INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO - CAMPUS SÃO PAULO PIRITUBA

ANNA BEATRIZ SANTOS E SOUZA, HILLARY MENDES MOREIRA, RAPHAELA GUILAND FERRAZ E VICTOR GABRIEL MARQUES

Desenvolvimento de uma aplicação web para divulgação de conteúdos e ferramentas acerca da cibersegurança

SÃO PAULO
2022

ANNA BEATRIZ SANTOS E SOUZA, HILLARY MENDES MOREIRA,
RAPHAELA GUILAND FERRAZ E VICTOR GABRIEL MARQUES

Desenvolvimento de uma aplicação web para divulgação de conteúdos e ferramentas acerca da cibersegurança

Projeto de Pesquisa Acadêmica apresentado ao curso Técnico em Redes de Computadores Integrado ao Ensino Médio do Instituto Federal de São Paulo - Câmpus Pirituba.

Orientador: Prof. Me. Adriano Jose Ferruzzi
Co-orientador: Prof. Me. Regivaldo Sousa Ferreira

SÃO PAULO
2022

Sumário

1. Introdução

Em 1946, conforme relatado por Maciel (2015), o primeiro computador digital eletrônico de grande escala era apresentado, o ENIAC (*Electronic Numerical Integrator and Computer*). Esse computador tinha o peso igual a 30 toneladas e ocupava 180 metros quadrados (MACIEL, 2015). 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.

Por consequência, é exatamente na década de 1980 que estão datados os primeiros ataques cibernéticos dos quais temos conhecimento. Charão (2017), expõe que, em 1982, Richard Skrenta, com apenas quinze anos de idade, desenvolveu o Elk Cloner, um vírus que tinha como objetivo contaminar computadores e que se difundia a partir de cópias de disquetes que já estavam infectados. Outrossim, Ribeiro e Albuquerque (2014) relatam que, ainda nos anos 80, o primeiro *worm* conhecido foi criado pelo estudante Robert T. Morris, chamado de Morris Worm. Esse *worm* infectou, segundo Serge Malenkovich (2013), "[...] cerca de 10% dos computadores conectados à internet na época", sendo semelhante ao que hoje conhecemos como um tipo de *DoS* (ataque de negação de serviço), uma vez que o *worm* se replicava inúmeras vezes num mesmo computador, deixando o sistema inoperante.

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. A título de exemplificação, a empresa holandesa de cibersegurança *Surfshark* estimou que, no ano de 2021, 1 em cada 5 pessoas em todo o mundo teve seus dados vazados, conforme publicado por Filipe Prado na revista IstoÉ (2021). Além disso, em fevereiro de 2022, segundo um levantamento da Serasa Experian (2021), 326.290 brasileiros foram alvos de tentativas de golpes - o que equivale a dizer que a cada 8 segundos um brasileiro foi vítima de golpistas.

Com a crescente onda dos crimes cibernéticos, criou-se um ramo de estudos, dentro da segurança da informação, relacionado a esses ataques. Esse ramo de estudos é a Cibersegurança ou, em inglês "*Cybersecurtiy*" ou "*Cyber security*", que, de acordo com a Oxford University Press (2014), consiste no estado de proteção contra o uso criminoso

ou não autorizado de dados eletrônicos, ou as medidas tomadas para isso (Apud Craigen et al, 2014).

Dessa maneira, é de extrema importância 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 uma ausência da democratização do acesso à informações relacionadas a esse tema, o que resulta em um grande número de pessoas desinformadas, principalmente crianças e idosos. Citando um caso análogo, o pesquisador de segurança sênior da Kaspersky, Fabio Assolini (2020), apontou, em uma notícia da empresa, que os idosos são, para os criminosos digitais, um grupo vulnerável e altamente lucrativo.

Nessa direção, o projeto propõe a criação de uma aplicação web que divulgará artigos, tutoriais e ferramentas que auxiliarão os usuários na garantia da segurança dos seus dados é imprescindível, uma vez que todas as pessoas, independente da idade, escolaridade ou conhecimento sobre a Segurança da Informação e Tecnologia da Informação, terão acesso a materiais de altíssima qualidade, criados de modo a garantir a democratização do acesso a conteúdos relacionados ao tema [cibersegurança].

Ademais, entre as ferramentas que serão expostas na aplicação, o projeto propõe que, com o objetivo de fortalecer a segurança dos usuários, seja disponibilizado um aplicativo *mobile*, para o sistema operacional Android, que seja capaz de armazenar, de maneira segura e confidencial, dados sigilosos dos usuários.

Dessa maneira, a aplicação *web* é composta pelas seguintes tecnologias: linguagem de marcação HTML5, linguagem de estilização CSS3 e as linguagens de programação JavaScript e Python (com o auxílio do *framework* Django). Em paralelo, o aplicativo *mobile* é composto pela tecnologia de programação em blocos, com o auxílio da plataforma Kodular, além do banco de dados em tempo real disponibilizado pelo Google Firebase.

Outrossim, o projeto está desenvolvido com preceitos na literatura como artigos relacionados à Segurança da Informação, Segurança Cibernética, Tecnologia da Informação e Acessibilidade na *Web*, além de livros e revistas também relacionados ao tema.

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 – tal como um *software mobile* para o armazenamento de informações confidenciais –, tendo em vista a democratização do acesso aos conteúdos que tratam sobre o tema.

1.1.2 Objetivos Específicos

- Realizar o levantamento de requisitos da aplicação *web*;
- 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 todos 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;
- Disponibilizar, entre as ferramentas, um *software mobile* que servirá como gerenciador de informações confidenciais dos usuários;
- Estudar sobre acessibilidade na *web*, visando o desenvolvimento semântico da aplicação, de modo que pessoas com 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, sobretudo crianças, adolescentes e idosos, 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 acessível a todos os públicos.

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 “Wanna Cry”, 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 "Wanna Cry", 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 o 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 alguma deficiência.

2. Revisão de Literatura

2.1 Acessibilidade

2.1.1 Acessibilidade Web

O avanço da tecnologia proporciona às pessoas o acesso a uma gama de websites e, dessa forma, é imprescindível que esses sites não tenham barreiras de acesso para as pessoas que possuem deficiência ou para aquelas que não possuem deficiência. Assim, é de extrema importância a garantia da acessibilidade em websites e, conforme a Cartilha de Acessibilidade na Web do W3C Brasil - Fascículo I (2014), a acessibilidade Web trata-se da possibilidade e a condição de percepção, alcance e entendimento, para uma utilização, com igualdade de oportunidades, de segurança e de autonomia, de sites e ferramentas que estão disponíveis na Web. Isso é reforçado, também, por Cusin e Vidotti (2009), que dizem que a acessibilidade Web é a capacidade e a garantia que as pessoas com deficiência têm de entender, interagir e navegar na Web, podendo contribuir com o mundo virtual.

Ademais, segundo a W3C WAI (2005), a acessibilidade Web proporciona uma variedade de benefícios para pessoas que não são portadoras de deficiência, sendo essas as pessoas idosas, que estão com suas habilidades em mudança devido ao envelhecimento, e as pessoas com “deficiências temporárias”, como àquelas que estão com um braço quebrado ou com os óculos perdidos. Ainda segundo a W3C WAI, a acessibilidade Web é benéfica, também, para pessoas que se encontram em situações diversas do cotidiano, como: pessoas que estão sob intensa luz solar e que precisam de um site que possua um bom contraste e tamanho de fontes; pessoas que estão em um ambiente que não se pode ouvir um áudio e que precisam de um recurso textual do conteúdo do site; ou pessoas que possuem uma conexão lenta com a Internet, a qual necessita de um site otimizado e bem estruturado para se ter um melhor rendimento.

Além dessas propriedades, a acessibilidade Web possibilita a natureza colaborativa que a Web possui, uma vez que todas as pessoas, independente de suas condições intelectuais, físicas e educacionais, podem ter acesso aos conteúdos que são oferecidos na Web e podem, também, fornecer conteúdos de própria autoria. Cusin e Vidotti (2009), afirmam que a acessibilidade Web é um fator que propulsiona as inclusões

informacional e digital, dado que há a presença de uma igualdade de acesso aos usuários, sejam esses portadores de deficiência ou não.

Outrossim, a acessibilidade em websites permite que pessoas deficientes possam realizar atividades simples do cotidiano, como consumir conteúdos informacionais que são disponibilizados na internet. De acordo com a Cartilha de Acessibilidade na Web do W3C Brasil - Fascículo II (2016), um site que não possui recursos de acessibilidade, faz com que pessoas com deficiência ou com mobilidade reduzida não consigam realizar uma pesquisa acadêmica, por exemplo, dado que as informações que estão presentes em um website sem acessibilidade não poderiam ser consumidas ou interpretadas por esses indivíduos, uma vez que podem utilizar as tecnologias assistivas, leitores de telas, ou podem realizar a navegação por teclado.

Há ferramentas que auxiliam a garantia da acessibilidade de sites para os usuários, de acordo com as suas necessidades. Em conformidade com a Cartilha de Acessibilidade na Web do W3C Brasil - Fascículo II (2016), há pessoas que são surdas ou que possuem uma deficiência auditiva e acessam as informações em áudio e vídeo com legendas, descrições e tradução em LIBRAS, dessa forma, é possível implementar um tradutor, através de plugins ou softwares, de conteúdos digitais em Português para Libras. Ainda de acordo com a Cartilha, há pessoas que acessam websites por dispositivos móveis, que possuem telas e teclados de tamanho reduzido, além de uma capacidade de processamento e armazenamento menor, dessa maneira, é possível implementar códigos de estilização - CSS - que garantam a responsividade do site. A Cartilha também expõe que há pessoas que possuem deficiência motora e mobilidade reduzida e, para navegar na Web, utilizam o teclado e, com isso, é necessária a implementação de um código de marcação do site - o HTML - semântico.

2.1.2 Acessibilidade Web em Dispositivos Móveis

A acessibilidade Web, quando garantida, pode alcançar outros tipos de benefícios para os diversos usuários existentes na Web e, um desses benefícios é a acessibilidade Web em dispositivos móveis. Para Oliveira e Silva Neto (2019), a acessibilidade Web mobile é entendida como a inclusão de usuários ao acesso de conteúdos, disponibilizados na Web, através da utilização de dispositivos móveis, como smartphones, tablets e outros.

De acordo com a pesquisa TIC de Domicílios (2020), realizada pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), os dispositivos móveis são os principais

tipos de dispositivos utilizados para acessar a Web, representando quase o total da população usuária de Internet com dez anos ou mais (99%). Com isso, é primordial a utilização de metodologias do desenvolvimento Web que garantam o acesso desses usuários que utilizam telefones celulares, sendo assim, essa acessibilidade mobile pode ser alcançada através da aplicação de atributos do HTML5 e de funções de estilização do CSS3.

2.1.3 Acessibilidade Web e a Inclusão Informacional

Como dito, a acessibilidade Web garante inúmeros benefícios para a comunidade digital e, também, para a educação da comunidade como um todo. A acessibilidade Web, então, garante a inclusão informacional, que, para Cusin e Vidotti (2009) é a habilidade de buscar, usar, acessar e recriar uma informação com responsabilidade social.

Ademais, para que se garanta a inclusão informacional, os conteúdos de cunho informativo devem se adequar a todos os usuários e isso é alcançado, também, pela acessibilidade Web. Através de um site acessível, as informações contidas neste, podem ser acessadas pelos usuários de forma igual, uma vez que um site semântico tem uma eficiência alta com leitores de tela e, de acordo com Silva, Lôbo e Mello (2021), os softwares para leitura de textos e comunicações alternativas, fazem com que as pessoas com deficiência consigam ter acesso ao conteúdo que está sendo oferecido pela Web, seja no ambiente de ensino básico, seja no ambiente de ensino superior.

Diante o exposto, a acessibilidade Web se encontra atrelada à inclusão informacional, algo de extrema importância para a educação dos cidadãos, sobretudo no que diz respeito aos direitos que as pessoas possuem dentro do mundo cibernético. Para Ishiyama e Tanaka (2017), o avanço da Web permite que as pessoas acessem diversos conteúdos na internet, os quais são produzidos de forma livre. Com isso, websites que fornecem conteúdos informacionais e possuem uma acessibilidade garantida, faz com que a educação da sociedade como um todo seja atingida de forma igual e inclusiva, isto é, garantem a inclusão informacional.

2.2 Segurança Cibernética

Segurança Cibernética, ou, em inglês "Cyber Security", de acordo com Craigen, Diakun-Thibault e Purse (2014) é um termo muito utilizado, cujas definições são variáveis e, muitas vezes, subjetivas ou pouco informativas. Nesse sentido, a International

Telecommunication Union, ou em português “União Internacional de Telecomunicações”, caracterizou a Segurança Cibernética como uma:

> [...] coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de risco, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e a organização e os ativos do usuário. Os ativos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e/ou armazenadas no ambiente cibernético. A segurança cibernética se esforça para garantir a obtenção e a manutenção das propriedades de segurança da organização e dos ativos do usuário contra riscos de segurança relevantes no ambiente cibernético. (ITU-T, 2008, p.2)

Além dessa definição, neste projeto será utilizado o conceito de Segurança Cibernética, mencionada ao longo deste trabalho como Cibersegurança, estabelecido pela Oxford University Press (2014), que caracteriza-a como um estado de proteção contra o uso criminoso ou não autorizado de dados eletrônicos, ou as medidas tomadas para isso (Apud Craigen et al, 2014).

Outrossim, considera-se importante para esse projeto a diferenciação entre Segurança da Informação e Cibersegurança. Nesse sentido, a Segurança da Informação, conforme explicitado por Hintzbergen et al. (2018), trata-se da preservação da Confidencialidade, Integridade e Disponibilidade da Informação. Nessa direção, entende-se que a área de atuação da Segurança da Informação é ampla, o que se diferencia da área de atuação da Segurança Cibernética que, como informado no parágrafo acima, corresponde apenas à proteção dos dados eletrônicos. Portanto, a Cibersegurança caracteriza-se como uma ramificação da Segurança da Informação.

2.2.1 Crimes Cibernéticos

De acordo com Wendt e Jorge (2013), os crimes cibernéticos são delitos praticados contra ou por meio de dispositivos informáticos (computadores, celulares, pendrives, etc). Nessa direção, os autores dividem os crimes cibernéticos em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Essa divisão também é realizada por Almeida et al. (2015), na qual os crimes cibernéticos são divididos em “crimes impróprios" e “crimes próprios”, os quais possuem o mesmo significado da divisão de Wendt e Jorge.

Com isso, os crimes cibernéticos abertos, conforme afirmam Wendt e Jorge (2013), são aqueles que podem ser praticados da maneira tradicional (com ação física) ou por meio de dispositivos informáticos, isto é, os dispositivos são apenas meios opcionais para a realização do delito. Como exemplo desses crimes destacam-se: crimes contra a honra, racismo, tráfico de drogas, estelionato, entre outros. Já os crimes exclusivamente cibernéticos, são aqueles que só podem ser praticados com a utilização de dispositivos informáticos.

Por fim, para a realização deste projeto é de suma relevância a explicitação dos crimes cibernéticos, uma vez que a aplicação web terá conteúdos informacionais sobre como o usuário pode se proteger deles.

2.2.2 Públicos Vulneráveis na Web

Com o avanço da Web e da internet, as informações passaram a estar presentes nesse meio virtual com bastante intensidade e, com isso, Fontes (2008) afirma que a Segurança da Informação é uma temática que tem ganhado espaço no cotidiano da sociedade, uma vez que essas informações estão disponíveis a muitas pessoas, sejam essas pessoas de uma organização, sejam essas pessoas usuárias da Web.

Assim, com a presença da Segurança da Informação no ambiente computacional, há a criação do termo “Vulnerabilidade”, o qual pode ter variações relacionadas ao seu significado. De acordo com Hintzbergen *et al.* (2018), esse termo, vulnerabilidade, significa a fraqueza que um ativo ou controle pode ter e pode, também, ser explorada por ameaças. Peltier (2005) reforça essa definição, dizendo que a fraqueza também pode afetar um bem e que, caso um desses itens - ativo, controle ou bem - sejam de fato explorados por uma ameaça, isso poderá causar algum impacto, seja na organização, seja para um indivíduo.

Dessa forma, o avanço da Web e das tecnologias fazem com que os eventos de vulnerabilidades, ocasionadas, majoritariamente, por ações pessoais, sejam reconhecidos de diversas maneiras e, uma delas, de acordo com Piekarski (2018), é a vulnerabilidade digital.

2.2.2.1 Crianças e Adolescentes

Como as Tecnologias de Informação e Comunicação se difundiram na sociedade, as crianças e adolescentes são um público alvo que, segundo Ferraz (2019), possuem um grande interesse pela utilização dos recursos que esses meios digitais oferecem. Diante

disso, a inserção massiva das TICs e de mídias sociais, fizeram com que, de acordo com Couto (2013), as crianças passassem a estar cada vez mais conectadas e imersas nesse cibermundo e, com isso, o referido autor também aponta a criação de uma cibercultura infantil, a qual é definida como uma maneira de comportamento, de socialização e de troca de informações realizadas por crianças pela internet. Assim, esse público alvo estão, também, propensos às vulnerabilidades digitais.

Com essa faixa etária de pessoas que se encontram cada vez mais conectadas, Ferraz (2019) aponta que as crianças desenvolvem suas habilidades com a tecnologia de forma rápida, fazendo com que elas entendam que esse ambiente virtual é um ambiente as quais estão fisicamente inacessíveis, além de terem uma liberdade maior de se comunicaram e de se expressarem.

Além das crianças, os adolescentes também se encontram em vulnerabilidade no mundo virtual. A Pesquisa Nacional por Amostras de Domicílios (PNAD), realizada em 2015, demonstra que adolescentes que estão nas faixas etárias de 15 a 17 anos e de 18 a 19 anos, são os indivíduos que mais acessam a internet, o que equivale, respectivamente, a 82% e 82,9%.

Os adolescentes, assim como as crianças, também veem a utilização dos recursos proporcionados pelas tecnologias como algo benéfico e, de acordo com Ferreira *et al.* (2020), as vantagens principais que os adolescentes reconhecem das tecnologias são a rapidez, a economia, a capacidade de conhecer pessoas e de aumentar o número de amigos.

A TIC Kids Online Brasil de 2019 aponta que a utilização de mídias digitais - recurso tecnológico que é proveniente das Tecnologias de Informação e Comunicação - por crianças e adolescentes é algo excessivo e problemático, dado que essas faixas etárias estão submetidas aos diversos riscos que o mundo digital possui.

Diante os expostos, Basile e Lopez (2020) expõem que a massiva utilização das tecnologias de informação aumenta a relevância do estudo sobre a defesa no mundo virtual. Ademais, há medidas que podem ser tomadas para a preservação e para a integridade das crianças e adolescentes, há, também, princípios, direitos e deveres para o uso da Internet no Brasil, as quais se encontram na Lei n° 12.965 de 23 de abril de 2014 - O Marco Civil da Internet.

2.2.2.2 Idosos

A tecnologia tornou-se o principal meio de comunicação e de informação na sociedade contemporânea e, Marioto e Basile (2020), apontam que a chegada dessas tecnologias TICs (Tecnologias de Informação e Comunicação) alteraram, significativamente, os modos de ser, estar, agir e interagir na sociedade, isto é, para se conviver no corpo social moderno, é necessário ter acesso ao conhecimento tecnológico.

Dessa maneira, Marioto e Basile (2020), apontam, também, que os idosos, pessoas com mais de 60 anos de idade, constituem um grupo da sociedade que possuem especificidades no que se refere à inserção social realizada por meio da tecnologia. Assim, para que esse público da Terceira Idade não seja excluído das atividades sociais realizadas por intermédio da tecnologia e que não tenha sua qualidade de vida omitida pela falta de conhecimento dos aparatos tecnológicos, os autores afirmam que é de suma relevância o desenvolvimento de atividades de ensino e aprendizagem, as quais atendam as especificidades desse grupo. Essas atividades de ensino e aprendizagem podem ser realizadas, com, por exemplo, a escrita de artigos que serão disponibilizados pelas tecnologias TICs.

A Terceira Idade, de acordo com Barros e Leite (2019), está exposta aos diversos perigos na internet, seja devido a falta de habilidades digitais, seja pelo declínio que essas pessoas estão vivenciando das competências cognitivas. As autoras também demonstram que esses aspectos fazem com que esse grupo se torne mais vulnerável aos golpes virtuais. Por isso, os idosos são vistos por cibercriminosos como alvos fáceis para aplicação de golpes. Isso é reforçado por Machado *et al.* (2019), que aponta que esse grupo de pessoas possuem habilidades e conhecimentos a serem desenvolvidos sobre essa temática.

Assim, as atividades de ensino e aprendizagem, através de artigos digitais, servirão de garantia para que os idosos consigam utilizar de forma segura a internet. A Segurança e Privacidade na Internet, de acordo com Silva (2018), conforme citado por Machado *et al.* (2019), é uma competência de extrema importância para os idosos e, para que eles consigam desenvolver essa competência, esse grupo de pessoas poderão utilizar ferramentas na internet para desenvolver cuidados relacionados ao mundo virtual, evitando o roubo de dados e informações pessoais.

2.3 Tecnologias

2.3.1 Front-End

2.3.1.1 HTML, CSS e JavaScript

Para se desenvolver uma aplicação web, é necessário utilizar linguagens específicas que são responsáveis pela formatação, estilização e dinamicidade dessa aplicação. A partir disso, a linguagem responsável pela marcação de uma página web é a HTML, que significa *HyperText Markup Language*, compreendida em português como Linguagem de Marcação de Hipertexto. O HTML foi criado por Tim Berners-Lee em meados de 1990 (Torres, 2018). De acordo com Flatschart (2011), essa é a principal linguagem utilizada na Web, a qual permite a criação de um documento, que será interpretado pelo navegador, com uma estruturação em parágrafos, títulos, listas, links, formulários e outros diversos elementos. Diante disso, o autor também afirma que o HTML permite a inclusão de outras linguagens no documento, como a linguagem de programação JavaScript. Atualmente, o HTML se encontra na sua quinta versão (HTML5) e conforme Costa e Andrade (2015), o HTML5, através de suas novas tags semânticas e da permissão da incorporação de outras tecnologias - como APIs, trouxe aos usuários uma melhor experiência na utilização da Web e uma possibilidade de garantir, de maneira efetiva, a acessibilidade das páginas disponíveis na internet. Ainda de acordo com os autores, a combinação do HTML5, com o CSS e o JavaScript, essa linguagem de marcação passa a ser multiplataforma, o que aumenta o acesso aos mais diversos tipos de sites.

A linguagem responsável pela estilização das páginas web é a CSS, que significa *Cascading Style Sheets*, compreendido em português como Folha de Estilo em Cascata. O CSS foi criado por Håkon Wium Lie e por Bert Bos em 1994, porém somente em 1996 que a W3C (World Wide Web Consortium) lançou as especificações oficiais da linguagem (EIS, 2006). De acordo com Flatschart (2011), essa é uma linguagem responsável pela estilizações dos conteúdos que serão apresentados aos usuários que acessam o website. Essas estilizações podem ser de *layout,* cores, tipos de fontes e entre outras. Atualmente, o CSS se encontra na sua terceira versão (CSS3), a qual, de acordo com Dhawan (2018), trouxe inúmeras funcionalidades que facilitam o desenvolvimento dos estilos das páginas Web, como: novos tipos de seletores, *pseudo-classes*, novos tipos de declaração de cores (como RGBA, HSL e HSLA).

Já a linguagem de programação responsável pela dinamicidade de sites é o JavaScript, que foi criada em 1995 por Brendan Eich. Essa linguagem também é reconhecida como ECMAScript, denominação dada pela *European Computer Manufacturers Association, ECMA,* em 1997 (AZAUSTRE, 2016). Em conformidade com Flatschart (2011), o JavaScript é classificado como *client side*, isto é, é uma linguagem que está funcionando na máquina em que o usuário está acessando a web. Ainda segundo o autor, essa é a linguagem que possui a responsabilidade direta do comportamento que a página web possui, uma vez que essa tem a capacidade de acessar o DOM (*Document Object Model),* um documento criado pelos navegadores que representa a hierarquia dos elementos que estão do documento HTML. Dessa maneira, o JavaScript consegue modificar os conteúdos e elementos do documento web, além de conseguir realizar validações de formulários - antes que sejam submetidos ao servidor, detecções das propriedades dos navegadores de cada usuário para que, caso seja necessário, esse seja redirecionado para uma página compatível e outras propriedades. Segundo a Ecma International, atualmente estamos na versão ECMA-262, definida em junho de 2021.

2.3.1.2 S.E.O.

A sociedade contemporânea possui como característica marcante a hiperconectividade. Neves *et al.*(2020), afirma que nesse mundo hiperconectado, a informação tem se multiplicado em diversos tipos de telas e, além disso, estão disponíveis em qualquer lugar, a qualquer hora, precisando somente de uma conexão com a internet.

Com isso, as informações e dados que estão na internet são inúmeros, tornando-se necessária a utilização de técnicas eficientes para a melhoria no tratamento e organização desses dados e informações que estão disponíveis na internet (Morais e Ambrósio, 2007). Essa forma de organização e tratamento ocorre devido à presença de Ferramentas de Busca que, de acordo com os autores, são “catálogos de endereços de outros sites que existem na Internet”. Neves *et al.* (2020), afirma que essas Ferramentas de Busca (ou Motores de Busca) possuem a responsabilidade de recuperar todas as informações que estão disponíveis na *World Wide Web (WWW).*

As Ferramentas de Busca podem ser do tipo Mecanismo de Busca, que, de acordo com Morais e Ambrósio (2007), é um conjunto de robôs que realizam rastreamento na Internet em busca de páginas, base de dados e índices e, após eles encontrarem a

página que o usuário pesquisou através, por exemplo, de palavras-chave, eles organizam e armazenam essas páginas encontradas.

A partir disso, pode-se definir que a estratégia de Otimização de Motores de Busca (*Search Engine Optimization - SEO),* conforme Neves *et al*. (2020), é uma maneira de alavancar a visibilidade de um periódico eletrônico, que estão disponíveis na Web, nos Motores de Busca, através das técnicas que são aplicadas à SEO.

Assim sendo, em um *website* é necessário adotar as técnicas de SEO, para que as Ferramentas de Busca e os Mecanismos de Busca possam realizar a indexação corretamente, de modo a alcançar um maior público alvo na Internet. Neves *et al.* (2020), expõe que, através dessas técnicas, o posicionamento de páginas web nos Motores de Busca pode alcançar o primeiro lugar, fazendo com que mais pessoas tenham acesso ao website.

2.3.2 Back-End

2.3.2.1 Python e Django

Para a criação da aplicação web, também são necessárias ferramentas de back-end, tais como a linguagem de programação Python e o *Framework* Django, que juntos são responsáveis pela estruturação do servidor da aplicação, além de serem utilizados em tarefas complementares.

Nessa direção, segundo Borges (2010), a linguagem de programação Python foi desenvolvida por Guido Van Rossum na Holanda, em 1990, no CWI (Centrum Wiskunde & Informatica ou, em português, Instituto Nacional de Pesquisa em Matemática e Ciência da Computação).

Inicialmente, essa linguagem era para ser utilizada por usuários como engenheiros e físicos, todavia, por conta de sua versatilidade, atualmente tem várias finalidades, tais como: automação de processos, desenvolvimento web, aplicações mobile, geoprocessamento, processamento de imagens, robótica, *Data Science*, programação para hardware - Arduíno e Raspberry Pi -, desenvolvimento de jogos, biotecnologia e também no desenvolvimento científico (BORGES, 2010; SILVA e SILVA, 2019).

Além disso, segundo Silva e Silva (2019), Python é uma linguagem de alto nível, dado que a sintaxe é bastante próxima à linguagem humana. Muitos componentes utilizados na linguagem são escritos com a própria palavra (em inglês), como é o caso dos operadores lógicos “e” e “ou”, que de forma pythonica são escritos como: “and” e “or”,

enquanto em outras linguagens, os mesmos operados, são escritos com símbolos ou caracteres especiais, como por exemplo “&&” e “| |”.

Outrossim, o framework utilizado para o desenvolvimento web da aplicação deste projeto é o Django que, segundo Ramos (2018, p.8), é um *framework* “de alto nível, escrito em Python que encoraja o desenvolvimento limpo de aplicações web” (apud Cardoso e Bispo, 2019, p.27). Além disso, conforme citado por Cardoso e Bispo (2019, p.27), o Django tem como objetivo, segundo a Django Software Foundation (2017, p. 5), “tornar tarefas comuns do desenvolvimento Web rápidas e fáceis”.

Nessa direção, o Django apresenta módulos prontos para realizar atividades como: autenticações, manuseio de banco de dados, segurança padrão e desenvolvimento de formulários, com mais agilidade, praticidade e menos codificação, ajudando o programador a desenvolver grandes aplicações e menos tempo (SILVA e SILVA, 2019).

Esse *framework* se baseia no padrão MTV (*Model*, *Template*, *View*). De acordo com Cardoso e Bispo (2019), na camada de *models* do Django estão localizadas as informações necessárias para integrar a aplicação com o banco de dados. Já na camada de *templates*, é construída a interface da aplicação para o usuário final. Por fim, na camada de *views*, em concordância com Ramos (2018), são processadas as requisições dos usuários, que são tratadas através de funções ou classes base do Django, facilitando o desenvolvimento (apud Cardoso e Bispo, 2019, p.29).

Além disso, o Django já fornece para o desenvolvedor toda a estrutura básica de arquivos necessários para o desenvolvimento do site, disponibilizado um arquivo para o modelo (models.py), outro para o controle (views.py), um para administração da base de dados (admin.py), outro para a lógica da aplicação (app.py) e outro para as configurações do projeto (settings.py) (SILVA e SILVA, 2019).

2.3.2.2 SQLite e PostgreSQL

De maneira geral, o “SQLite é uma biblioteca escrita na linguagem C, que implementa um banco de dados e utiliza a linguagem SQL para criar sua estrutura e realizar consultas” Fróes e Weber (2021). Ainda de acordo com Fróes e Weber (2021), o SQLite é considerado um banco de dados portátil e compacto, não necessitando da instalação prévia de um SGBD (Sistema Gerenciador de Banco de Dados).

Já o PostgreSQL, de acordo com Milani (2008), é uma das opções de banco de dados, pois se trata de um servidor SGBD com um amplo potencial, além de ser confiável e competir igualmente com os bancos de dados concorrentes no mercado.

Nesse sentido, o SQLite foi utilizado para servir como banco de dados local da aplicação, isto é, serviu como um banco de dados para a realização de testes. Já o PostgreSQL, por se tratar de um banco de dados mais robusto, serviu como o banco de dados oficial da aplicação, sendo utilizado como armazenamento dos conteúdos da aplicação.

2.4 Artigos Relacionados

Existem diversas metodologias para a criação de uma aplicação web, uma vez que há a possibilidade da utilização de diversas ferramentas e tecnologias. Este trabalho, por sua vez, faz uso das tecnologias supramencionadas, o que caracteriza-o como um projeto de ponta, uma vez que utiliza as mais atuais tecnologias para o desenvolvimento front-end, tal como HTML5 e CSS3, e para o desenvolvimento back-end, tal como Python3 e Django4.

Em relação à semelhança com as técnicas de desenvolvimento front-end para uma aplicação web acessível, Cecílio (2010) realiza o desenvolvimento de uma aplicação utilizando as recomendações da *Web Content Accessibility Guidelines (WCAG)* 1.0 da W3C, através da implementação de funcionalidades que auxiliem o público Portador de Necessidade Especial auditiva e visual. Entretanto, somente a utilização das recomendações da WCAG não é capaz de garantir a acessibilidade web, dado que é necessária a utilização de tags semânticas do HTML5 e de estilizações acessíveis do CSS3. Por isso, o desenvolvimento da aplicação web deste projeto destaca-se por seguir tanto as especificações de acessibilidade fornecidas pela *World Wide Web Consortium* (W3C) e pela *Web Content Accessibility Guidelines (WCAG)* quanto a semântica que o HTML5 proporciona com suas novas tags, além da escrita de uma Folha de Estilo em Cascata - CSS3 - acessível, o que beneficia usuários diversos, sobretudo os usuários que utilizam tecnologias assistivas e/ou que realizam a navegação por teclado.

Além do mais, o desenvolvimento da aplicação web desse projeto se encontra em conformidade com França (2015) no que diz respeito à web responsividade, dado que a presente aplicação possui, em sua essência, a acessibilidade web, o que engloba,

também, a possibilidade da utilização dessa plataforma nos mais diversos dispositivos: *smartphones*, *tablets*, *desktops*, *notebooks* entre outros.

Outrossim, em concordância com Pantofa et al. (2008), o desenvolvimento deste projeto, por prezar a acessibilidade, está fundamentado no entendimento de que os usuários não são iguais, isto é, algumas características dos usuários foram levadas em consideração, tais como: nível de escolaridade, nível de leitura, alfabetização tecnológica, experiência na aplicação, etc.

Além disso, o objetivo desse projeto está em concordância com Oliveira (2019), uma vez que está fundamentado na ideia de que a tecnologia serve como um espaço para democratizar o conhecimento científico. Nesse sentido, a aplicação contribuirá para o acesso a materiais que, mesmo sendo de natureza profundamente técnica, serão legíveis e inteligíveis por uma ampla parcela da população.

Ademais, em assentimento com Cardoso et al. (2019), o desenvolvimento da aplicação faz uso do framework Django por diversos fatores, tais como: maior escalabilidade, gerenciamento claro, testes facilitados e manutenção do código simplificada.

Com isso, durante a revisão bibliográfica desse projeto, foi encontrado um site com um propósito semelhante ao objetivo geral da aplicação web desenvolvida no presente trabalho, o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). Nesse sentido, foi constatado a presença de diversos conteúdos informacionais sobre Segurança Cibernética no site, tais como: cartilhas, guias e recomendações de segurança. Todavia, como a divulgação desses materiais não é o objetivo principal do site, uma vez que o projeto tem como missão o tratamento de incidentes (CERT.br, 2022), nota-se a ausência da acessibilidade no site, o que, em contraposição ao atual projeto, não garante a democratização do acesso às informações disponibilizadas.

3. Método

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

Para o início do desenvolvimento da aplicação web Cyber Security Information, a segmentação das áreas de desenvolvimento em front-end e back-end foi o primeiro passo. Nessa etapa, dois dos integrantes do grupo de autores, Anna Santos e Victor Marques, ficaram responsáveis pelo desenvolvimento back-end da aplicação, enquanto Raphaela Ferraz ficou responsável pelo desenvolvimento front-end da aplicação.

Outrossim, dando continuidade ao projeto realizado em 2021, isto é, o projeto de desenvolvimento de um software mobile para o armazenamento de dados confidenciais, o qual o resultado (aplicativo Digital Authenticator) será exposto na aplicação, dois dos integrantes do grupo, Anna Santos e Victor Marques, ficaram responsáveis pelo aprimoramento do software, enquanto Raphaela Ferraz ficou responsável pela criação do layout das novas telas.

Etapa 2) **Estudo sobre as tecnologias das áreas de desenvolvimento**

Uma vez realizada a divisão das áreas de desenvolvimento, a próxima etapa trata do estudo das principais tecnologias de cada área. Com isso, os integrantes Raphaela Ferraz e Victor Marques, representantes das áreas de desenvolvimento front-end e back end, foram responsáveis por criar guias de estudo para cada uma das duas áreas. Sendo assim, os guias de estudo foram constituídos por cursos, vídeos, sites e páginas em redes sociais que abordavam conteúdos relacionados ao tema de desenvolvimento.

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 dos ambientes, o próximo passo foi a realização do levantamento de requisitos da aplicação web. O levantamento foi baseado nos requisitos funcionais e

nas tecnologias para a criação da *Cyber Security Information*, conforme demonstram os quadros a seguir (quadro 1 e quadro 2) e para o desenvolvimento do *Digital Authenticator*, de acordo com os quadros 3 e 4:

QUADRO 1 – Requisitos funcionais da aplicação web

Atividades	Requisitos Funcionais
Garantir 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. Ex.: Digital Authenticator
Disponibilizar Software Mobile	Disponibilizar o aplicativo Digital Authenticator para download
Enviar E-mails	Enviar newsletter, para os usuários cadastrados no banco de dados, com avisos sobre a inclusão de conteúdos na aplicação
Informar Sobre o Projeto	Disponibilizar informações sobre os desenvolvedores, os orientadores e a instituição de ensino
Disponibilizar um Canal de Contato	Expor um formulário para que os usuários possam contatar os desenvolvedores

Fonte: Os autores (2022)

QUADRO 2 – Tecnologias utilizadas na aplicação web

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
Configurar o Ambiente de Produção	Windows, PyCharm, Git, Heroku CLI, Heroku, Namecheap
Desenvolver as Funcionalidades da Aplicação	Django, Python3, HTML5, CSS3, JavaScript, jQuery, PostgreSQL, SQLite

Fonte: Os autores (2022)

QUADRO 3 – Requisitos funcionais do aplicativo mobile

Atividades	Requisitos Funcionais
Permitir o Cadastro de um Novo Usuário	Possibilitar a criação de uma conta no aplicativo, de modo a salvar o nome, o e-mail e a senha do usuário
Permitir o Login no Aplicativo	Autenticar usuário, permitindo ou não o acesso ao aplicativo
Redefinir a Senha do Usuário	Viabilizar a redefinição da senha do usuário
Armazenar os Dados Sensíveis do Usuário	Realizar o armazenamento dos dados do usuário localmente
Expor Manual de Cibersegurança	Permitir a visualização dos conteúdos do manual de cibersegurança

Criptografar os Dados	Criptografar os dados armazenados com o padrão AES-128
Expor Gerador de Senhas	Disponibilizar um gerador de senhas seguras

Fonte: Os autores (2022)

QUADRO 4 – Tecnologias utilizadas no aplicativo mobile

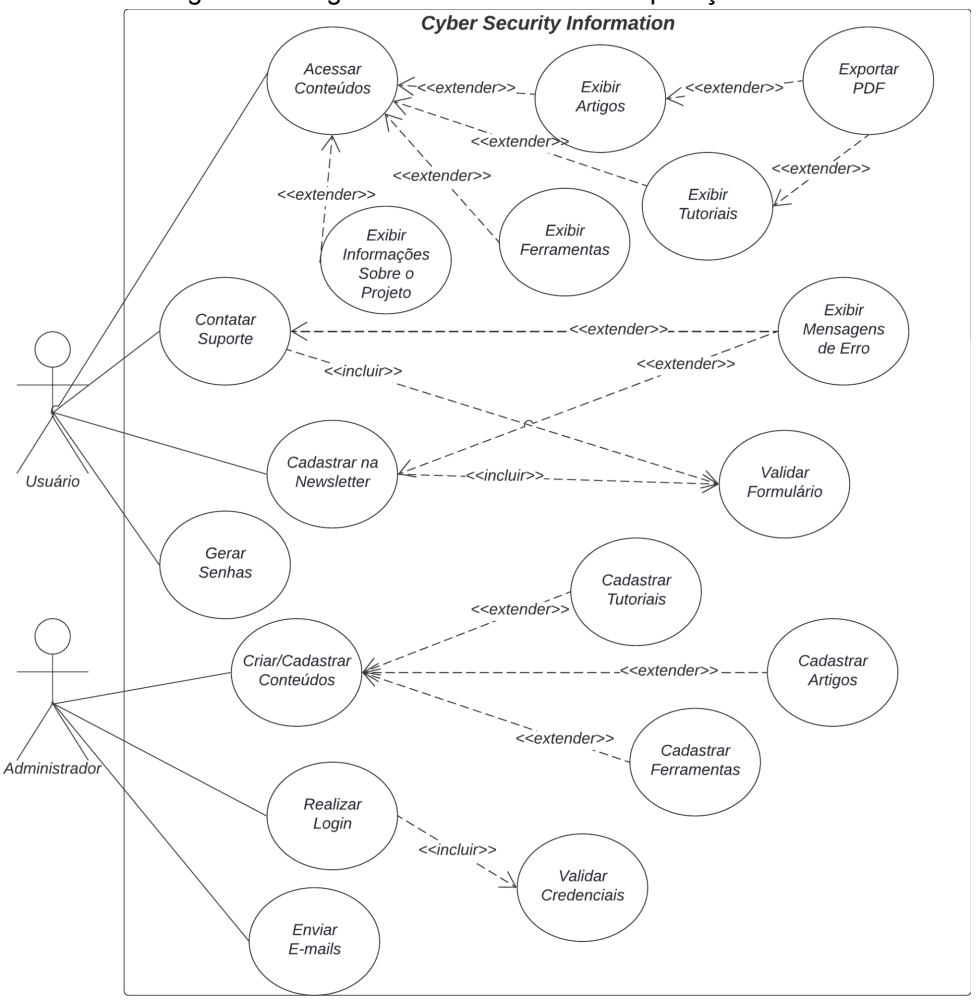
Atividades	Tecnologias
Criar Layout do Aplicativo	Windows, Figma
Configurar o Ambiente de Desenvolvimento	Windows, Kodular
Criar o Aplicativo	Windows, Kodular, TinyDB, Google Firebase
Desenvolver as Funcionalidades do Aplicativo	Linguagem de Programação em Blocos, TinyDB, Real-Time Database, AES-128 bits

Fonte: Os autores (2022)

Etapa 5) **Criação do Diagrama de Caso de Uso da Aplicação Web**

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

Figura 1 - Diagrama de caso de uso da aplicação web

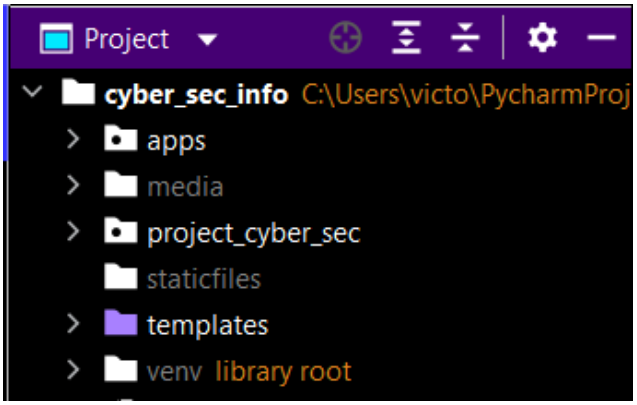


Fonte: Os autores (2022)

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. A divisão dos diretórios está representada na figura 2.

Figura 2 - Diretórios da aplicação Cyber Security Information



Fonte: Os autores (2022)

Conforme demonstrado na figura acima, o diretório “apps” é responsável por organizar os aplicativos, o diretório “media” é onde ficam as mídias da aplicação no ambiente de desenvolvimento e homologação, o diretório “project_cyber_sec” é o *Django Project*, responsável por armazenar todas as configurações da aplicação, o diretório “staticfiles” é onde ficam os arquivos estáticos (arquivos de estilização, arquivos “.js” e imagens) no ambiente de produção, o diretório “templates” é onde ficam os templates em HTML5 e, por fim, o diretório “venv” é o “ambiente virtual” da aplicação nos ambientes de desenvolvimento e homologação.

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**

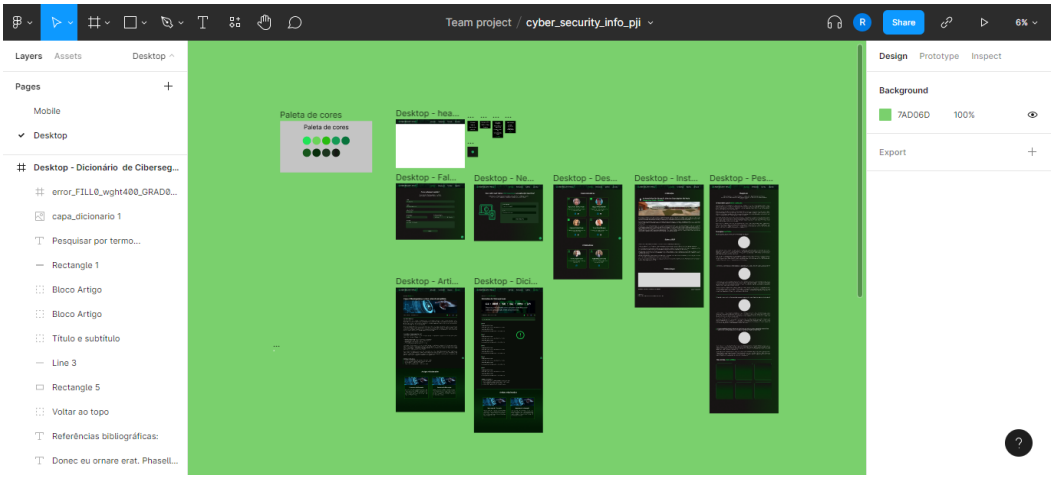
Para o início do desenvolvimento *front-end* das páginas da aplicação, o estudo sobre a inserção da acessibilidade na estruturação das páginas trata-se do primeiro passo. Com isso, foram realizados os estudos sobre a semântica que o HTML5 proporciona, através das suas tags de marcação com significado. Ademais, também foi estudado os tipos de leitores de telas e como utilizá-los para navegar em páginas web. Já o segundo passo para o desenvolvimento das páginas, trata-se 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)**

Dado a realização dos estudos sobre a acessibilidade web, a próxima etapa consiste 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, conforme demonstra a figura 3.

Figura 3 - Ambiente de design Figma da aplicação Cyber Security Information

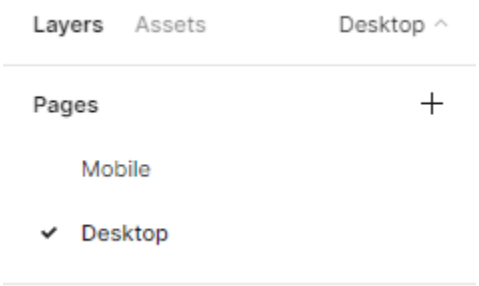


Fonte: Os autores (2022)

Conforme mostra a figura acima, o design das páginas da aplicação é desenvolvido através da responsividade. Sendo assim, no ambiente de design há a divisão da criação dos layouts, existindo uma página da criação dos designs relacionados aos desktops e

uma página de criação dos designs relacionados aos dispositivos mobile, de acordo com a figura 4.

Figura 4 - Divisão do ambiente de design Figma



Fonte: Os autores (2022)

Etapa 11) **Criação das páginas da aplicação, através da utilização da acessibilidade web e *mobile first***

Através da realização de todas as etapas acima, a última etapa necessária para o início da programação front-end da aplicação consiste em desenvolver os códigos de marcação (HTML), de estilização (CSS) e de dinamicidade (JavaScript) com os recursos que garantem a acessibilidade e a responsividade do site.

Etapa 12) **Estudo sobre a segurança cibernética**

Visando a produção de conteúdos informacionais acerca da Cibersegurança, nessa etapa os integrantes realizaram 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 13) **Produção de artigos, tutoriais e ferramentas**

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

Ademais, nessa etapa o software mobile Digital Authenticator - responsável por armazenar informações confidenciais de maneira segura - é melhorado e implementado na aplicação Cyber Security Information.

Etapa 14) **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.

4. 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/, tal como o aplicativo móvel “Digital Authenticator”, o qual foi integrado, em continuação ao projeto realizado no ano de 2021, na aplicação.

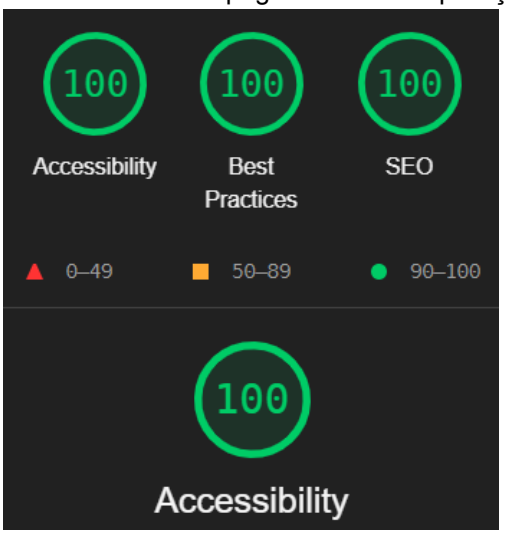
Nesse viés, os resultados foram divididos para apresentar as tecnologias desenvolvidas e, também, compará-las com as tecnologias disponíveis no mercado digital. Com isso, para detalhar os resultados obtidos neste trabalho, os seguintes tópicos estão vinculados ao levantamento de requisitos, etapa 3 da criação da referida aplicação.

4.1 Aplicação Web

4.1.1 Garantia da Acessibilidade nas Páginas

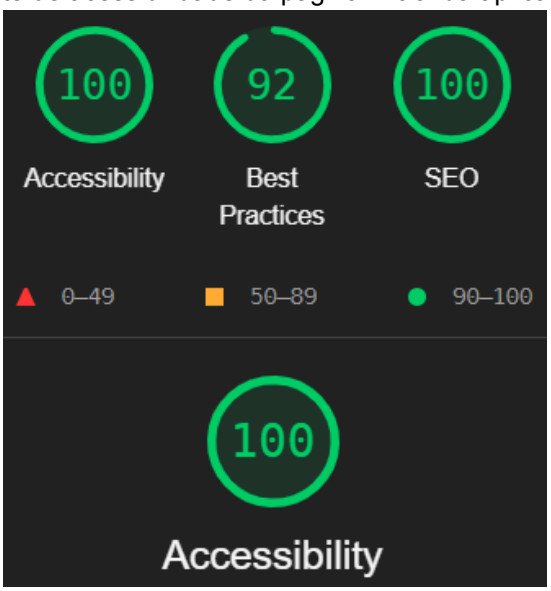
De acordo com a metodologia do projeto, o desenvolvimento das páginas está fundamentado na acessibilidade *web*, uma vez que há, na estrutura do HTML, mecanismos que garantem tal aspecto, como as *tags* semânticas, atributos para leitores de tela, etc. Dessa maneira, as pessoas que possuem alguma deficiência terão acesso aos conteúdos que estão disponibilizados, algo que democratiza não só o acesso à internet, como também o acesso aos conteúdos relacionados à cibersegurança. Assim, as figuras abaixo demonstram a eficácia e a presença do desenvolvimento semântico e acessível da CSI, através do medidor de qualidade das páginas, o *Google LightHouse*.

Figura 5 - Resultados do teste de acessibilidade da página inicial da aplicação, visualizada pelo computador



Fonte: Os autores (2022)

Figura 6 - Resultados do teste de acessibilidade da página inicial da aplicação, visualizada pelo celular



Fonte: Os autores (2022)

Outrossim, para a efetividade da acessibilidade na aplicação, foi implementado nas páginas um plugin de código aberto, VLibras, que traduz os conteúdos digitais presentes no site do Português para a Língua Brasileira de Sinais (LIBRAS). Dessa forma, a democratização das informações é, mais uma vez, garantida, pois pessoas que são surdas e que não possuem conhecimento da língua portuguesa podem consumir, sem nenhum tipo de empecilho, todo o assunto relacionado à segurança cibernética. Assim sendo, a figura 7 evidencia a funcionalidade do *plugin* na página da *Cyber Security Info.*, especificamente na página de Artigos.

Figura 7 - VLibras em funcionamento na página de um artigo

Fonte: Os autores (2022)

Ademais, todas as páginas foram criadas a partir da responsividade, isto é, todas as páginas do *site* possuem suporte nos mais diferentes dispositivos, como em *notebooks*, celulares, *tablets*, PC e até mesmo em computadores que possuem a tela *widescreen*. Sendo assim, as imagens a seguir demonstram a responsividade das páginas em um dispositivo móvel com as telas de dimensões 375 x 667, em um computador de dimensões 1678 x 670 e em um *tablet* de tamanhos 820 x 1180.

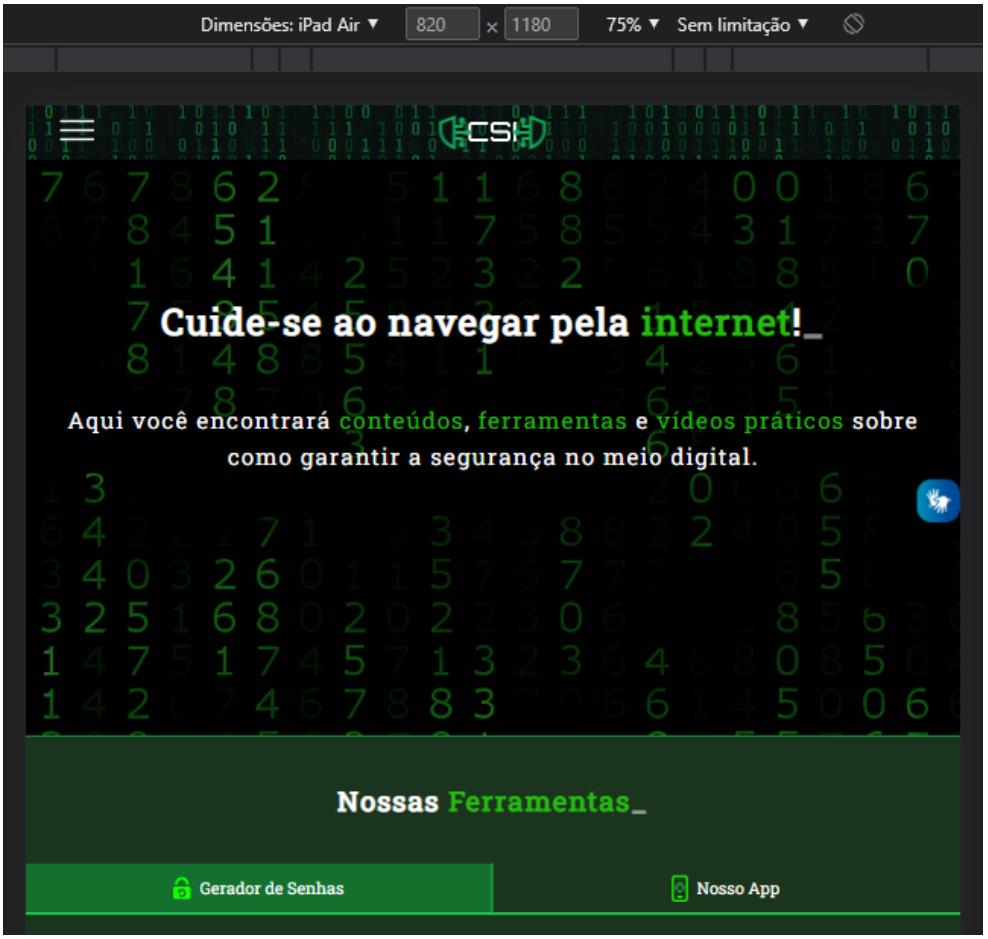
Figura 8 - Responsividade da página inicial em um dispositivo móvel

Fonte: Os autores (2022)

Figura 9 - Responsividade da página inicial em um computador

Fonte: Os autores (2022)

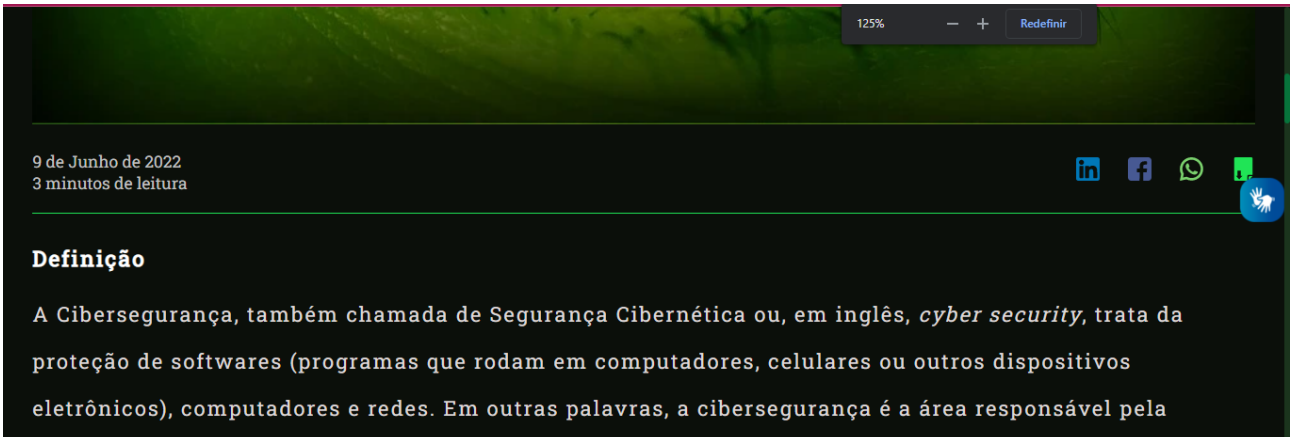
Figura 10 - Responsividade da página inicial em um tablet



Fonte: Os autores (2022)

Além disso, a responsividade da aplicação contribui, também, para a acessibilidade, principalmente no que diz respeito à possibilidade de aumentar ou diminuir as letras do site para uma visualização melhor dos conteúdos escritos (como os que estarão presentes na página de Artigos www.ciberseguranca.info/artigos/) ou, até mesmo, para uma visualização melhor do site em si. À vista disso, as figuras 11 e 12 demonstram a efetividade do *zoom* aumentado na página de Artigo e a funcionalidade do *zoom* diminuído na mesma página.

Figura 11 - Zoom aumentado de 125% na página do artigo sobre cibersegurança



Fonte: Os autores (2022)

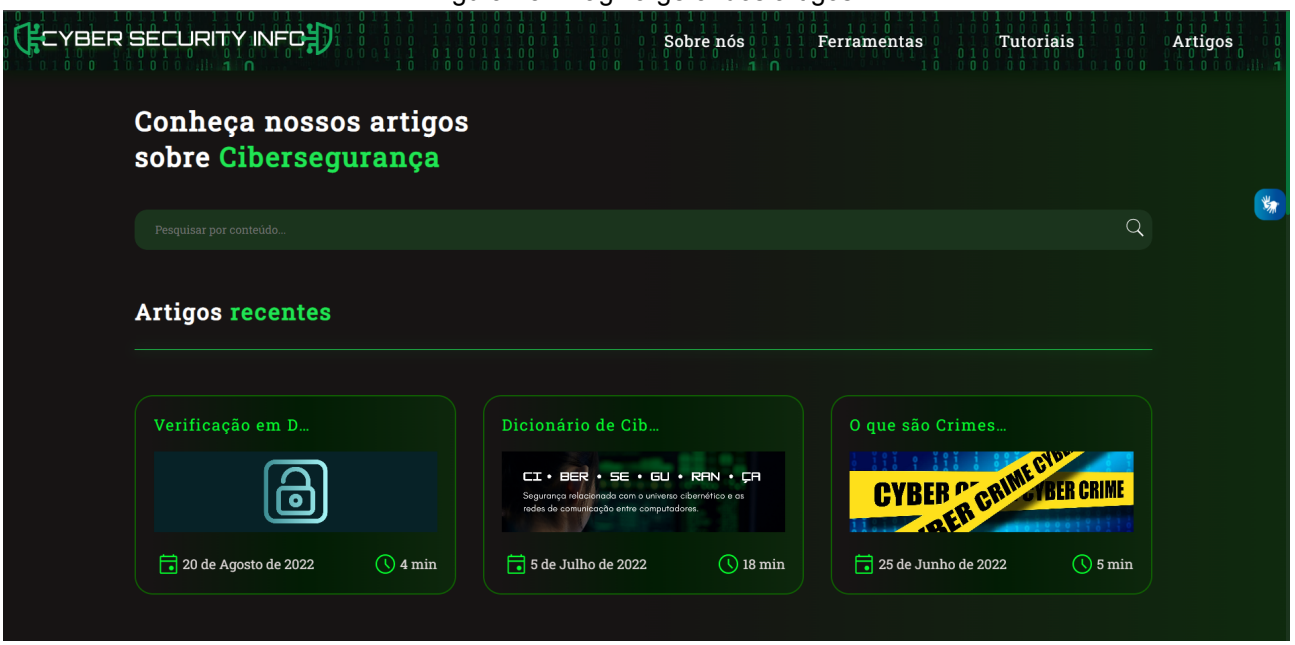
Figura 12 - Zoom diminuído de 80% na página do artigo sobre cibersegurança

Fonte: Os autores (2022)

4.1.2 Disponibilização de Artigos

No tocante à disponibilização de artigos sobre a cibersegurança, o desenvolvimento da aplicação *web* cumpriu esse requisito funcional, uma vez que, dentro do item “Artigos”, no cabeçalho do *site*, encontram-se três principais artigos sobre o tema, além de um *link* para a página que contém todos os artigos já publicados, a qual está demonstrada na figura 13.

Figura 13 - Página geral dos artigos



Fonte: Os autores (2022)

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 assunto do artigo, conforme demonstra a figura a seguir (figura 14).

Figura 14 - Artigo sobre o que é a Cibersegurança

Fonte: Os autores (2022)

Ademais, acerca da linguagem do artigo, os integrantes do grupo prezaram por uma escrita simples, de modo que o máximo de pessoas possível consiga ler e

compreender o artigo, inclusive as pessoas com algum tipo de deficiência, já que, como mencionado no tópico anterior, as páginas garantem a acessibilidade web.

4.1.3 Disponibilização de Tutoriais

Acerca da disponibilização de tutoriais com exemplos práticos para a aplicação dos conteúdos dos artigos, este projeto 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* (https://www.ciberseguranca.info/tutoriais/).

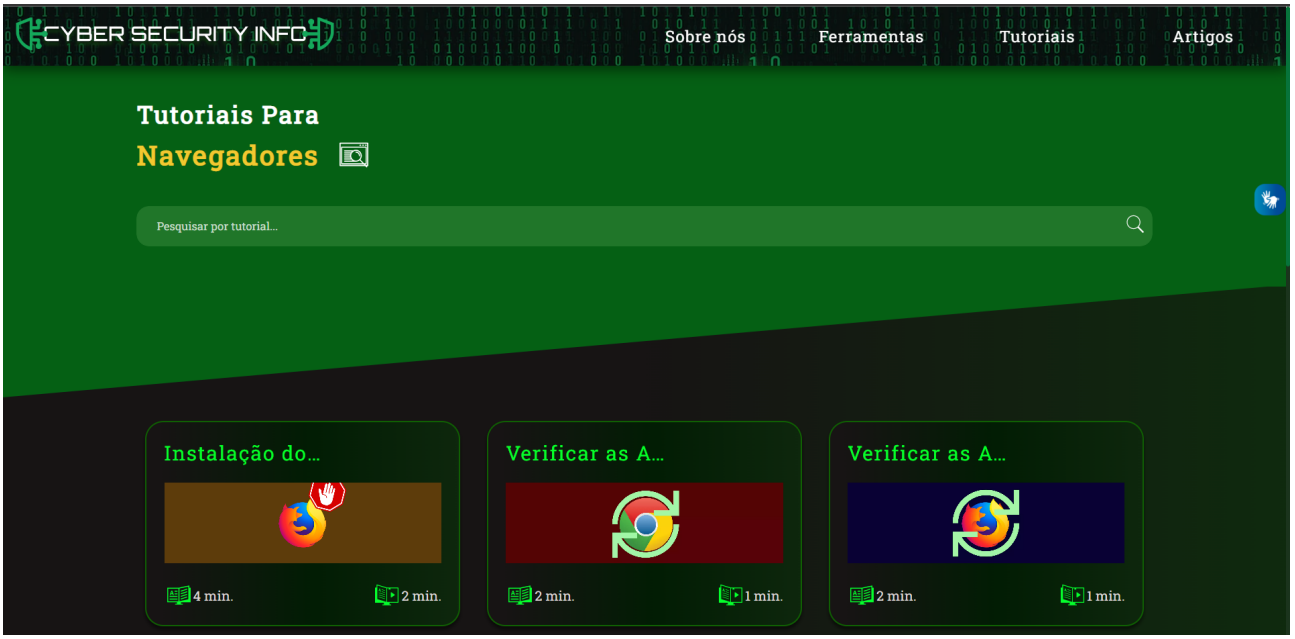
Sobre a página expositiva do tutorial, ela contém os seguintes componentes: caminho do tutorial, capa, data da publicação, tempo de leitura e tempo de vídeo, botões para compartilhamento nas principais redes sociais (Instagram, Linkedin e Facebook), botão para *download* da página, texto introdutório, tutorial em vídeo, conteúdo escrito do vídeo, sugestão de tutoriais relacionados e sugestão de artigos relacionados, conforme exposto na figura 15.

Figura 15 - Tutorial sobre como instalar um bloqueador de anúncios no Google Chrome

Fonte: Os autores (2022)

Já sobre a página das categorias, ela apresenta todos os tutoriais da categoria requisitada pelo usuário. As categorias são: Redes Sociais, Computadores, Celulares e Navegadores. Sendo assim, o usuário pode acessar a página de cada categoria através da página geral ou através do caminho disponibilizado na página de um tutorial. Dito isso, a imagem a seguir (figura 16) demonstra a aparência da página das categorias.

Figura 16 - Página da categoria “Navegadores”



Fonte: Os autores (2022)

Além disso, a terceira página trata da exposição de todos os tutoriais já publicados, separados por categorias, além de disponibilizar, no topo da página, três tutoriais publicados recentemente. A imagem a seguir expõe o comportamento dessa página.

Figura 17 - Página geral dos tutoriais

Fonte: Os autores (2022)

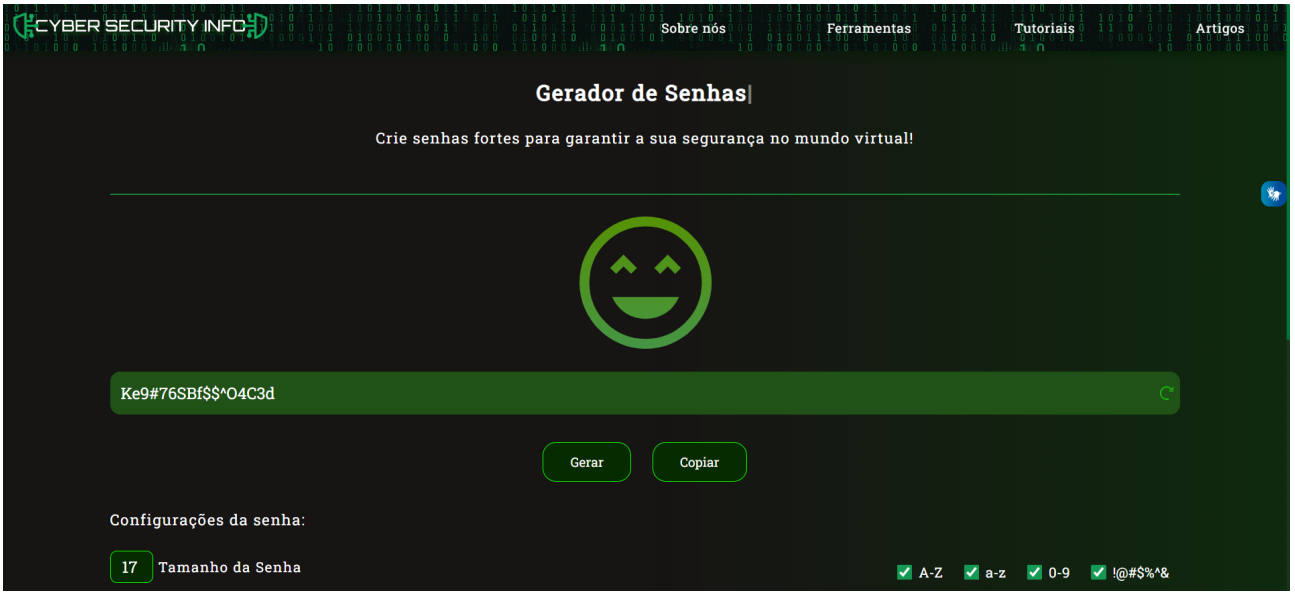
4.1.4 Disponibilização de Ferramentas para Proteção

No que tange à disponibilização de ferramentas voltadas à cibersegurança, cuja finalidade é proporcionar mais segurança aos usuários da aplicação *web*, esse requisito funcional foi cumprido neste projeto. Tal realização se dá pelo fato de que foram

desenvolvidas quatro páginas para as ferramentas, as quais estão disponíveis no cabeçalho da aplicação através do item “Ferramentas”. A primeira página trata de uma ferramenta que valida a segurança de uma URL através de uma tecnologia desenvolvida pela empresa Google.

Já a segunda página expõe 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 18).

Figura 18 - Página do gerador de senhas



Fonte: Os autores (2022)

A terceira e a quarta página demonstram, respectivamente, a página expositiva do aplicativo móvel “Digital Authenticator” (demonstrada na figura 19) e a página de recomendações de algumas ferramentas externas (antivírus, extensões de navegadores, etc).

4.1.5 Disponibilização do Software Mobile

No que diz respeito à disponibilização do *software mobile* “Digital Authenticator”, foi disponibilizado no cabeçalho da aplicação *web* o *link* para *download* do aplicativo, dentro do item “Ferramentas”, na opção “Nosso App”. Além disso, também foi disponibilizada uma explicação sobre as funcionalidades do aplicativo, de modo que o leitor saiba do que o *software mobile* é capaz, além de instigá-lo a baixar e utilizar o aplicativo. Com isso, essa página está demonstrada na imagem a seguir (figura 19).

Figura 19 - Página que expõe o aplicativo móvel *Digital Authenticator*

Fonte: Os autores (2022)

4.1.6 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, novos artigos ou novas ferramentas. Nesse sentido, os usuários que sentirem vontade podem cadastrar os seus e-mails através da página “Newsletter” (https://www.ciberseguranca.info/sobre-nos/email/newsletter) e, a cada nova publicação na aplicação *web*, receberão e-mails contendo as informações dos objetos postados, o que inclui: resumo sobre o artigo, a ferramenta ou o tutorial postado, imagem de capa do tutorial e/ou do artigo, *link* para acesso específico para cada nova publicação e *link* geral da aplicação.

Nesse viés, as próximas imagens demonstram, respectivamente, o código-fonte da ferramenta de envio de e-mails, o qual foi desenvolvido utilizando a linguagem de programação Python, a página para cadastramento dos e-mails e um e-mail recebido através da execução do *script.*

Figura 20 - Código da *newsletter*

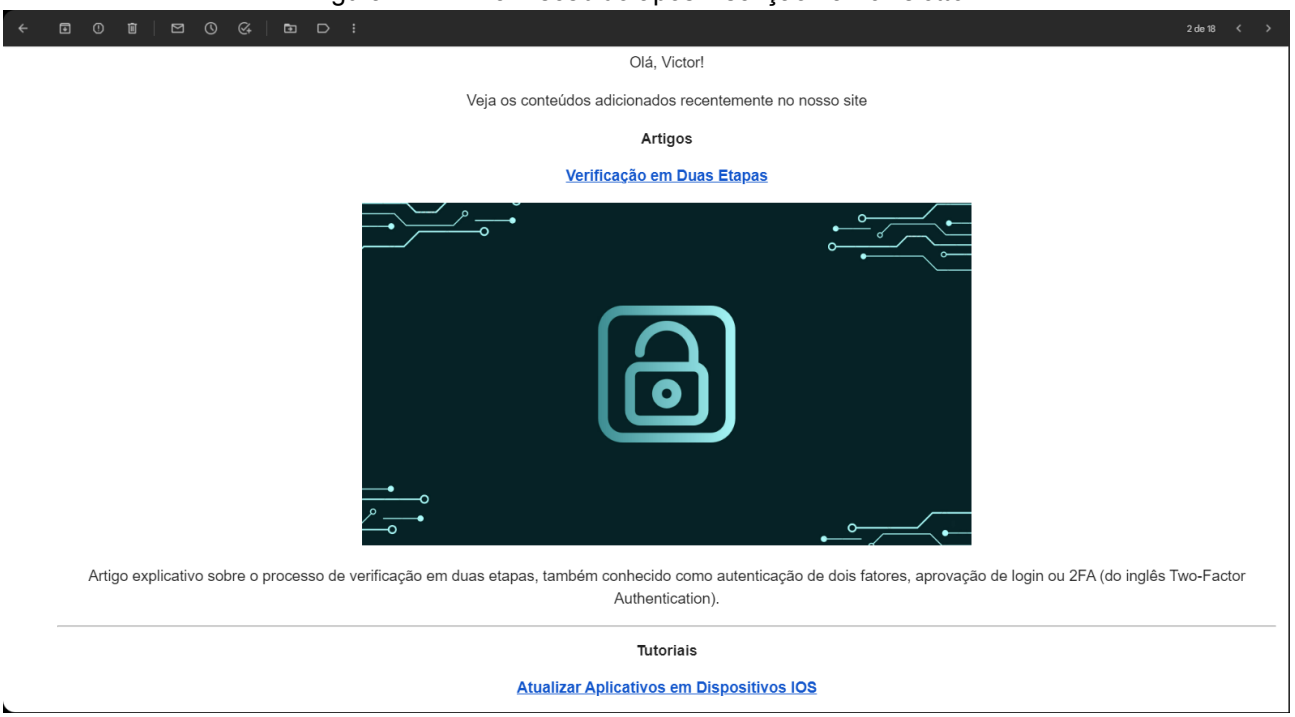
```python
from project_cyber_sec import settings
# modelos
from apps.artigos_cyber_sec.models import Artigo
from apps.emails_cyber_sec.models import Email
from apps.ferramentas_cyber_sec.models import Ferramenta
from apps.tutoriais_cyber_sec.models import Tutorial


class Command(BaseCommand):
    help = "Execute para o envio dos e-mails de atualização (newsletter)"

    def handle(self, *args, **options):
        try:
            artigos = Artigo.objects.filter(data_publicacao=datetime.today()).filter(publicado=True)
            ferramentas = Ferramenta.objects.filter(data_criacao=datetime.today())
            tutoriais = Tutorial.objects.filter(data_publicacao=datetime.today()).filter(publicado=True)
            inscritos = Email.objects.all()

            if artigos.exists() or tutoriais.exists() or ferramentas.exists():
                assunto = "Novo Conteúdo: Cyber Security Information"  # Assunto do e-mail
                mensagem = "Novo conteúdo no site"
                host = settings.EMAIL_HOST_USER  # E-mail que enviará a mensagem

                for inscrito in inscritos:
                    destinatario = [inscrito.email]
                    nome = inscrito.nome

                    email = EmailMultiAlternatives(assunto, mensagem, host, destinatario)
```

Fonte: Os autores (2022)

Figura 21 - Página que apresenta o formulário de cadastro da *newsletter*

Fonte: Os autores (2022)

Figura 22 - E-mail recebido após inscrição na *newsletter*



Fonte: Os autores (2022)

4.1.7 Informações Sobre o Projeto

No que se refere às informações relacionadas ao projeto, foi disponibilizado na aplicação *web*, na página intitulada “Sobre o Projeto”, um resumo do projeto integrador de 2022. Além disso, também foram disponibilizados *links*, tanto para o acesso ao relatório - localizado no repositório do projeto, na plataforma de hospedagem de código GitHub -, quanto para artigos escritos pelos desenvolvedores da aplicação *web* “Cyber Security Information”, publicados no Congresso de Inovação, Ciência e Tecnologia (CONICT) e na revista acadêmica Qualif. Ademais, nesta página, há outro *link* para o acesso a uma história em quadrinhos, da série de gibis intitulada “Dona Ciência”, a qual, os autores do projeto em parceria com o Instituto do Sono, foram responsáveis pela criação.

4.1.8 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, a página possibilita que o usuário envie uma mensagem, podendo ser de reclamação, sugestão, dúvidas ou reporte de erros, a partir do preenchimento dos campos obrigatórios que são: nome, e-mail e o número de telefone. Além disso, o usuário, ao querer contatar os desenvolvedores, precisará preencher o tipo de contato, isto é, qual será a forma de resposta, por parte dos responsáveis pela aplicação, a qual pode ser via e-mail ou via WhatsApp.

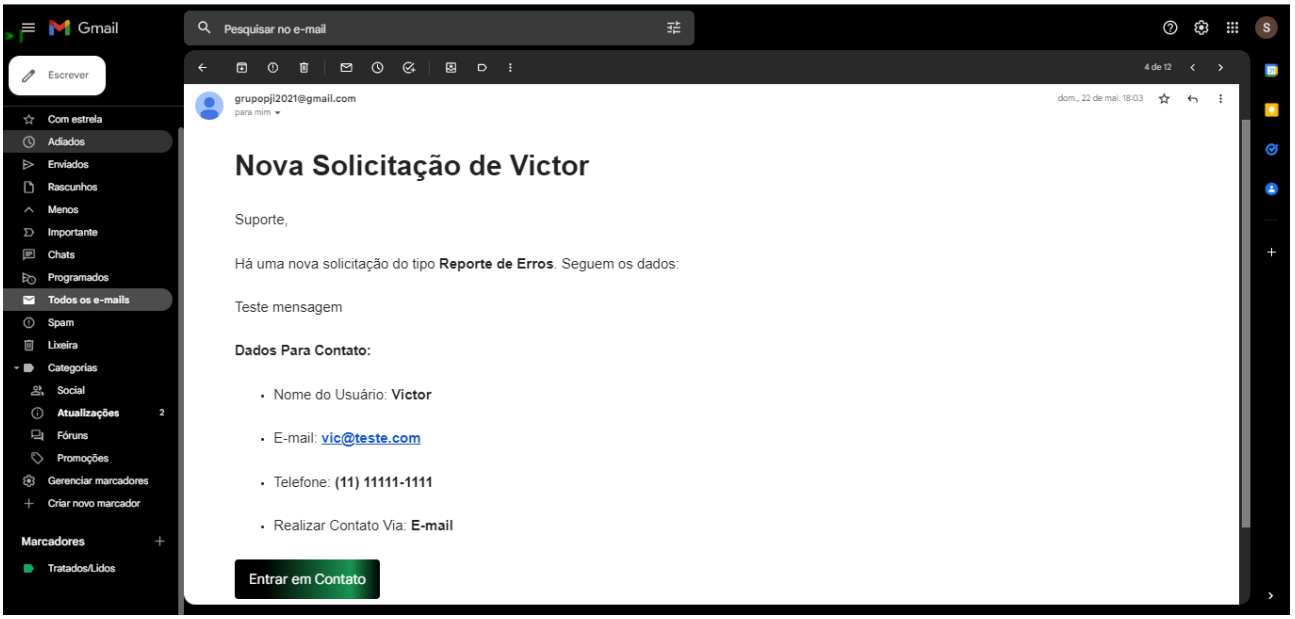
A mensagem que o usuário enviar, por meio deste formulário, chegará no e-mail de suporte da aplicação, ou seja, no e-mail em que os responsáveis do site têm acesso e, por conseguinte, respondem as mensagens recebidas.

Dessa maneira, as imagens abaixo exibem o formulário que o usuário responderá para contatar os desenvolvedores e exibem, também, uma mensagem de exemplo recebida no e-mail de suporte.

Figura 23 - Página que apresenta o formulário de contato com o suporte

Fonte: Os autores (2022)

Figura 24 - Exemplo de e-mail recebido pelo suporte quando o usuário preenche o formulário de contato



Fonte: Os autores (2022)

4.2 Aplicativo Mobile Android

4.2.1 Cadastro

Em conformidade com a metodologia do projeto, o aplicativo conta com um formulário de cadastro, o qual possui os seguintes campos obrigatórios: nome, sobrenome, e-mail, senha e confirmação da senha.

Dessa forma, entre essas informações do usuário, apenas o e-mail e a senha cadastradas são salvas no banco de dados do Google Firebase, o qual é utilizado para realizar essa autenticação das credenciais. Assim, a imagem a seguir demonstra o formulário que o usuário precisará preencher para utilizar o aplicativo.

Figura 25 - Formulário de cadastro do aplicativo

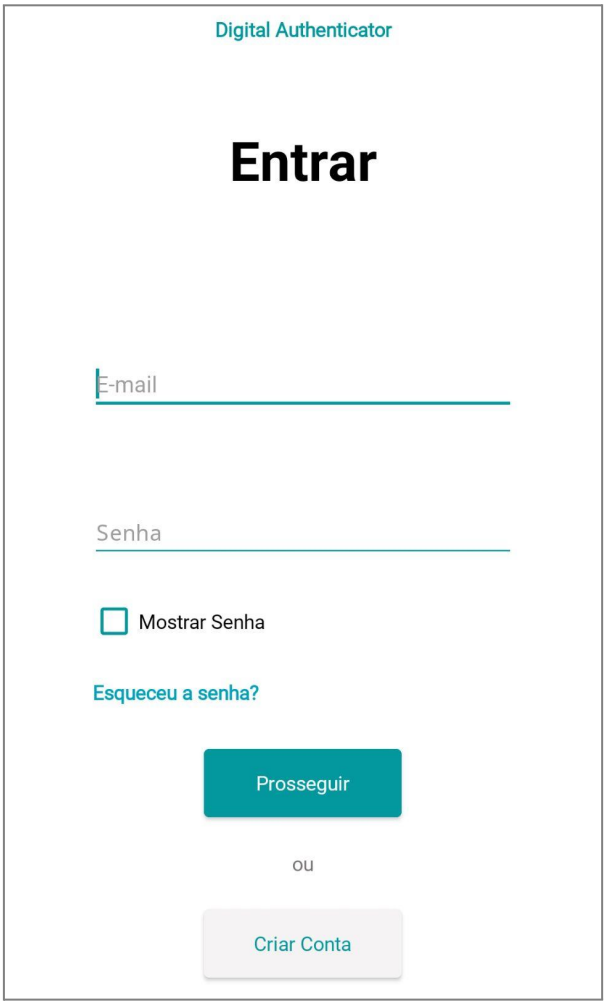
Fonte: Os autores (2022)

4.2.2 Login

Em relação à tela de login do aplicativo, ela conta com um pequeno formulário que exige o preenchimento das credenciais cadastradas. Dessa forma, tal formulário conta com os campos de e-mail e de senha. Desse modo, a imagem 26 expõe a tela de login.

Após clicar no botão “Prosseguir”, conforme mostra a figura 26, o aplicativo pedirá para o usuário realizar a leitura biométrica, a qual será comparada com a biometria que está cadastrada no próprio celular.

Figura 26 - Formulário de Login para acessar o aplicativo



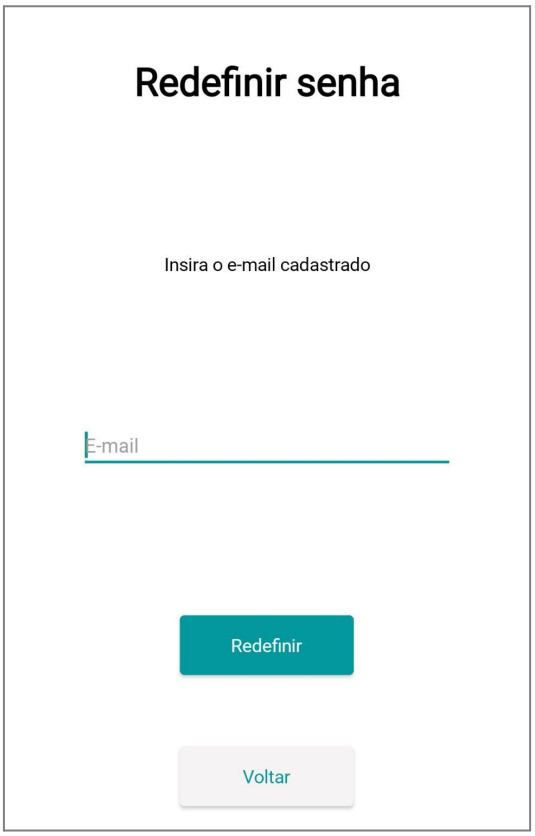
Fonte: Os autores (2022)

4.2.3 Redefinição de Senha

No tocante à redefinição de senhas do usuário, este projeto cumpriu esse requisito, uma vez que foi desenvolvido um formulário obrigatório que solicita o e-mail, o qual foi cadastrado no aplicativo, conforme demonstra a figura 27.

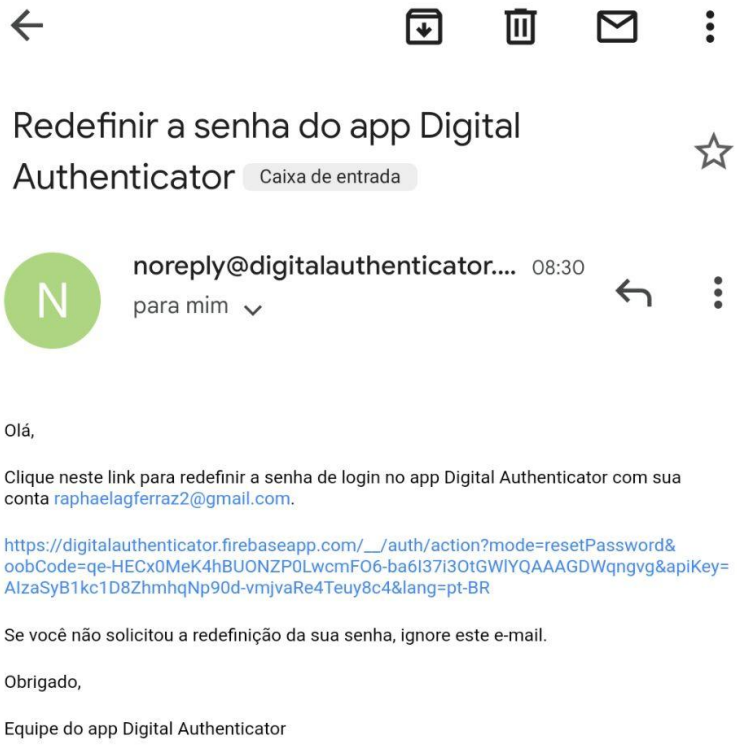
Dessa forma, assim que o usuário preencher o campo, o mesmo receberá um e-mail, o qual contém um link para a página web que permite a modificação da senha, conforme expõe a imagem 28.

Figura 27 - Tela de redefinição de senha



Fonte: Os autores (2022)

Figura 28 - E-mail recebido com o link para a redefinição da senha



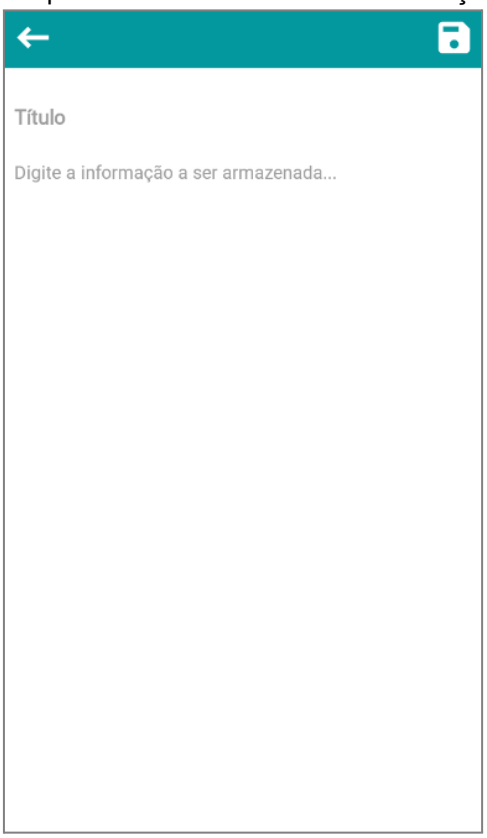
Fonte: Os autores (2022)

4.2.4 Armazenamento de Dados Sensíveis

No que se refere ao armazenamento de dados sensíveis, esse requisito funcional foi atendido, uma vez que foi desenvolvida uma tela na qual o usuário poderá inserir e salvar as suas informações confidenciais.

Essa tela apresenta dois campos, um para o título da informação e outro para a informação propriamente dita, como evidencia a imagem 29.

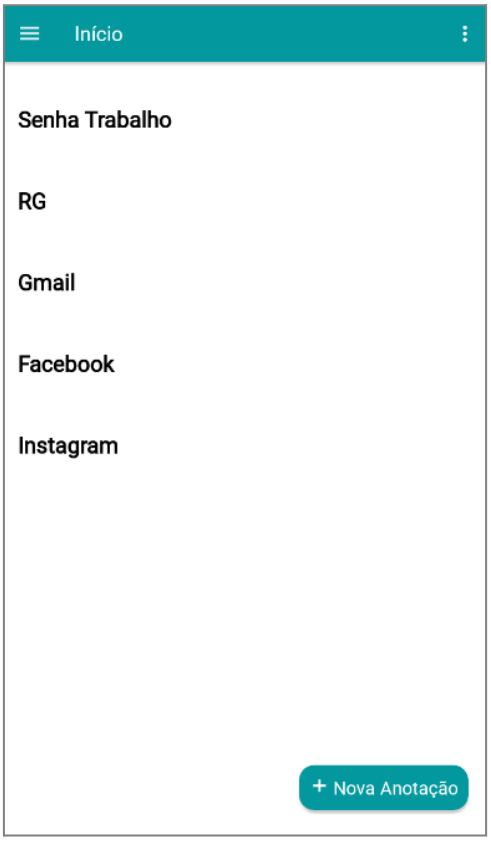
Figura 29 - Tela para o armazenamento de informações sensíveis



Fonte: Os autores (2022)

Dessa forma, após o usuário clicar no botão para salvar os dados confidenciais, esses dados serão salvos, de maneira local, no banco de dados TinyDB e, após isso, o usuário será direcionado para a tela inicial do aplicativo, a qual disponibilizará uma lista com cada título das informações que foram armazenadas, como demonstra a imagem 30.

Figura 30 - Tela inicial do aplicativo com a lista de informações armazenadas



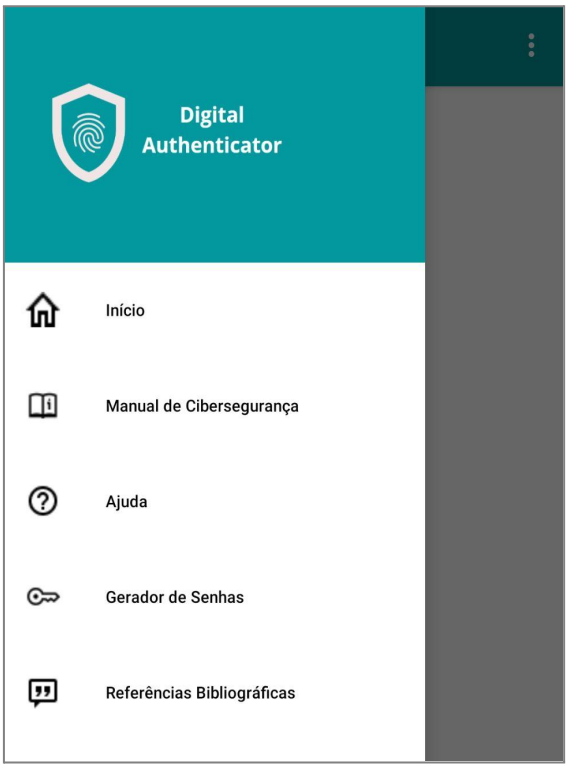
Fonte: Os autores (2022)

4.2.5 Manual de Cibersegurança

No que diz respeito ao manual de cibersegurança, foi disponibilizado no menu do aplicativo uma página que direciona para os tópicos que tal material aborda, como evidencia a imagem 31. Dessa forma, os tópicos presentes no manual desenvolvido são: *O que é cibersegurança*, *O que são crimes cibernéticos*, *Como se proteger de crimes cibernéticos* e *Dicionário de cibersegurança*. Esses tópicos são acessados através da página principal do manual (figura 32).

