CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

ETEC SYLVIO DE MATTOS CARVALHO

Curso de Técnico em desenvolvimento de sistemas

Ana Carolina Santos Reginatto

Gustavo Henrique Da Silva Campi

João Pedro Alves

Kamily Vitória Simeão

Olga Leticia Lopes

CyberSafeZone - Denúncias e estratégias para prevenção de crimes cibernéticos

Matão, SP
2023

Ana Carolina Santos Reginatto
Gustavo Henrique Da Silva Campi
João Pedro Alves
Kamily Vitória Simeão
Olga Leticia Lopes

CyberSafeZone - Denúncias E Estratégias Para Prevenção De Crimes Cibernéticos

Trabalho de Conclusão do Curso apresentado ao Curso Técnico em Desenvolvimento de Sistemas da Escola Técnica Estadual Sylvio de Mattos Carvalho, orientado pelo(a) Prof(a). Amanda Carolina da Cunha, como parte dos requisitos para a obtenção do título de Técnico em desenvolvimento de sistemas.

Matão, SP
2023

RESUMO

No contexto atual, marcado pela expansão da internet e pela dependência crescente da tecnologia, semelhante ao que é retratado na série "Mr. Robot", observamos um aumento expressivo de crimes cibernéticos durante a pandemia de COVID-19. Dados de 2022 indicam um crescimento de 21% em golpes e ataques cibernéticos em comparação ao ano anterior. Estes ataques, semelhantes às tramas da série, afetaram mais de 300 mil pessoas. A conscientização sobre esses riscos é crucial, destacando a importância de proteger a privacidade e a segurança online. O CyberSafeZone oferece uma abordagem holística para prevenção, fornecendo informações, ferramentas como geradores de senhas e criptografadores. A plataforma visa capacitar os usuários a fortalecer sua segurança online, sem armazenar dados pessoais, garantindo máxima segurança e privacidade. Assim como os personagens de "Mr. Robot" enfrentam desafios cibernéticos, a mensagem é que todos têm o poder de navegar com confiança no mundo digital, priorizando a segurança e a tranquilidade online.

Palavras-Chave: cibernético, tecnologia, golpe, crime, site, ataque, internet.

SUMÁRIO

1. INTRODUÇÃO

Nas últimas décadas, a expansão da internet e o crescente uso de tecnologia digital transformaram radicalmente a forma como vivemos e interagimos. No entanto, essa transformação também trouxe consigo uma sombra preocupante: o aumento significativo de crimes cibernéticos e ataques virtuais.

Durante o período da pandemia de COVID-19, quando o mundo se voltou ainda mais para a internet em busca de entretenimento, educação e trabalho remoto, testemunhamos um aumento notável na utilização da rede. No entanto, à medida que a dependência da tecnologia cresceu, também cresceram os riscos associados a crimes cibernéticos.

O levantamento do Portal Terra revela que o crescimento de golpes disfarçados de jogos aumentou em 21% no ano de 2022, em comparação com o ano anterior. Isso resultou em mais de 300 mil pessoas infectadas por malwares e adwares.

Um ataque hacker pode acontecer de diversas maneiras e ter diferentes objetivos. O tipo de ataque mais comum é a invasão, que em geral tem como objetivo roubar dados sigilosos por troca de dinheiro ou estragar o funcionamento da página.

No caso do ataque realizado pelo grupo Lulz Security Brazil, não foi exatamente uma invasão, mas sim um ataque distribuído por negação de serviço. Esse tipo de ataque não visa roubar dados, porém tem como objetivo retirar determinado site do ar temporariamente sem causar grandes danos. Os objetivos por trás do ataque como o que aconteceu podem ser muitos, desde uma reinvindicação política até atividades criminosas.

Diante dessas informações, é de extrema importância conscientizar sobre os casos mais comuns de golpes atualmente. Conforme relatado pelo site globo.com (data), o número de golpes cometidos pela internet aumentou em 175% durante a pandemia. Isso inclui diversos tipos de fraudes, como stalking, doxxing e fraudes financeiras.

Doxxing consiste na coleta e divulgação não autorizada de informações pessoais de um indivíduo, como nome completo, endereço, número de telefone e fotos. Embora a coleta de informações não seja ilegal, essa prática frequentemente é usada para intimidar pessoas com opiniões impopulares ou envolvimento em atividades políticas ou sociais. Ela também pode ser direcionada a empresas e

organizações, o que pode afetar sua reputação e ter implicações legais. O doxxing é amplamente considerado uma forma de assédio online e é ilegal em muitos países. Em um contexto em que a privacidade online é uma preocupação crescente, é vital proteger as informações pessoais e a privacidade.

O stalking envolve um comportamento persistente e repetitivo de assédio, que pode incluir perseguição física, virtual, por mensagens e telefonemas indesejados. Essa prática é uma forma de violência de gênero e pode causar danos emocionais e físicos significativos, incluindo violência, agressão sexual, dano à reputação e até homicídio. O stalking é considerado um crime em muitos países, e é crucial que as vítimas recebam apoio e orientação para garantir sua segurança e bem-estar. Estima-se que uma em cada seis mulheres e um em cada dez homens já tenham sido vítimas de stalking em algum momento de suas vidas.

As vítimas de crimes e assédio online podem enfrentar várias consequências graves, como aumento da ansiedade, depressão, isolamento social, traumas e perda de confiança. Isso ressalta a necessidade crucial de discutir crimes cibernéticos e de oferecer suporte às vítimas que podem não saber onde ou como procurar ajuda após serem alvo desses crimes.

O objetivo deste trabalho é fornecer ajuda e informações sobre os tipos de ataques e maneiras de prevenção aos crimes visando auxilio às vítimas de doxxing (roubo de dados) e outros ataques virtuais, auxiliando-as nos primeiros passos após um ataque e conscientizando-as sobre a importância da prevenção de roubo de dados. Espera-se que, com as informações adquiridas, as vítimas tenham um maior entendimento sobre o assunto e saibam como se proteger contra possíveis ataques.

2. METODOLOGIA

Foi realizado um levantamento por meio de um formulário para avaliar a percepção da utilidade desse projeto.

A abordagem metodológica adotada incluiu pesquisa bibliográfica, análise de dados sobre crimes cibernéticos, e uma análise comparativa com a série "Mr. Robot". A metodologia prática envolveu o desenvolvimento do CyberSafeZone, com detalhes registrados em todas as etapas.

Surpreendentemente, 60% dos participantes admitiram não ter conhecimento sobre estratégias e prevenções diante de um crime cibernético, revelando uma lacuna significativa na conscientização. Além disso, alarmantes 89% dos entrevistados afirmaram não se sentirem seguros ao utilizar mídias sociais. Esses resultados ressaltam a extrema relevância e urgência desse projeto.

Para a realização deste projeto utilizamos as seguintes metodologias:

2.1 TABULAÇÃO DE DADOS

Segundo os dados obtidos no questionário é notável que o público respondente tem uma percepção sobre os crimes na rede bem proporcional ao devido crescimento da tecnologia.

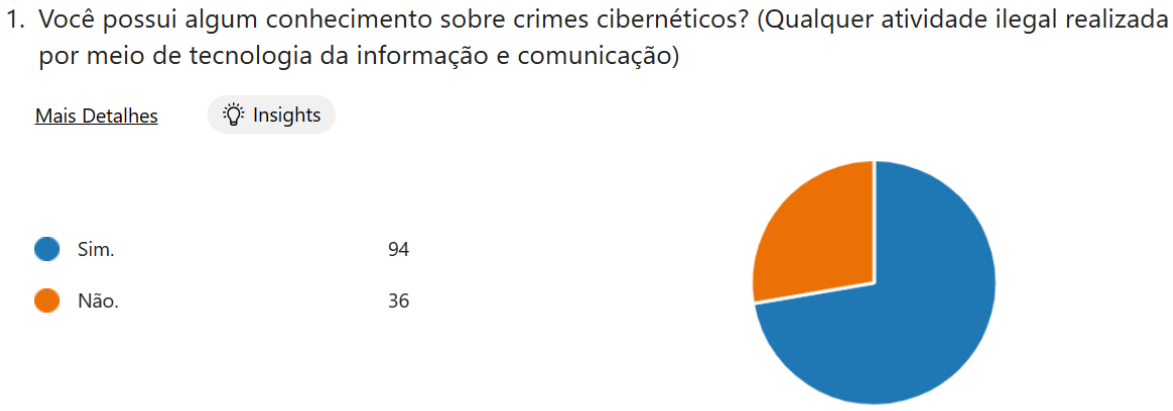


Figura 1: Pergunta 1 do Formulário

FONTE: Arquivo Pessoal

Mesmo com uma noção sobre crimes cibernéticos grande parte das pessoas não tem instrução de como e onde realizar as denúncias desses crimes por isso é um fator que contribui para a relevância do presente trabalho.

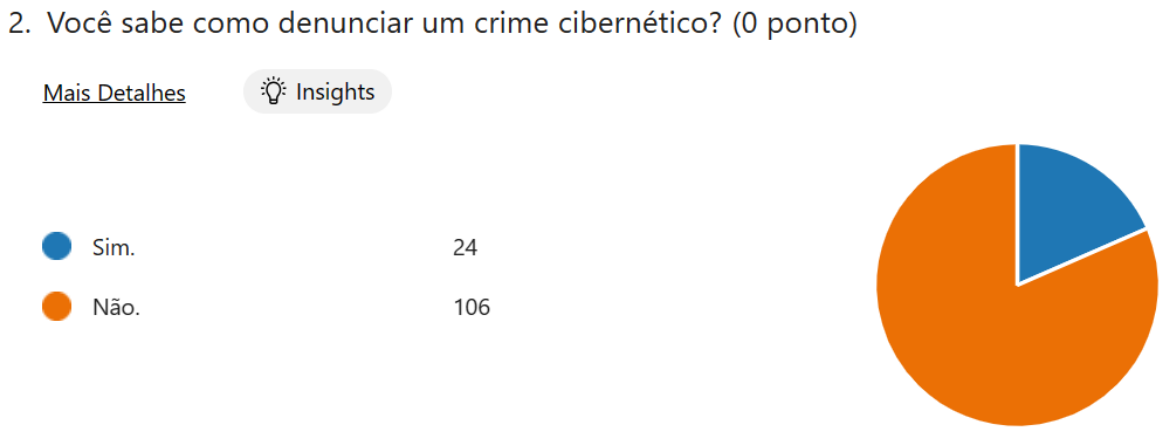


Figura 2: Pergunta 2 do Formulário

FONTE: Arquivo Pessoal

A metade dos usuários responderam não ter conhecimento sobre técnicas ou/e estratégias sobre prevenção da sua segurança na internet, outro fator que contribui para o desenvolvimento do projeto.

