubl.com/arace/article/view/3442 Acesso em: 19 de nov. 2025.

SÁNCHEZ, Raquel. **Segurança na Internet como parte da competência digital do cidadão, 2024**

Disponível em: https://periodicos.ufmg.br/index.php/textolivre/article/view/51787 Acesso em: 10 de nov. 2025

SILVA, Lavandoski **Segurança cibernética no Brasil: uma análise dos fatores institucionais que precedem a política de segurança cibernética entre 2008 – 2020.**

Disponível em: https://dspace.unila.edu.br/items/26957db7-9e20-4144-9bd9-45ca0be122e6 Acesso em: 7 de nov. 2025

SNOWDEN, Edward. **Mensagem a Glenn Greenwald sobre criptografia. In: GREENWALD, Glenn. Sem Lugar Para Se Esconder: Edward Snowden, a NSA e o Estado de Vigilância Americano. Rio de Janeiro: Sextante, 2014.**

Disponível em: https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower