Cyber Security Information: aplicação web para a democratização do acesso aos conteúdos relacionados à cibersegurança

Raphaela Guiland Ferraz[1,2], Victor Gabriel Marques[1,2], Anna Beatriz Santos e Souza[1,2], Adriano José Ferruzzi[1,2], Regivaldo Sousa Ferreira[1,2]

Resumo: Na contemporaneidade, a temática da Cibersegurança, também reconhecida como Segurança Cibernética, tem ganhado uma notória atenção, dado que, através do desenvolvimento intenso da tecnologia, há o surgimento e o avanço de diversos tipos de ataques cibernéticos. Nesse sentido, é observável a falta da democratização dessa temática para toda a comunidade, uma vez que os conteúdos que são disponibilizados, na internet ou em outros meios, possuem a característica predominante de serem restritos a um grupo específico de pessoas, pois, na maioria das vezes, são de difícil compreensão ou de difícil acesso. Além disso, constata-se a carência do compartilhamento de ferramentas e mecanismos que são capazes de proteger, instruir e informar os indivíduos sobre esse tema imprescindível. Dessa forma, para amenizar essas adversidades vigentes na comunidade, foi desenvolvida uma aplicação *web*, a *Cyber Security Information* (CSI), voltada para a socialização da segurança cibernética, seja através da presença da acessibilidade web nas suas páginas, seja pela utilização de uma linguagem mais simples na escrita dos conteúdos disponibilizados neste sistema web.

Palavras–chave: Cibersegurança. Sistema web. Democratização.

Abstract: In contemporary times, the theme of Cybersecurity, also recognized as Cybersecurity, has gained notable attention, given that, through the intense development of technology, there is the emergence and advancement of various types of cyberattacks. In this sense, the lack of democratization of this theme for the whole community is observable, since the contents that are made available, on the internet or in other means, have the predominant characteristic of being restricted to a specific group of people, since, in most cases, sometimes they are difficult to understand or difficult to access. In addition, there is a lack of sharing of tools and mechanisms that

[1] Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), São Paulo, SP, Brasil.

[2] Grupo de Informática e Tecnologia em Educação e Sociedade, GITES.

are capable of protecting, instructing and informing individuals about this essential topic. Thus, to alleviate these adversities prevailing in the community, a web application was developed, Cyber Security Information (CSI), aimed at the socialization of cybersecurity, either through the presence of web accessibility on its pages, or through the use of simpler language in the writing of the contents made available in this web system.

Keywords: *Cybersecurity. Web system. Democratization.*

1. INTRODUÇÃO

O desenvolvimento da tecnologia, historicamente, ocorreu de forma intensa e, nessa direção, Maciel (2015) relata que o primeiro computador digital eletrônico de grande escala, o *Electronic Numerical Integrator and Computer* (ENIAC), foi apresentado em 1946. Com o passar do tempo, os computadores foram aperfeiçoados, tornando-se multifuncionais e disponíveis para uso pessoal. Cury e Capobianco (2011) relatam que foi a partir de 1980 que a fase dos computadores portáteis e em rede se iniciou e, por consequência, é exatamente nessa década, que estão datados os primeiros registros de ataques cibernéticos, como o desenvolvimento do Elk Cloner, em 1982, por Richard Skrenta, um vírus[3] que tinha como principal objetivo a contaminação de computadores e o seu espalhamento se dava através de cópias de disquetes que já estavam infectados (CHARÃO, 2017).

Com o passar do tempo, na medida que os aparelhos eletrônicos foram sendo aprimorados, os crimes cibernéticos tornaram-se cada vez mais amplos e complexos. Com isso, criou-se, então, um ramo de estudos relacionado ao entendimento desses ataques e às formas de como garantir a segurança no espaço digital, área essa que é denominada como Cibersegurança, ou como Segurança Cibernética (em inglês, “Cybersecurity” ou “Cyber Security”). Diante disso, tal área pode ser definida como a segurança vigente no mundo virtual, a qual realiza a proteção desse ambiente, isto é, a segurança cibernética é responsável pela defesa dos sistemas de informação, dos

[3] Vírus corresponde a um software malicioso que se espalha, por conta própria, no computador. O vírus só é executado, de fato, através de um “software hospedeiro”, ou seja, ele por si só não consegue infectar a máquina, pois necessita que o programa infectado seja executado.

dados, das informações e de qualquer outra entidade que esteja presente no espaço computacional, dos mais variados crimes cibernéticos existentes (Brasil, 2021).

Dessa maneira, é de extrema relevância que a comunidade como um todo saiba a importância da cibersegurança e como ela pode impactar, positiva ou negativamente, a vida de inúmeras pessoas. Todavia, nota-se a ausência da democratização no acesso às informações relacionadas a esse tema, o que resulta em um grande número de pessoas desinformadas, principalmente o público mais isolado digitalmente (crianças, idosos e pessoas portadoras de deficiência).

Além disso, é observável que há, ainda, uma carência de tecnologias e ferramentas que auxiliem todas as pessoas da comunidade a, de fato, aplicar a segurança cibernética no cotidiano. Diante o exposto, o desenvolvimento de uma aplicação web, chamada de *Cyber Security Information* (CSI), é imprescindível, haja vista que as pessoas contarão com conteúdos de fácil compreensão e de fácil acesso e, ademais, o sistema web contará com recursos que garantirão a acessibilidade *web,* de modo a, em concordância com Cusin e Vidotti (2009), assegurar a inclusão informacional e digital de usuários que são portadores de deficiência.

Outrossim, a CSI é composta pelas seguintes tecnologias: linguagem de marcação HTML5[4], linguagem de estilização CSS3[5], linguagens de programação JavaScript[6] e Python[7] (com o auxílio do *framework* Django) e bancos de dados SQLite[8] e PostgreSQL[9].

[4] HTML5 corresponde à Linguagem de Marcação de Hipertexto (HyperText Markup Language), especificamente na versão 5, a qual é responsável pela estruturação das páginas da aplicação web.

[5] CSS3 corresponde à Folha de Estilos em Cascata (Cascading Style Sheets), responsável pela estilização das páginas da aplicação web, especificamente na versão 3.

[6] JavaScript trata-se de uma linguagem de programação que atua no navegador do usuário da aplicação web, sendo responsável pela dinamicidade das páginas.

[7] Python corresponde a uma linguagem de programação que atua no servidor da aplicação, além de ser responsável pela comunicação com o banco de dados e pela organização do *framework* Django. Este, por sua vez, é responsável por estruturar todas as funcionalidades da CSI.

[8] SQLite trata-se de um banco de dados, ou seja, é uma coleção organizada de dados. No caso deste projeto, o SQLite foi utilizado para armazenar, nos ambientes de desenvolvimento e de homologação, os artigos, os tutoriais, as ferramentas e os e-mails - cadastrados na *newsletter*.

[9] PostgreSQL é, assim como o SQLite, um tipo de banco de dados, o qual foi escolhido para ser utilizado no ambiente de produção, ou seja, na aplicação final disponibilizada publicamente.

Portanto, o objetivo do presente artigo é de apresentar o desenvolvimento da *Cyber Security Information,* a qual irá fornecer à comunidade ferramentas, artigos e tutoriais voltados à segurança cibernética. Sendo assim, este projeto busca a conscientização dos usuários acerca do tema, já que, por meio dos materiais disponibilizados, os usuários poderão se informar e se capacitar para uma segura utilização da internet.

1.1 Objetivos

1.1.1 Objetivo Geral

- Desenvolver uma aplicação *web* para difundir materiais sobre a cibersegurança, incluindo ferramentas para a aplicação dos conteúdos apresentados, tendo em vista a democratização do acesso aos conteúdos que tratam sobre o tema.

1.1.2 Objetivos Específicos

- Realizar o levantamento de requisitos;
- Produzir tutoriais, incluindo vídeos, imagens e textos, que tratem da aplicação da segurança cibernética nas redes sociais, aplicativos e aparelhos eletrônicos;
- Produzir artigos relacionados a cibersegurança, com uma linguagem acessível, de modo a garantir que os usuários da CSI possam compreender os assuntos abordados;
- Desenvolver ferramentas, as quais serão disponibilizadas na aplicação *web*, para que os usuários possam se precaver no mundo digital, aplicando os conteúdos expostos na aplicação;
- Estudar sobre acessibilidade na *web*, visando um desenvolvimento semântico da aplicação, de modo que pessoas portadoras de deficiências possam acessar, compreender, navegar e interagir na aplicação;
- Aperfeiçoar os conhecimentos relacionados à linguagem de marcação HTML5, à linguagem de estilização CSS3 e às linguagens de programação JavaScript e Python, de modo a desenvolver a aplicação seguindo boas práticas de programação;
- Inserir critérios/objetivos de segurança no desenvolvimento e na disponibilização da *Cyber Security Information*;

- Criar páginas nas principais redes sociais para um maior alcance de usuários da aplicação.

1.2 Justificativa

A realização do presente trabalho é de suma relevância, principalmente para as pessoas que não possuem um conhecimento prévio sobre Tecnologia da Informação e Segurança da Informação, uma vez que trata do desenvolvimento de uma aplicação *web* para divulgação de conteúdos essenciais sobre a Segurança Cibernética, além de tutoriais e ferramentas. Sendo assim, esta pesquisa será essencial para a disseminação e enfatização da importância do conhecimento acerca da cibersegurança, além de contribuir com a democratização do acesso aos conteúdos relacionados a essa área, pois a aplicação será desenvolvida seguindo padrões de acessibilidade.

Dessa forma, a abordagem que esse trabalho realiza sobre a cibersegurança é algo de extrema importância para o contexto atual, dado que a tecnologia está cada vez mais inserida na sociedade. Assim sendo, com o avanço da tecnologia, há também o avanço de crimes cibernéticos e isso é evidenciado pelo surgimento do “WannaCry”, em 2017, que, de acordo com Mohurle e Patil (2017), é um software malicioso do tipo *ransomware* responsável pela criptografia de arquivos ou dispositivos inteiros. A restituição desses dados só ocorre após a vítima realizar um pagamento ao sequestrador (*ranson*). Nessa direção, além do surgimento do “WannaCry”, muitos outros crimes cibernéticos desse tipo foram registrados e o mais recente deles, de acordo com a publicação de Henrique Andrade do jornal CNN Brasil (2021), foi o sequestro dos dados do Ministério de Saúde, em dezembro de 2021, pelo grupo de crackers “Lapsus$”. Diante do exposto, é necessário que as pessoas tenham conhecimento sobre o que é a cibersegurança e quais são as maneiras de aplicar esse conceito no dia-a-dia, de modo a evitar mais vítimas de crimes virtuais.

Com isso, este trabalho apresenta uma plataforma moderna na área de Segurança Cibernética, pois, além dos conteúdos teóricos, tutoriais e ferramentas reunidos em um único lugar, a aplicação *web* desenvolvida objetiva a possibilidade de acesso para o maior número de pessoas, por meio da acessibilidade *web*, o que, em concordância com Loja et al. (2015), visa minimizar as limitações das pessoas deficientes, além de contribuir para a inclusão dessas pessoas na sociedade (apud

Silva et al., 2018). Para isso, esse projeto utilizará outras tecnologias que facilitam a utilização, a navegação e o entendimento da aplicação, como, por exemplo, a ferramenta VLibras, responsável por traduzir o conteúdo digital (texto, áudio e imagem) em LIBRAS (Brasil, 2019). Ademais, o desenvolvimento da aplicação *web* conta com a utilização de recursos do HTML5 que possibilitam a navegação por teclado, algo fundamental para os usuários que utilizam softwares de leitura de tela e para usuários que não conseguem utilizar o *mouse* devido a alguma deficiência.

2. MÉTODO

Primordialmente, é válido salientar que a construção deste projeto se baseia, sobretudo, na democratização de conteúdos relacionados à segurança na internet. Com isso, a definição das etapas para a produção da aplicação web foi centrada na acessibilidade, de modo que este trabalho possa colaborar, de fato, com a socialização de seus materiais para um maior público-alvo. Não obstante, como o tema do projeto é a divulgação da cibersegurança, também foram definidas etapas diretamente relacionadas ao assunto. Portanto, a seguir há o detalhamento desses procedimentos.

Etapa 1) **Segmentação das áreas de desenvolvimento**

Para o início do desenvolvimento da *Cyber Security Information*, a segmentação das áreas de desenvolvimento em *front-end* e *back-end* foi o primeiro passo.

Etapa 2) **Definição dos critérios de segurança do sistema web**

Após dividir as áreas responsáveis pela concepção da aplicação, os critérios de segurança foram definidos, os quais foram:

- Comprar um certificado TLS/SSL - o qual é responsável por aumentar a segurança na transmissão de dados, haja vista que são criptografados. Ademais, esse certificado possibilita a utilização do protocolo HTTPS, o que demonstra para o usuário que a aplicação acessada é segura e confiável;
- Implementar, em todos os formulários da aplicação web, a utilização de CSRF Tokens - os quais servem para proteger o usuário de ataques *Cross-Site Request Forgery*, cujo objetivo é a falsificação de solicitações entre sites, de

modo que o atacante se passe pela vítima e realize ações em seu nome. Nesse sentido, é essencial que os tokens sejam utilizados, uma vez que são responsáveis por identificar, exclusivamente, um determinado usuário;

- Ocultar arquivos e informações sensíveis - os quais podem conter credenciais, dados armazenados na aplicação (arquivos de extensão .sqlite3), variáveis de ambiente e chaves de acesso à aplicações externas;
- Não permitir a indexação de páginas administrativas - ação que evita que o painel de administração da aplicação web apareça em buscas no navegador;
- Criar *backups* dos dados armazenados, isto é, criar cópias de todos os dados para evitar a indisponibilidade do sistema;

Etapa 3) **Criação dos ambientes para os diferentes estágios do ciclo de vida da aplicação web**

Nessa etapa, a área de *back-end* foi responsável por criar o **ambiente de desenvolvimento**, ou seja, o ambiente utilizado pelos integrantes para a programação da aplicação, o **ambiente de homologação**, isto é, o ambiente utilizado para a realização de testes na aplicação e o **ambiente de produção**, ou seja, o ambiente que os usuários finais utilizarão. Ademais, a área de *front-end* foi responsável por criar o **ambiente de design**, ou seja, o ambiente utilizado para a criação do design das páginas da aplicação.

Etapa 4) **Levantamento de Requisitos**

Após a criação da infraestrutura necessária para o desenvolvimento, foi realizado o levantamento de requisitos funcionais e de tecnologias necessárias para a criação da *Cyber Security Information*. O levantamento foi feito com a equipe de desenvolvimento, tendo como objetivo entregar uma aplicação simples, acessível e funcional para o público geral. Os quadros a seguir demonstram, respectivamente, os requisitos e as tecnologias utilizadas (Quadro 1 e Quadro 2).

QUADRO 1 – Requisitos funcionais da aplicação web

Atividades	Requisitos Funcionais
Garantir a Acessibilidade nas Páginas	Apresentar os conteúdos de maneira acessível para todos os públicos
Disponibilizar Artigos de Cibersegurança	Expor artigos, escritos de maneira acessível, sobre a Cibersegurança

Disponibilizar Tutoriais	Apresentar tutoriais em diversos formatos com exemplos de aplicações dos conteúdos dos artigos
Disponibilizar Ferramentas para Proteção	Exibir ferramentas voltadas à cibersegurança
Enviar E-mails	Enviar newsletter, para os usuários cadastrados no banco de dados, com avisos sobre a inclusão de conteúdos na aplicação
Disponibilizar um Canal de Contato	Expor um formulário para que os usuários possam contatar os desenvolvedores

Fonte: Os autores (2022)

QUADRO 2 – Tecnologias utilizadas

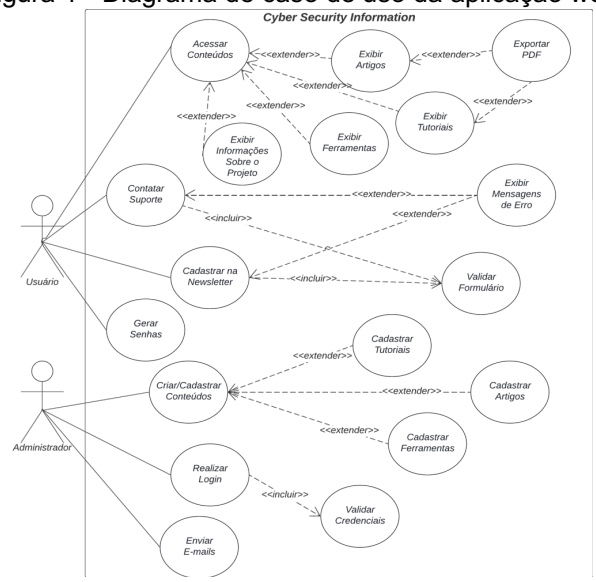
Atividades	Tecnologias
Criar o Layout da Aplicação	Windows, Figma
Configurar o Ambiente de Desenvolvimento	Windows, PyCharm, Git
Configurar o Ambiente de Homologação	Windows, PyCharm, Git
Criar as Páginas da Aplicação	Windows, PyCharm, Git, GitHub, HTML, CSS, JavaScript, Django
Configurar o Ambiente de Produção	Windows, PyCharm, Git, Heroku CLI, Heroku, Namecheap
Criar Infraestrutura de Armazenamento	Windows, Git, Heroku, PostgreSQL

Fonte: Os autores (2022)

Etapa 5) **Criação do Diagrama de Caso de Uso**

Com o objetivo de definir as metas de interações entre usuários e o sistema web, além de representar graficamente os seus requisitos funcionais, foi criado um diagrama de caso de uso (representado na Figura 1).

Figura 1 - Diagrama de caso de uso da aplicação web



Fonte: Os autores (2022)

Etapa 6) **Estruturação dos diretórios**

Por meio da utilização de projetos e aplicativos em *Django*, os diretórios da aplicação foram segmentados de maneira a seguir com as boas práticas de programação *back-end*, tornando a organização da aplicação mais simplificada e, por consequência, garantindo uma maior escalabilidade da aplicação *web*.

Etapa 7) **Criação e segmentação dos aplicativos**

Após a organização dos diretórios, os aplicativos *Django* foram segmentados por funcionalidade dentro do diretório “apps”. Nesse sentido, as páginas relacionadas aos artigos ficarão dentro de um *app* específico, assim como as páginas relacionadas aos tutoriais e as demais.

Etapa 8) **Criação dos bancos de dados**

Após todas as etapas supramencionadas, a última etapa necessária para o início da programação *back-end* da aplicação foi a criação dos bancos de dados SQLite (para os ambientes de desenvolvimento e de homologação) e a criação do banco de dados PostgreSQL (para o ambiente de produção).

Etapa 9) **Estudo sobre a acessibilidade e sobre a responsividade**

Para o início do desenvolvimento *front-end* das páginas da aplicação, o estudo sobre a inserção da acessibilidade na estruturação das páginas foi o primeiro passo. Com isso, foram realizados os estudos sobre a semântica que o HTML5 proporciona, através das suas tags de marcação com significado. Ademais, também foram estudados os tipos de leitores de telas e como utilizá-los para navegar em páginas web. Já o segundo passo para o desenvolvimento das páginas, tratou de realizar estudos sobre a inserção da responsividade no design. Com isso, foram realizados os estudos sobre *mobile first* e *media queries*.

Outrossim, foram feitas pesquisas acerca das recomendações descritas nas Diretrizes de Acessibilidade para Conteúdo Web (WCAG, versão 2.1), definidas pela *World Wide Web Consortium* (W3C), as quais foram utilizadas como modelos de desenvolvimento das páginas da *Cyber Security Information.*

Etapa 10) **Criação dos designs no Figma (*mobile* e *desktop*)**

Dada a realização dos estudos sobre a acessibilidade web, a próxima etapa consistiu na criação do design de cada página da aplicação web e, para isso, a plataforma de design Figma foi utilizada como o ambiente de design.

Etapa 11) **Estudo sobre a segurança cibernética**

Visando a produção de conteúdos informacionais acerca da Cibersegurança, nessa etapa foi realizada uma pesquisa aprofundada sobre Segurança da Informação aplicada à Segurança Cibernética, de modo a obter conhecimento e fundamentação teórica para a produção de artigos, tutoriais e ferramentas.

Etapa 12) **Produção de artigos, tutoriais e ferramentas**

Uma vez realizada a etapa anterior, a próxima etapa tratou da produção dos artigos, tutoriais e ferramentas, os quais serão disponibilizados em diversos tipos de mídias na aplicação web.

Etapa 13) **Realização de testes e publicação**

Nessa etapa, os responsáveis pelo ambiente de homologação ficam encarregados de validar todas as implementações na aplicação antes da publicação destas no ambiente de produção, o que inclui a verificação das páginas desenvolvidas nas plataformas que validam a conformidade da aplicação com as Diretrizes de Acessibilidade para Conteúdo Web (WCAG), tal como o *AccessMonitor*, o *Google Lighthouse*, o ASES (Avaliador e Simulador de Acessibilidade em Sítios) e o *Color Contrast Accessibility Validator* (Validador de Acessibilidade de Contraste de Cor). Após a realização dos testes, as funcionalidades implementadas na aplicação, se forem aprovadas, serão disponibilizadas para os usuários finais.

Além disso, nesta etapa seriam realizados os testes de segurança da aplicação web, todavia, devido à limitação de tempo - decorrente da necessidade de produzir os materiais teóricos e práticos de forma simultânea à produção do sistema - não foi possível implementar tais verificações.

3. RESULTADOS E DISCUSSÃO

A priori, com base nos objetivos e na metodologia deste projeto, a aplicação *web* “Cyber Security Information” foi desenvolvida e disponibilizada publicamente através da URL https://www.ciberseguranca.info/ e, para detalhar os resultados

obtidos neste trabalho, os seguintes tópicos estão vinculados ao levantamento de requisitos, etapa 3 da criação da referida aplicação. Além do mais, vale frisar que o código-fonte está disponível através deste repositório.

3.1. Aplicação *web*

3.1.1. Garantia da acessibilidade nas páginas

De acordo com a metodologia do projeto, o desenvolvimento das páginas da CSI está fundamentado na acessibilidade *web*, uma vez que há, na estrutura do HTML, mecanismos que garantem tal aspecto do site, como as *tags* semânticas, atributos para leitores de tela etc. Dessa maneira, as pessoas que são portadoras de alguma deficiência conseguem ter acesso aos conteúdos que estão disponibilizados, algo que democratiza não só o acesso à internet, como também o acesso aos conteúdos relacionados à cibersegurança.

Nesse viés, foram realizados testes de acessibilidade em importantes ferramentas especializadas nesta área, todas elas gratuitas, de modo que foram obtidos excelentes resultados. Tais resultados comprovam a atenção especial para o tema de inclusão digital neste trabalho, uma vez que cada parte da aplicação web está fundamentada na acessibilidade.

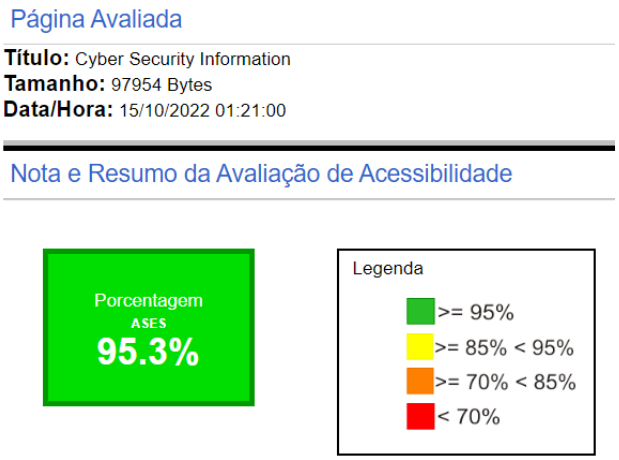
Sendo assim, conforme demonstra a Figura 2, a plataforma do governo português, chamada de *AccessMonitor*, fez uma varredura na página inicial da CSI e a classificou com a nota 9.4 de 10, tendo encontrado apenas duas práticas não recomendáveis.

Figura 2 - Teste de acessibilidade na ferramenta *AccessMonitor*

Fonte: Os autores (2022)

Outrossim, a ferramenta do governo digital brasileiro, chamada de ASES (Avaliador e Simulador de Acessibilidade em Sítios), classificou a mesma página como sendo 95.3% adepta aos padrões de acessibilidade web, conforme demonstra a Figura 3.

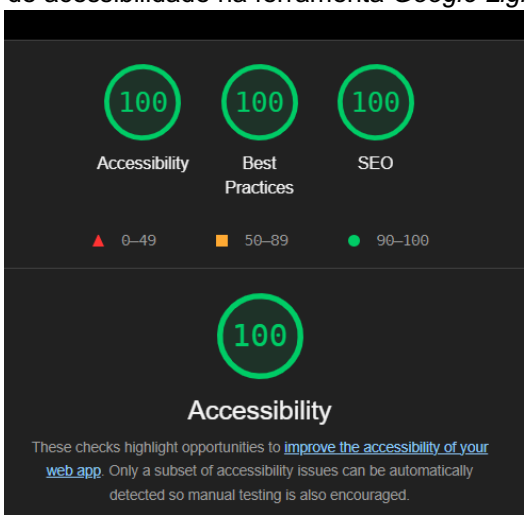
Figura 3 - Teste de acessibilidade na ferramenta ASES



Fonte: Os autores (2022)

Ademais, a ferramenta *Google Lighthouse* catalogou essa página como 100% fiel aos padrões de acessibilidade, não encontrando nenhuma prática não recomendada. Tal classificação está exposta na Figura 4.

Figura 4 - Teste de acessibilidade na ferramenta *Google Lighthouse*

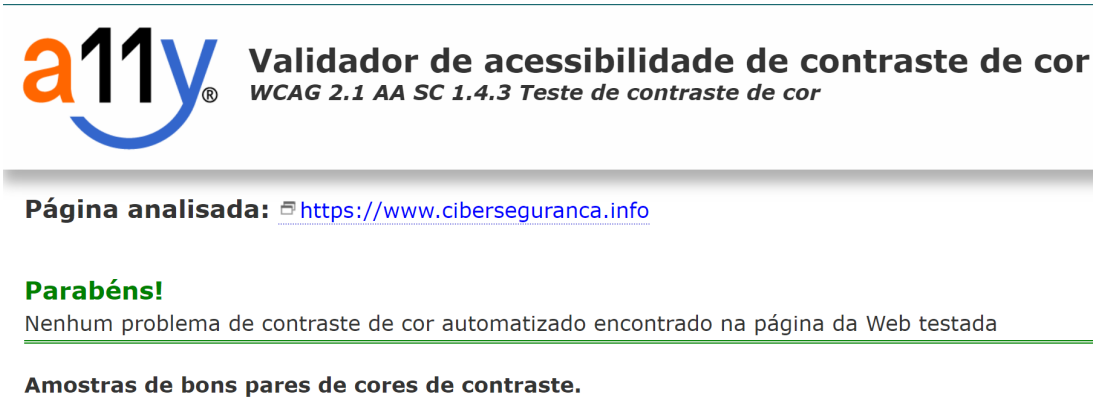


Fonte: Os autores (2022)

Além disso, para averiguar as cores utilizadas nessa página inicial - as quais foram repetidas em todas as outras -, foi empregada a plataforma Color Contrast Accessibility Validator (Validador de Acessibilidade de Contraste de Cor), a qual não

identificou nenhum empecilho acerca dos contrastes utilizados, conforme a Figura 5 descreve.

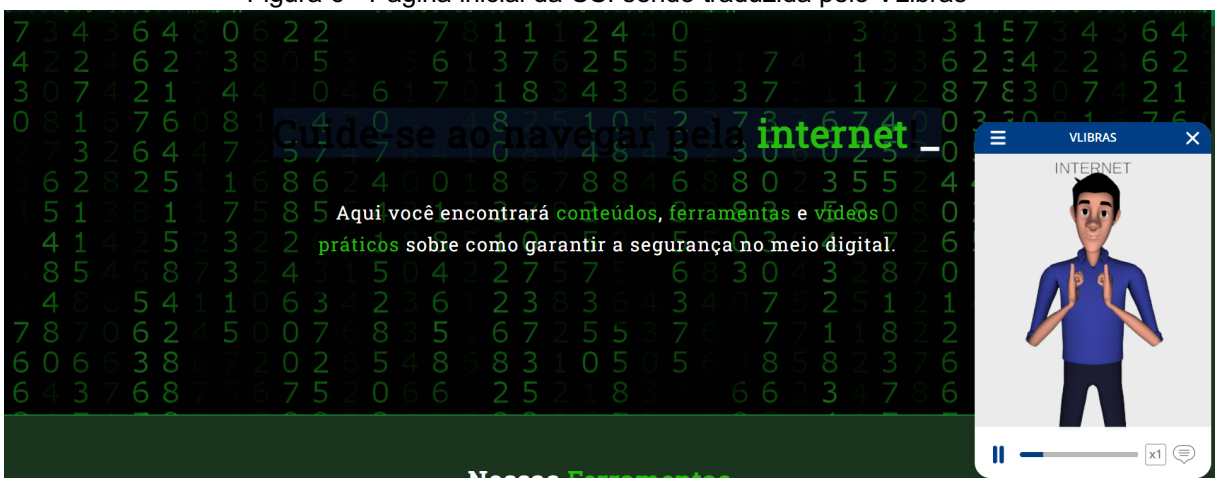
Figura 5 - Teste de acessibilidade das cores na ferramenta Color Contrast Accessibility Validator



Fonte: Os autores (2022)

Finalmente, no que se refere à utilização de tecnologias externas para ampliar a inclusão digital na aplicação, foi empregada, em todas as páginas, a ferramenta VLibras, do governo digital brasileiro, a qual é responsável por dar assistência às pessoas com dificuldades auditivas, convertendo o conteúdo das páginas para a Língua Brasileira de Sinais (LIBRAS). Tal tecnologia assistiva está demonstrada na Figura 6 e seu ícone aparece em todas as demais figuras expositivas da aplicação (Figuras 7, 8, 9 e 10).

Figura 6 - Página inicial da CSI sendo traduzida pelo VLibras



Fonte: Os autores (2022)

3.1.2. Disponibilização de artigos

No tocante à disponibilização de artigos sobre a segurança cibernética, tal projeto cumpriu esse requisito funcional, haja vista que, dentro do item “Artigos”, no cabeçalho das páginas, encontram-se três principais artigos sobre o tema, além de um *link* para a página que contém todos os artigos já publicados.

Com isso, a página expositiva de cada artigo possui, além do conteúdo escrito, os seguintes componentes: caminho do artigo, capa, data da publicação, tempo de leitura em minutos, botões para compartilhamento nas principais redes sociais (Instagram, Linkedin e Facebook), botão para *download* da página e sugestões de leitura com base no artigo atual, conforme demonstra a figura a seguir.

Figura 7 - Artigo sobre o que é a cibersegurança

Fonte: Os autores (2022)

3.1.3. Disponibilização de tutoriais

Acerca da disponibilização de tutoriais com exemplos práticos para a aplicação dos conteúdos dos artigos, este trabalho cumpriu esse requisito. Isso devido ao fato de que foram desenvolvidas três páginas relacionadas aos tutoriais, sendo elas: a própria página do tutorial, a página das categorias dos tutoriais e a página que expõe todos os tutoriais já publicados no site.

Sobre a página do tutorial, ela contém todos os componentes da página expositiva dos artigos, com adição do tempo de vídeo e dos tutoriais relacionados.

Figura 8 - Tutorial sobre como instalar um bloqueador de anúncios no Google Chrome

Fonte: Os autores (2022)

3.1.4. Disponibilização de ferramentas para proteção

No que tange à disponibilização de ferramentas voltadas à cibersegurança, esse requisito funcional foi atingido. Tal realização se dá pelo fato de que foram desenvolvidas páginas para as ferramentas, as quais estão disponíveis no cabeçalho da aplicação através do item “Ferramentas”.

Uma das ferramentas trata-se de um gerador de senhas, desenvolvido em *JavaScript*, capaz de gerar senhas pseudo-aleatórias com caracteres alfabéticos, caracteres numéricos e caracteres especiais (conforme demonstra a Figura 9).

Figura 9 - Página do gerador de senhas

Fonte: Os autores (2022)

Ademais, outra ferramenta que se encontra disponível na aplicação é o *software mobile* “Digital Authenticator”, o qual foi desenvolvido - pela mesma equipe em um projetor anterior - por meio da tecnologia de programação em blocos, com o

auxílio da plataforma *Kodular*, cuja finalidade é o armazenamento seguro de informações confidenciais dos usuários, como as senhas, por exemplo. Esse armazenamento ocorre por meio da criptografia *AES-128*, isto é, toda vez que o usuário cadastra alguma informação no aplicativo, ela é criptografada e armazenada no banco de dados local, *TinyDB*, algo que torna esses dados mais seguros - é válido destacar que o algoritmo AES só foi utilizado devido à limitação do *Kodular* no que tange ao uso de *hashes* (algoritmos ainda mais seguros). Além do mais, há a utilização da autenticação em duas etapas, por meio da biometria do usuário (digital) e da senha do aplicativo. A Figura 10 apresenta a página em que se encontra a aplicação desenvolvida.

Figura 10 - Página do *software mobile* “Digital Authenticator”

Fonte: Os autores (2022)

3.1.5. Envio de e-mails

Para o compartilhamento de notificações acerca das novas publicações, foi desenvolvido um código personalizado para o envio de e-mails quando há a postagem de novos tutoriais, de novos artigos ou de novas ferramentas. Nesse sentido, os usuários que sentirem vontade, podem cadastrar os seus e-mails através da página “Newsletter” e, diariamente, desde que haja uma nova publicação na aplicação web, receberão e-mails contendo as informações dos conteúdos postados, o que inclui: resumo sobre o artigo, sobre a ferramenta ou sobre o tutorial postado, imagem de capa do tutorial e/ou do artigo, *link* para acesso específico para cada publicação e *link* geral da aplicação.

3.1.6. Disponibilização de um canal de contato

Em consentimento com o requisito de disponibilização de um meio para contato, na aplicação *web* há a página denominada “Fale Conosco”. Assim, tal página possibilita que o usuário envie uma mensagem, podendo ser uma reclamação, uma sugestão, uma dúvida ou um reporte de erros. Nesse viés, a mensagem que o usuário enviar, por meio deste formulário, chegará no e-mail de suporte da aplicação, ou seja, no e-mail em que os responsáveis do site têm acesso e, por conseguinte, respondem as mensagens recebidas.

3.1.7. Inclusão de métodos de segurança

Em consenso com os objetivos e com a segunda etapa de desenvolvimento deste projeto, critérios básicos de segurança foram abrangidos, tais como: utilização de certificado TLS/SSL e do protocolo HTTPS, criação do arquivo .gitignore para evitar que informações sigilosas fiquem disponíveis no repositório público do projeto, adição de CSRF tokens nos formulários (página da *newsletter* e página de contato), criação do arquivo robots.txt (https://www.ciberseguranca.info/robots.txt) para evitar que páginas confidenciais (e outras páginas desnecessárias) apareçam nas pesquisas, configuração de backups rotineiros e outras ações, como a preferência por não utilizar cookies que violem a privacidade dos usuários.

3.2. Discussão

Com o avanço da tecnologia, sobretudo da Internet, as informações passaram a estar presentes no meio virtual com bastante intensidade e, a partir disso, Fontes (2008) afirma que a Segurança nesse meio é um tema que tem ganhado atenção no cotidiano da sociedade. Assim, é importante que a comunidade reconheça o quanto a Cibersegurança é imprescindível, em concordância com Hintzbergen *et al.* (2018), para a proteção dos dados que se encontram no ambiente computacional. Dessa forma, para que as pessoas saibam o que é, de fato, essa temática, além de como colocá-la em prática nas atividades rotineiras, o desenvolvimento das tecnologias apresentadas neste artigo é fundamental, uma vez que as pessoas terão acesso aos conteúdos atrelados a esse assunto [segurança cibernética], além da fácil utilização de ferramentas e materiais que auxiliarão na proteção da comunidade.

Sob essa ótica, vale ressaltar que, a partir dos resultados obtidos neste projeto, ficou claro a importância da Segurança Cibernética e o quanto ainda há muito a se fazer para democratizar tal assunto. Nesse sentido, conforme estabelecido como objetivo principal deste trabalho, a aplicação *Cyber Security Information* foi desenvolvida para contribuir para a inclusão digital, no que diz respeito à democratização da informação, especialmente acerca da cibersegurança. Sendo assim, é válido discutir a relevância deste trabalho.

No que se refere à contribuição da tecnologia desenvolvida para a coletivização de conteúdos acessíveis sobre a cibersegurança, é notório que, com a produção, a disponibilização e a constante atualização dos materiais teóricos, particularmente dos artigos, nota-se que um grande público poderá acessar, entender e compartilhar importantes termos e conceitos sobre o tema. Nesse viés, a CSI disponibiliza esses materiais de maneira acessível, a partir da leitura simples, do acesso facilitado e da gratuidade de tais materiais, além da possibilidade de leitura em diferentes dispositivos eletrônicos e da possibilidade de *download*.

Em contrapartida, é notória a necessidade de difundir, ainda mais, outras ferramentas que assegurem ao máximo a proteção das pessoas na internet. Isso devido ao fato de que, por meio deste trabalho, não foi possível (e nem seria) suprir toda a carência da população mais vulnerável quanto à posse de aparatos tecnológicos gratuitos, de fácil acesso e entendimento e, sobretudo, acessíveis.

4. CONCLUSÕES

A priori, o desenvolvimento do presente projeto possibilitou uma análise acerca da importância das ferramentas que possuem a acessibilidade como sendo um pilar, haja vista que tal ação possibilita a ampliação da área de impacto desses aparatos tecnológicos, sobretudo para os públicos mais vulneráveis, o que, em outras palavras, viabiliza a democratização do acesso aos conteúdos presentes nessas ferramentas.

Além disso, a construção da aplicação web *Cyber Security Information*, a qual é resultado desta pesquisa, viabilizou o estudo dos impactos da Segurança Cibernética no mundo contemporâneo, uma vez que a sua concepção partiu da constatação da carência global de uma maior proteção na internet. Nesse viés, tal

aplicação web foi criada para colaborar com a disseminação de conteúdos pertinentes a este tema.

Sob essa ótica, ao unir o desenvolvimento web semântico e acessível ao compartilhamento de informações e tecnologias acerca da cibersegurança, este projeto foi capaz de demonstrar o quanto a tecnologia pode democratizar temas elitizados, tal qual a segurança na internet, por meio de ferramentas que permitem que os seus usuários possam acessar, entender e compartilhar as informações, sem que necessitem de um conhecimento prévio ou de uma determinada característica física.

Sendo assim, por meio da utilização de ferramentas assistivas, da escrita semântica das páginas HTML, da escrita simplificada dos artigos teóricos, da disponibilização dos tutoriais em diversos formatos - vídeos, imagens e textos - e, sobretudo, do oferecimento gratuito de tal tecnologia, a *Cyber Security Information* colabora para a coletivização da cibersegurança aos seus usuários, sejam eles jovens, adultos, pessoas portadoras de deficiências ou quaisquer pessoas imperitas no assunto.

Outrossim, constata-se que este projeto, além de contribuir para a ampliação do tema, colabora para a melhoria da segurança dos seus usuários frente aos inúmeros ataques cibernéticos no mundo digital, tendo em vista que concede diversos materiais didáticos e práticos para a efetivação de tal proteção.

Finalmente, como a CSI disponibiliza publicamente seu código-fonte, torna-se viável a ampliação do seu alcance, além do seu contínuo melhoramento, por qualquer pessoa que deseje isso, o que oportuniza, acima de tudo, a incessante realização da inclusão digital. Além disso, sua infraestrutura atual suporta a inclusão de centenas de conteúdos.

5. REFERÊNCIAS

ANDRADE, Henrique. Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar. **CNN Brasil.** São Paulo, 10 dez. 2021. Disponível em: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/. Acesso em: 20 ago. 2022.

BRASIL. Gabinete de Segurança Institucional. Portaria nº 93, de 18 de outubro de 2021. **Glossário de Segurança da Informação**. Diário Oficial da União. Brasília, DF, Edição: 198 | Seção: 1 | Página: 36. Disponível em:

https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=19/10/2021&jornal=515&pagina=36. Acesso em: 30 jul. 2022.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. **VLibras**. Brasília, 2019. Disponível em: https://www.gov.br/governodigital/pt-br/transformacao-digital/ferramentas/vlibras Acesso em: 20 jun. 2022.

CHARÃO, Júlia. **Os crimes cibernéticos na legislação brasileira e os procedimentos de investigação**. Orientador: Cristiano Cuozzo Marconatto. 2017. 63 f. TCC (Graduação em Direito). Universidade de Santa Cruz do Sul. Santa Cruz do Sul, 2017. Disponível em: http://hdl.handle.net/11624/1984. Acesso em: 30 jul. 2022.

CURY, Lucilene; CAPOBIANCO, Ligia. Princípios da história das tecnologias da informação e comunicação grandes invenções. **VIII Encontro Nacional de História da Mídia. Anais... Guarapuava: Unicentro**, p. 1-13, 2011. Disponível em: http://www.ufrgs.br/alcar/encontros-nacionais-1/8o-encontro-2011-1/artigos/Principios%20da%20Historia%20das%20Tecnologias%20da%20Informacao%20e%20Comunicacao%202013%20Grandes%20Invencoes.pdf. Acesso em: 30 jul. 2022.

CUSIN, C. A.; VIDOTTI, S. A. B. G. Inclusão digital via acessibilidade web | Digital inclusion via web accessibility. **Liinc em Revista**, [S. l.], v. 5, n. 1, p. 45-65, 2009. DOI: 10.18617/liinc.v5i1.297. Disponível em: https://revista.ibict.br/liinc/article/view/3189. Acesso em: 30 jul. 2022.

FONTES, Edison. **Praticando a segurança da informação**. Brasport, 2008. Acesso em: 30 jul. 2022.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Brasport, 2018. Acesso em: 30 jul. 2022.

MACIEL, Ariane Durce. O lugar das mulheres: Gênero e inclusão digital. **P2P e inovação**, v. 2, n. 1, p. 66-85, 2015. Disponível em: https://revista.ibict.br/p2p/article/view/1450. Acesso em: 30 jul. 2022.

MOHURLE, Savita; PATIL, Manisha. A brief study of wannacry threat: Ransomware attack 2017. **International Journal of Advanced Research in Computer Science**, v. 8, n. 5, p. 1938-1940, 2017. Acesso em: 10 mai. 2022.

SILVA, Diego Pereira da et al. AACVOX: mobile application for augmentative alternative communication to help people with speech disorder and motor impairment. **Research on Biomedical Engineering**, v. 34, p. 166-175, 2018.