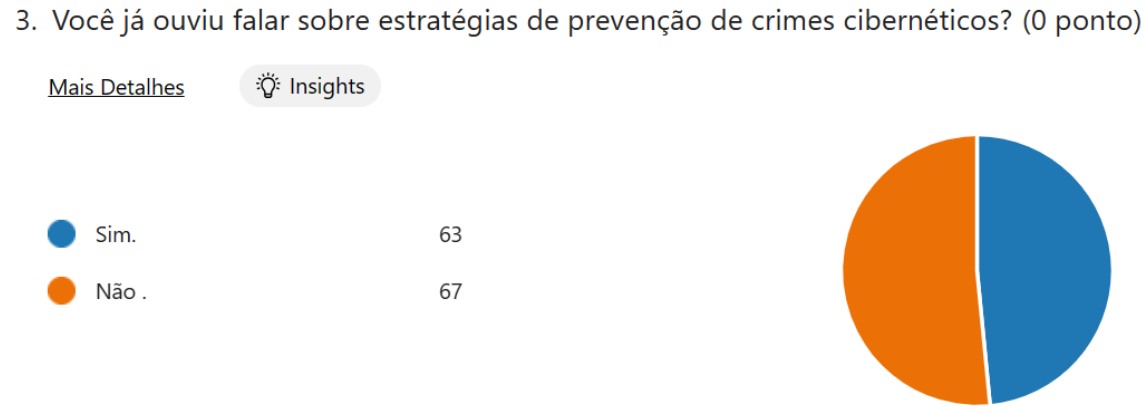


Figura 3: Pergunta 3 do Formulário

FONTE: Arquivo Pessoal

Grande parte do público tem ciência de que as redes sociais não são seguras para a exposição de seus dados pessoais, mas ainda se faz necessário informar cada vez mais pessoas sobre a segurança nas redes e a necessidade do presente trabalho.

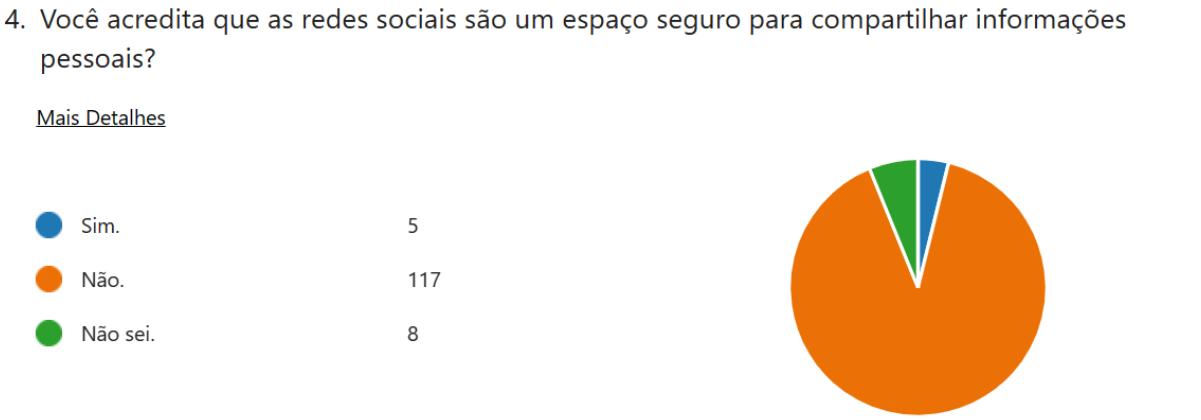


Figura 4: Pergunta 4 do Formulário

FONTE: Arquivo Pessoal

Com as respostas obtidas é observado a necessidade de ressaltar maior cuidado em sites pois os termos de uso e os cookies utilizam da informação dos usuários, e dependendo do site utilizado podendo roubar suas informações.

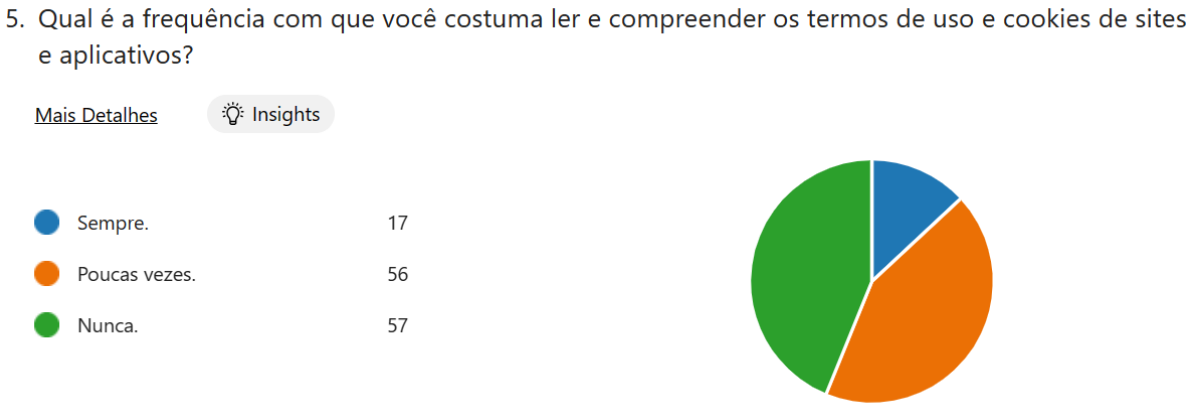


Figura 5: Pergunta 5 do Formulário

FONTE: Arquivo Pessoal

3. FERRAMENTAS

3.1 HTML

HTML: Uma abreviação de Hypertext Markup Language, utilizada para marcação de Hipertextos, ou seja, uma ferramenta responsável pela publicação dos conteúdos de textos, vídeos, imagens em uma aplicação web.

Para um melhor entendimento, a linguagem HTML é baseada em um contexto de hipertexto onde os elementos são conectados formando uma ponte de informações, permitindo a comunicação de dados junto à organização de conhecimentos.

3.2 CSS

CSS: Cascading Style Sheets é uma linguagem que controla a aparência e o layout de páginas web. Ele separa o estilo do conteúdo, permitindo estilizar elementos HTML com propriedades como cor, tamanho de fonte e margens. O CSS é usado para criar designs responsivos, layouts complexos e animações suaves, sendo aplicado a elementos selecionados por meio de seletores. Ele é escrito em arquivos separados, chamados folhas de estilo, e conectado aos documentos HTML para definir como os elementos são exibidos no navegador.

3.3 SCSS

SASS: Syntactically Awesome Style Sheets é um pré-processador CSS que melhora a escrita de estilos. Ele introduz recursos como variáveis, aninhamento de seletores, funções e mixins para criar folhas de estilo mais organizadas e eficientes. Sass é convertido em CSS regular durante a compilação, facilitando a manutenção e o desenvolvimento de estilos avançados para sites e aplicativos web.

3.4 JAVASCRIPT

JavaScript é uma linguagem de programação amplamente utilizada em desenvolvimento web e além. Ela permite adicionar interatividade e comportamento dinâmico a páginas web. JavaScript é executado no navegador do usuário e pode ser usado para manipular elementos da página, responder a eventos como cliques de mouse e submissões de formulários, além de fazer requisições para servidores e criar aplicativos web complexos. Com uma sintaxe versátil, JavaScript é usado tanto no front-end (navegador) quanto no back-end (servidor), graças a ambientes como o Node.js.

3.5 VERCEL

A Vercel é uma plataforma de hospedagem focada em oferecer uma experiência rápida e fácil para implantar projetos web. Ela é conhecida por sua integração perfeita com frameworks populares, como Next.js, React, Angular, e outros, tornando-a uma escolha popular para desenvolvedores que trabalham com essas tecnologias.

4 DESENVOLVIMENTO

Durante a concepção do presente projeto, uma série de considerações cuidadosas foram empreendidas visando a promoção de apoio e a disseminação de recursos destinados a vítimas de delitos cibernéticos, bem como a formulação de estratégias eficazes para prestar auxílio. Neste contexto, foi cunhado o termo "CyberSafeZone," cujo significado é "Zona Segura da Web."

Com o conceito concebido, a elaboração do projeto contemplou a criação de ferramentas concretas, nomeadamente geradores de senhas, dispositivos de encriptação e validadores de senhas.

Neste contexto, a abordagem de temáticas críticas relacionadas aos crimes cibernéticos foi meticulosamente subdividida em seções relevantes, visando à exploração de aspectos como o aumento significativo da exposição online, fenômeno acentuado pela pandemia global. Paralelamente, estabeleceu-se correlações pertinentes com o enredo da aclamada série "Mr. Robot," a fim de enriquecer a análise com insights da cultura popular contemporânea.

Na sequência, foram apresentadas estatísticas acerca da incidência de crimes cibernéticos, com especial ênfase nos tipos mais comuns de ataques e suas motivações subjacentes. Tais informações, fundamentadas em fontes confiáveis, concorreram para a construção de um contexto sólido e embasado.

No que fere à seleção das linguagens de programação utilizadas para a implementação do CyberSafeZone, optou-se por HTML, CSS e JavaScript. Essa escolha se pautou pela premissa de simplicidade, acessibilidade e eficiência, de modo a assegurar que a plataforma fosse acessível e de fácil utilização para um público diversificado.

4.1 CAPTURAS DO FRONT-END

Na tela inicial há uma barra de navegação, opção de modo noturno, onde ícones e elementos de interface gráfica do usuário em cores claras em um fundo escuro do site.

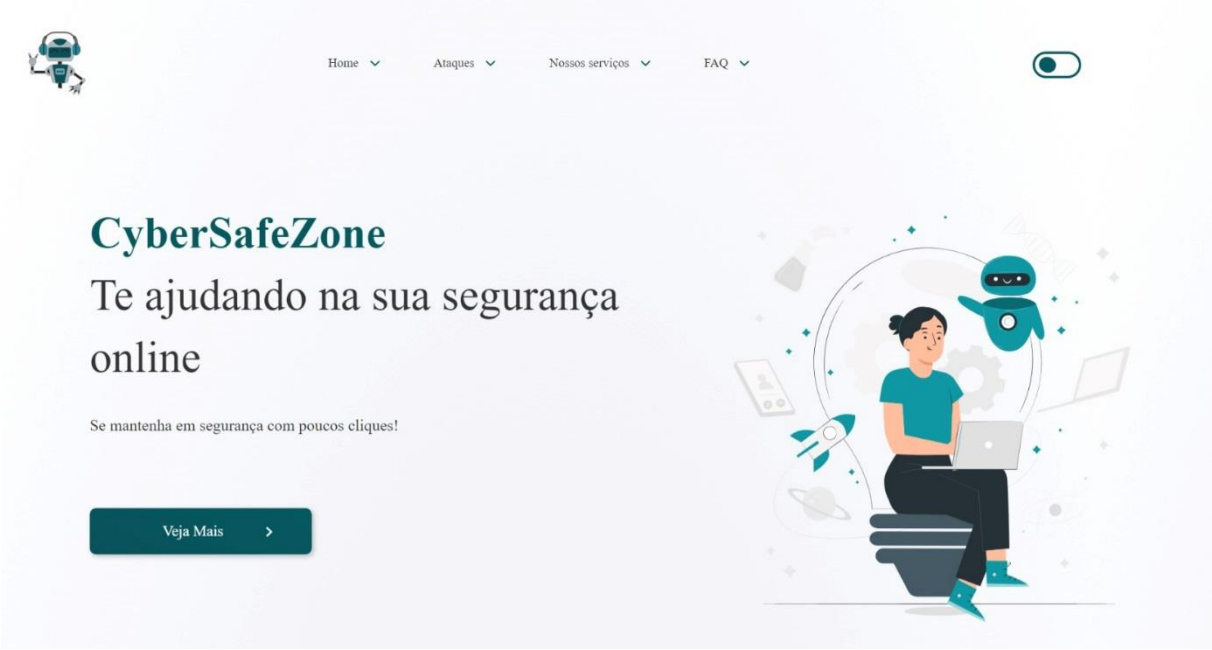


Figura 6: Home Page

FONTE: Arquivo Pessoal

```html
<main>
        <section id="featured">
            <div class="container">
                <div class="featured-main-page">
                    <div class="container-content-featured scrollReveal200">
                        <h1>
                            <span>CyberSafeZone</span> <br>
                            Te ajudando na sua segurança online
                        </h1>
                        <h3>Se mantenha em segurança com poucos cliques!</h3>
                        <div class="featured-open-account">
                            <button id="button-open-account" href="#innovation" rel="noopener">
                                <h4>Veja Mais</h4>
                                <div class="arrow-wrapper">
                                    <div class="arrow"></div>
                                </div>
                            </button>
                            <div class="container__img-principal">
                                <img class="main-img" src="assets/img/home/imagem-principal.svg" alt="imagem principal">
                            </div>
                        </div>
                    </div>
                </div>
            </div>
        </section>
```

Figura 7: Código home Page

FONTE: Arquivo Pessoal

Na página de links, há recursos para obter informações de Doxxing, fraudes financeiras, phishing, para informar sobre ataques cibernéticos e como se prevenir.

Figura 8: Página de Links

FONTE: Arquivo Pessoal

```
<section id="innovation">
            <div class="container">
                <h2>Quais São Os Principais Crimes
                    <span>Cibernéticos?</span>
                </h2>
                <div class="container-benefits scrollReveal200">
                    <img class="phone-card" src="assets/img/home/GloboPhone.svg" alt="crimes-image">
                    <div class="benefits scrollReveal300">
                        <article>
                            <div>
                                <img src="assets/img/icons/segurancaCibernetica.svg" alt="Cartão icon">
                            </div>
                            <h4>Segurança Cibernética </h4>
                            <p>O que é segurança cibernética? <br>
                            <p>Importância da segurança cibernética.</p>
                            </p>
                            <h6>
                                <a href="./pages/informative/cybersecurity.html" rel="noopener">Saiba mais</a>
                            </h6>
                        </article>

                        <article>
                            <div>
                                <img src="assets/img/icons/chaveSeguranca.svg" alt="Coração icon">
                            </div>
                            <h4>Gestão de Senhas Seguras </h4>
                            <p>Criando senhas fortes. <br> Gerenciadores de senhas. <br> Autenticação de dois fatores
                                (2FA). </p>
                            <h6 class="padding-know-more3">
                                <a href="./pages/informative/password-management.html" rel="noopener">Saiba mais</a>
                            </h6>
                        </article>

                        <article>
                            <div>
                                <img src="assets/img/icons/segurancaProtection.svg" alt="Pix icon">
                            </div>
                            <h4>Estratégias de Denuncias </h4>
                            <p>Oque fazer após dados vazados<br>Como agir e se proteger
                                <br>Plano de resposta a incidentes
                            </p>
                            <h6 class="padding-know-more">
                                <a href="./pages/informative/incident -response.html" rel="noopener">Saiba mais</a>
                            </h6>
                        </article>

                        <article>
                            <div>
                                <img src="assets/img/icons/segurancaEscudo.svg" alt="Pix icon">
                            </div>
                            <h4> Segurança de Redes</h4>
                            <p>Proteção na internet<br>Criptografia e dicas de proteção
                                <br>Casos reais
                                <br>Firewalls
                            </p>
                            <h6 class="padding-know-more">
                                <a href="./pages/informative/network-security.html" rel="noopener">Saiba mais</a>
                            </h6>
                        </article>
                        <article>
                            <div>
                                <img src="assets/img/icons/doxxing.svg" alt="Pix icon">
                            </div>
                            <h4> Doxxing</h4>
                            <p>Ladrão de Informações<br>Se proteja e Colete Informações
                                <br>Casos reais e mais.
                            </p>
                            <h6 class="padding-know-more">
                                <a href="./pages/informative/doxxing.html" rel="noopener">Saiba mais</a>
                            </h6>
                        </article>
                        <article>
                            <div>
                                <img src="assets/img/icons/Alarmedenuncia.svg" alt="Porcentagem icon">
                            </div>
                            <h4>Canais de Denuncia</h4>
                            <p>
                                Denunciar crimes cibernéticos é fundamental
                                para combater atividades ilegais na internet
                                e promover a segurança online. <br>
                            <h6 class="padding-know-more2">
                                <a href="./pages/informative/complaints.html" rel="noopener">Saiba mais</a>
                            </h6>
                        </article>
                    </div>
                </div>
            </div>
        </section>
```

Figura 9: Código página de Links

FONTE: Arquivo Pessoal

A Terceira página mostra os serviços que o site oferece ao usuário, de criação de senhas criptografadas e como descriptografar a mesma.

Figura 10: Página serviços

FONTE: Arquivo Pessoal

```
<section id="blog">
            <div class="container">
                <h2>Acesse os serviços do
                    <span>cybersafezone</span>
                    e se mantenha em <span>segurança</span>
                </h2>

                <div class="container-blog-items">
                    <article class="scrollReveal300">
                        <img src="./assets/img/functions/gerar-senha.svg" alt="Segurança">
                        <h3>Usa a mesma senha para todos os apps?</h3>
                        <p>Use nosso serviço que gera uma senha customizada para você<br>
                            <a class="button-link" href="./pages/passwords/passwords-steps.html">Use agora</a>
                        </p>
                    </article>

                    <article class="scrollReveal400">
                        <img src="./assets/img/functions/cripto.svg" alt="Segurança">
                        <h3>Precisa enviar dados sigilosos?</h3>
                        <p>Utilize nossa criptografia para enviar-los em segurança<br> <a class="button-link"
                                href="./pages/cryptography/cryptography-steps.html">Use agora</a></p>
                    </article>

                    <article class="scrollReveal500">
                        <img src="./assets/img/home/passwordInvasion.svg" alt="Segurança">
                        <h3>Quer verificar a segurança da sua senha atual?</h3>
                        <p>Use nosso serviço de verificação de senha e veja por quanto tempo ela seria quebrada<br> <a
                                class="button-link" href="./pages/passwords/checkpasswords.html">Use agora</a>
                        </p>
                    </article>
                </div>
                </article>

            </div>
            </div>
        </section>
```

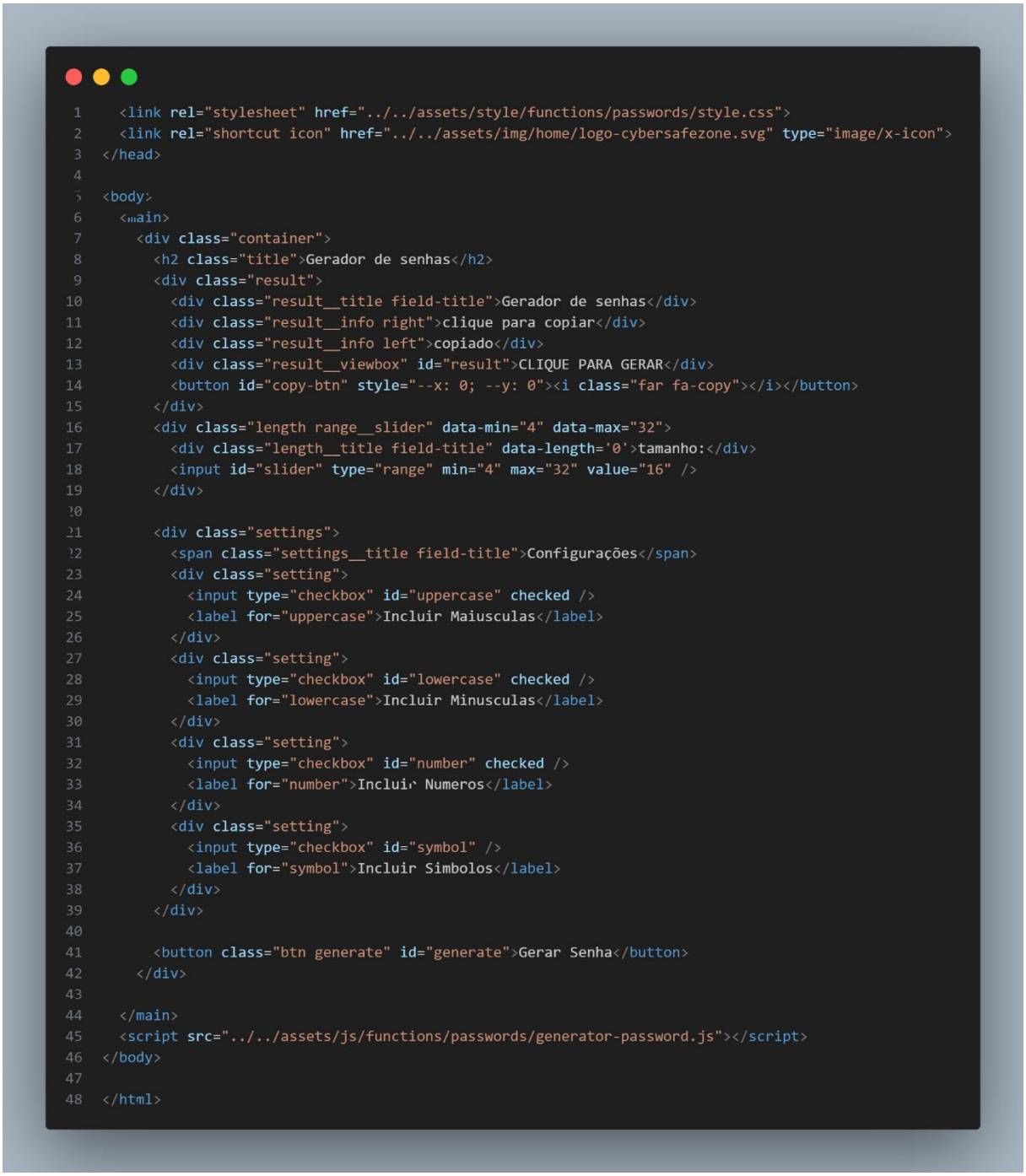
Figura 11: Código página serviços

FONTE: Arquivo Pessoal

O site conta com um gerador de senhas aonde o usuário será capaz de escolher os caracteres que irão compor sua senha.

Figura 12: Gerador de senhas

FONTE: Arquivo Pessoal



```
  <link rel="stylesheet" href="../../assets/style/functions/passwords/style.css">
  <link rel="shortcut icon" href="../../assets/img/home/logo-cybersafezone.svg" type="image/x-icon">
</head>

<body>
  <main>
    <div class="container">
      <h2 class="title">Gerador de senhas</h2>
      <div class="result">
        <div class="result__title field-title">Gerador de senhas</div>
        <div class="result__info right">clique para copiar</div>
        <div class="result__info left">copiado</div>
        <div class="result__viewbox" id="result">CLIQUE PARA GERAR</div>
        <button id="copy-btn" style="--x: 0; --y: 0"><i class="far fa-copy"></i></button>
      </div>
      <div class="length range__slider" data-min="4" data-max="32">
        <div class="length__title field-title" data-length='0'>tamanho:</div>
        <input id="slider" type="range" min="4" max="32" value="16" />
      </div>

      <div class="settings">
        <span class="settings__title field-title">Configurações</span>
        <div class="setting">
          <input type="checkbox" id="uppercase" checked />
          <label for="uppercase">Incluir Maiusculas</label>
        </div>
        <div class="setting">
          <input type="checkbox" id="lowercase" checked />
          <label for="lowercase">Incluir Minusculas</label>
        </div>
        <div class="setting">
          <input type="checkbox" id="number" checked />
          <label for="number">Incluir Numeros</label>
        </div>
        <div class="setting">
          <input type="checkbox" id="symbol" />
          <label for="symbol">Incluir Simbolos</label>
        </div>
      </div>

      <button class="btn generate" id="generate">Gerar Senha</button>
    </div>

  </main>
  <script src="../../assets/js/functions/passwords/generator-password.js"></script>
</body>

</html>
```

Figura 13: Código gerador de senhas

FONTE: Arquivo Pessoal

Há também outra ferramenta na qual é possível executar um teste de força, e visualizando um tempo estimado para a quebra da senha.

Figura 14: Teste de Senha

FONTE: Arquivo Pessoal

```html
<!DOCTYPE html>
<html>
<head>
    <title>Teste de Força de Senha</title>
    <link rel="stylesheet" href="../../assets/style/functions/passwords/checkpasswords.css">
    <link rel="shortcut icon" href="../../assets/img/home/logo-cybersafezone.svg" type="image/x-icon">

</head>
<body>
    <div class="main-container">
        <div class="card">
            <h1>Teste de Força de Senha</h1>
            <input type="password" id="senha" placeholder="Digite sua senha">
            <button onclick="verificarForca()">Verificar Força</button>
            <p id="resultado"></p>
            <p id="tempoEstimado"></p>
        </div>
        <div class="container__img-principal">
            <img class="main-img" src="../../assets/img/home/imagem-principal.svg" alt="imagem principal">
        </div>
    </div>

    <script src="../../assets/js/functions/passwords/check-password.js">
    </script>
</body>
</html>
```

Figura 15: Código teste de Senha

FONTE: Arquivo Pessoal

Para o uso de um de um dos serviços no CyberSafeZone, há passos para conduzir os usuários de como se utilizar apenas seguindo as etapas com atenção.

Figura 16: Etapa do Criptografador

FONTE: Arquivo Pessoal

Compondo os serviços do CyberSafeZone, há um criptografador a qual é possível criptrografar mensagens a partir de chaves.

Figura 17: Criptografador

FONTE: Arquivo Pessoal

5 CONSIDERAÇÕES FINAIS

Considerando a complexidade inerente ao cenário dos crimes cibernéticos e as constantes mudanças no ambiente digital, este estudo se empenhou em analisar os desafios e as estratégias de enfrentamento relacionados a essa ameaça em evolução. A pesquisa realizada revelou diversas constatações dignas de atenção e reflexão.

Primeiramente, a análise dos tipos comuns de ataques cibernéticos e suas motivações subjacentes permitiu uma compreensão mais profunda das estratégias empregadas por agentes maliciosos. A identificação de fatores motivadores, como ganhos financeiros, espionagem cibernética e atividades de hacktivismo, realça a necessidade de uma abordagem complexa na prevenção e combate a essas ameaças.

No que tange à segurança cibernética, a análise das melhores práticas e a importância de medidas proativas, como a implementação de sistemas de detecção de intrusões avançados e a educação contínua sobre segurança digital, ressaltam a necessidade de preparação e conscientização constantes.

O projeto também ressaltou a importância de tecnologias de segurança, como o gerador de senhas fortes e o verificador de senhas, na mitigação de ameaças cibernéticas. Tais avanços representam oportunidades significativas para fortalecer a defesa contra ataques e aprimorar a resiliência cibernética.

Por fim, é fundamental destacar que a cibercriminalidade é um desafio dinâmico que continuará a evoluir à medida que a tecnologia avança. Portanto, a pesquisa nesse campo deve ser contínua e adaptativa, buscando novas soluções e estratégias à medida que surgem ameaças inéditas.

Nesse contexto, as conclusões deste trabalho enfatizam a necessidade de um compromisso contínuo com a pesquisa e a colaboração entre diferentes atores, incluindo governos, empresas, sociedade civil e organizações internacionais, para enfrentar eficazmente a cibercriminalidade em um mundo cada vez mais interconectado.

REFERÊNCIAS

ANTÓNIO KOMBO, Carlos. **Monitoramento De Invasões, Simulação De Ataques De Um Servidor Honeypot Em Ambiente Controlado**. 2019. Trabalho de Conclusão de Curso. Universidade Do Extremo Sul Catarinense - Unesc. Disponível em: http://repositorio.unesc.net/handle/1/8199. Acesso em: 27 de abril de 2023.

BOTTCHER, Geisi. GRAFF, Suelen. **Segurança Da Informação: Como Prevenir Roubo De Dados Pessoais. Uma Abordagem Socioeducativa Segurança Da Informação: Como Prevenir Roubo De Dados Pessoais. Uma Abordagem Socioeducativa**. 2015. Artigo Cientifico. Instituto Federal Catarinense . Disponível em: http://videira.ifc.edu.br/fice/wp-content/uploads/sites/27/2015/11/Seguranca-da-informacao-como-prevenir-roubo-de-dados-pessoais.pdf. Acesso em: 27 de abril de 2023.

DE AZEVEDO FILHO, Edison. CLAUDIA LARA DA COSTA, Maria. **Segurança em Servidores com Banco de Dados Microsoft SQL Server: Meios de Proteção contra invasões**. 2019. Artigo Cientifico. SEGeT – Simpósio de Excelência em Gestão e Tecnologia. Disponível em: https://www.aedb.br/seget/arquivos/artigos08/261_261_Seguranca.pdf. Acesso em: 27 de abril de 2023.

DE OLIVEIRA GARCIA, Rafael. **Estudos de Técnicas de Invasão e Segurança de Sistemas de Informação Online**. 2021. Trabalho de Conclusão de Curso. Centro Universitário Sagrado Coração. Disponível em: https://repositorio.unisagrado.edu.br/jspui/handle/handle/145. Acesso em: 27 de abril de 2023.

FERNANDO ARAUJO TEIXEIRA, Cleyson. **Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos**. 2021. Trabalho de Conclusão de Curso. Universidade Federal De Ouro Preto Escola De Minas Colegiado Do Curso De Engenharia De Controle E Automação - Cecau. Disponível em: https://monografias.ufop.br/bitstream/35400000/3567/1/MONOGRAFIA_Seguran%C3%A7aCibern%C3%A9ticaRedes.pdf. Acesso em: 27 de abril de 2023.

RODRIGUES DA SILVA, Washington. **Análise Econômica Dos Impactos De Ataques Cibernéticos**. 2018. Trabalho de Conclusão de Curso. Universidade de Brasília Faculdade de economia, administração, contabilidade E gestão de políticas públicas Programa de pós-graduação em economia Mestrado em economia. Disponível em: https://repositorio.unisagrado.edu.br/jspui/handle/handle/145. Acesso em: 27 de abril de 2023.

VERCEL. **Introdução à Vercel**. 2023. Disponível em: https://vercel.com/docs/getting-started-with-vercel. Acesso em: 02 de novembro de 2023.

MDN Mozilla. **Controle de fluxo e manipulação de erro**. 2023. Disponível em: https://developer.mozilla.org/pt-BR/docs/Web/JavaScript/Guide/Control_flow_and_error_handling. Acesso em: 02 de novembro de 2023.

HORA DE CODAR. **Qual a diferença entre SCSS e CSS**. 2023. Disponível em: https://horadecodar.com.br/css/sass-scss/. Acesso em: 09 de novembro de 2023.

W3SCHOOL. **HTML Tutorial**. 2023. Disponível em: https://www.w3schools.com/html/default.asp. Acesso em: 16 de novembro de 2023.

CRYPTOJS. **Cryptojs Documentação**. 2023. Disponível em: https://cryptojs.gitbook.io/docs/. Acesso em: 16 de novembro de 2023.

HOSTINGER TUTORIAIS. **O que é CSS guia básico para iniciantes**. 2023. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-css-guia-basico-de-css. Acesso em: 12 de novembro de 2023.

KASPERSKY Lab. **Segurança na internet: o que é e como você pode se proteger on-line?** 2023. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-internet-security. Acesso em: 04 de novembro de 2023.