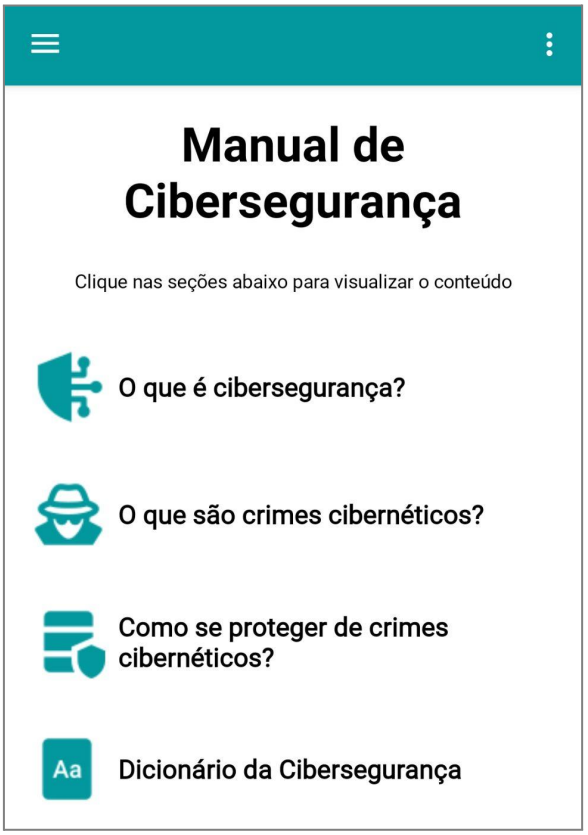
A partir disso, os conteúdos escolhidos pelo grupo para serem redigidos no manual são essenciais para se ter um conhecimento básico sobre a cibersegurança e, por isso, eles foram escritos com uma linguagem simples e explicativa para que, assim, seja possível alcançar a democratização desse conhecimento.

Figura 31 - Menu do aplicativo que possui as opções de navegação no próprio app, incluindo o Manual de Cibersegurança



Fonte: Os autores (2022)

Figura 32 - Tela com os conteúdos presentes no Manual de Cibersegurança



Fonte: Os autores (2022)

4.2.6 Criptografia dos Dados

Quanto à criptografia dos dados, o aplicativo utiliza o padrão *AES-128 bits*, um tipo de criptografia avançado e um dos melhores existentes, visto que esse padrão é extremamente difícil de ser quebrado.

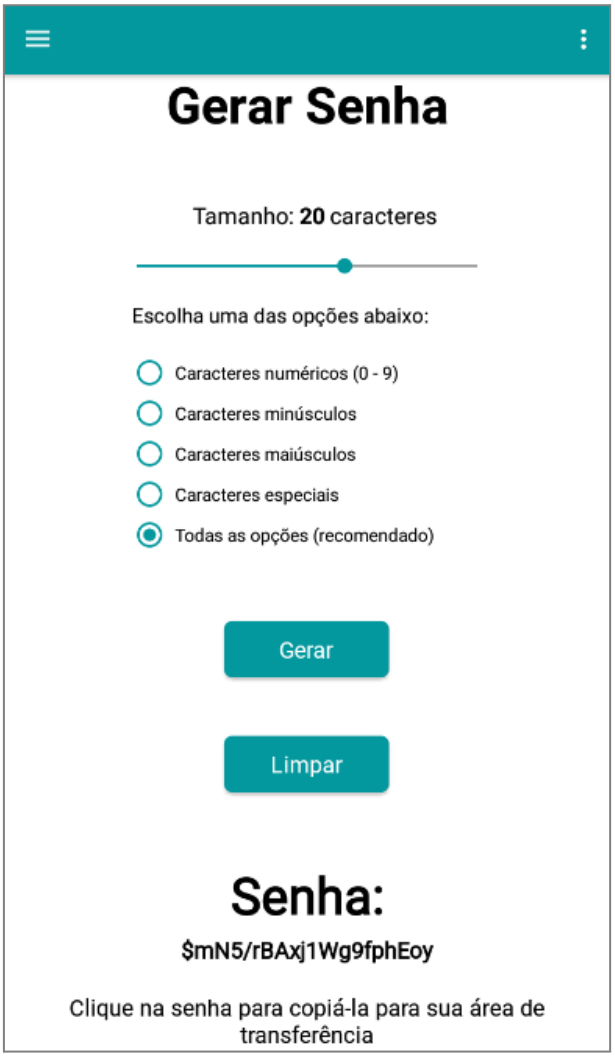
Sendo assim, cada vez que o usuário salvar um dado confidencial, este será criptografado antes de ser armazenado no banco de dados *TinyDB* e quando o usuário acessar determinada informação, seja para visualizá-la ou seja para editá-la, ela será descriptografada. Caso o dispositivo em questão possua alguma impressão digital cadastrada, para acessar os dados armazenados o usuário precisará realizar a segunda autenticação via leitura biométrica, então, somente após isso, a informação será descriptografada.

4.2.7 Gerador de Senhas

Em relação ao desenvolvimento de um gerador de senhas, o aplicativo cumpriu esse requisito funcional, uma vez que tal ferramenta foi disponibilizada no menu do *app* (figura 31).

Nesse viés, o gerador de senhas apresenta um *input range*, que permite ao usuário escolher um número entre o valor mínimo (4 caracteres) e o valor máximo (30 caracteres), o qual corresponde ao tamanho da senha que será gerada, um botão para gerar a senha e um botão para limpar os dados da tela. Além disso, o usuário deve escolher uma das cinco opções exibidas na tela, as quais definem o tipo de senha que será criada. Por fim, há uma parte da tela reservada para apresentar a senha que será gerada a partir das características definidas pelo usuário, conforme demonstra a figura 33.

Figura 33 - Tela que apresenta o gerador de senhas com a senha criada



Fonte: Os autores (2022)

4.3 Discussão

A priori, 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* e o aplicativo *Digital Authenticator* foram desenvolvidos para contribuir para a inclusão digital, no que diz respeito à democratização da informação, especialmente da informação acerca da cibersegurança. Sendo assim, é válido discutir a relevância deste trabalho.

No que se refere à contribuição das tecnologias desenvolvidas 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, integrados nas plataformas supracitadas, nota-se que um grande público poderá acessar, entender e compartilhar importantes termos e conceitos sobre o tema. Nesse viés, ambos os *softwares* disponibilizam esses materiais de maneira acessível, a partir de uma leitura mais simples, de um 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 a carência da população mais vulnerável quanto à posse de aparatos tecnológicos gratuitos, de fácil acesso e entendimento e, sobretudo, acessíveis.

4.3.1 Comparação Crítica com a Literatura Pertinente

Nessa direção, conforme detalhado na revisão literária deste projeto, foi identificada uma outra plataforma que também oferece acesso à materiais voltados à cibersegurança, o CERT.br. Todavia, no quesito acessibilidade, constata-se que o site apresenta uma difícil navegação, o que dificulta, também, o acesso à informação. Por esse motivo, o quadro a seguir compara a aplicação *Cyber Security Information* com o site CERT.br.

QUADRO 5 – Comparação entre a aplicação CSI e o site do CERT.br - Artigos

Recursos	Cyber Security Information	CERT.br
Disponibilização de Materiais Teóricos Sobre	Sim	Sim

Segurança Cibernética		
Disponibilização do Material em PDF	Sim	Sim
Leitura Simplificada	Sim	Sim
Navegação Simplificada	Sim	Não
Link para os Materiais Teóricos no Cabeçalho da Aplicação	Sim	Não
Adaptação do Material para Diferentes Dispositivos	Sim	Sim
Aplicação Principal Responsiva	Sim	Não
Utilização de Imagens	Não	Sim
Conteúdos Disponibilizados na Aplicação Principal	Sim	Não (cartilha.cert.br)
Compartilhamento da Informação Simplificado	Sim	Não

Fonte: Os autores (2022)

Já no tocante a disponibilização de tutoriais, úteis para a aplicação dos conceitos abordados nos artigos supracitados, constata-se que, a partir deles, um grande número de usuários poderá aplicar boas práticas de segurança na internet. Isso devido ao fato de que esses materiais foram desenvolvidos sob o viés da acessibilidade digital, por meio da disponibilização de conteúdos audiovisuais legendados - disponibilizados no canal do youtube deste projeto (Cybersecurity Info), de textos e de imagens para auxiliar na execução dos procedimentos.

Nesse viés, a aplicação web *Cyber Security Information* possui os tutoriais em diferentes formatos - justamente para maximizar a possibilidade de acesso e aplicação dos conteúdos ensinados. Por isso, o quadro a seguir apresenta uma breve comparação dos tutoriais disponíveis no site CERT.br, especificamente no site cartilha.cert.br, com os tutoriais disponíveis na plataforma desenvolvida neste projeto.

QUADRO 6 – Comparação entre a aplicação CSI e o site do CERT.br - Tutoriais

Recursos	Cyber Security Information	CERT.br
Disponibilização dos Tutoriais em Texto	Sim	Sim
Disponibilização dos Tutoriais em PDF	Sim	Sim
Disponibilização dos Tutoriais em Vídeo	Sim	Não
Vídeos Legendados Manualmente	Sim	Não
Disponibilização de Imagens	Sim	Não
Adaptação do Material para Diferentes Dispositivos	Sim	Sim
Conteúdos Disponibilizados na Aplicação Principal	Sim	Não (cidadaonarede.nic.br)

Fonte: Os autores (2022)

No que tange à disposição de ferramentas, voltadas principalmente para o público inexperiente na área de segurança cibernética, a aplicação *CSI* contribui para a democratização dos aparatos básicos para uma mínima garantia de segurança aos usuários. Portanto, o quadro a seguir expõe uma conferência entre a referida aplicação web e o site CERT.br, sob a perspectiva da exposição de tais ferramentas.

QUADRO 7 – Comparação entre a aplicação CSI e o site do CERT.br - Ferramentas

Recursos	Cyber Security Information	CERT.br
Disponibilização de Ferramentas Básicas	Sim	Não
Recomendação de Ferramentas para Profissionais	Não	Sim
Recomendação de Ferramentas para Uso Pessoal	Sim	Não
Conteúdos Disponibilizados na Aplicação Principal	Sim	Sim

Fonte: Os autores (2022)

Outrossim, é válido ressaltar que, conforme consta nos resultados deste trabalho, a aplicação web *Cyber Security Information* foi desenvolvida para a população em geral, diferente do CERT.br, cujo foco principal é o tratamento de incidentes cibernéticos relacionados às redes brasileiras. Portanto, é evidente que este trabalho buscou um olhar cauteloso para as necessidades das pessoas iniciantes no ramo da Segurança da Informação, de modo a prezar pela inclusão digital e informacional.

Sob essa perspectiva, a aplicação web também assegura a democratização do acesso a ferramentas tecnológicas voltadas à cibersegurança por meio da disponibilização de um aplicativo móvel que armazena, de maneira confidencial e local, dados dos usuários, sejam eles sigilosos ou não.

4.3.2 Limitações e Aspectos Positivos

Primordialmente, é inegável que a produção dos materiais teóricos, disponíveis sobretudo na aplicação web *CSI*, ainda é quantitativamente restrita, uma vez que o principal resultado desta pesquisa foi, além da produção desses materiais, a construção de uma ferramenta tecnológica escalável que viabiliza e incentiva a coletivização de instrumentos para o aprendizado e para a aplicação da Segurança na Internet.

Sob tal perspectiva, a aplicação *Cyber Security Information*, em seu estado atual, possibilita a inserção de inúmeros conteúdos textuais e visuais, além de seguir à risca os cenários criados no “diagrama de caso de uso da aplicação” (figura 1). Nesse viés, todas

as principais funcionalidades, tendo como base essa diagramação e o levantamento de requisitos, estão em seus estados ideais de aplicabilidade.

Outrossim, a continuidade do projeto de desenvolvimento de um software mobile para o armazenamento de dados confidenciais, estabelecido no ano de 2021, foi garantida, uma vez que o aplicativo *mobile Digital Authenticator* foi melhorado (com a inclusão de novas telas e funcionalidades) e integrado à aplicação desenvolvida no presente ano.

Nessa direção, é de suma relevância salientar que o aplicativo conta com uma limitação técnica de armazenamento, sobretudo no que diz respeito à forma de armazenamento. Isso ocorre devido ao fato de que, sob o viés da restrição de tecnologias gratuitas para o desenvolvimento Android por meio da linguagem de programação em blocos, não foi possível concretizar o armazenamento em nuvem dos dados armazenados no aplicativo, restando apenas o armazenamento local. Ou seja, cada usuário do *software* terá suas informações armazenadas em seu próprio dispositivo Android, correndo o risco de, na hipótese de perda total do aparelho eletrônico, perder o acesso a essas informações.

5. 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.

Outrossim, 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 ao seus usuários, sejam eles jovens, adultos, pessoas portadoras de deficiências ou quaisquer pessoas imperítas 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, embora sua infraestrutura seja limitada pela gratuidade, tal aplicação, em seu estado atual, suporta a inclusão de centenas de conteúdos.

6. Referências

ALMEIDA, J. de J. et al. Crimes cibernéticos. **Caderno de Graduação - Ciências Humanas e Sociais - UNIT - SERGIPE**, [S. l.], v. 2, n. 3, p. 215–236, 2015. Disponível em: https://periodicos.set.edu.br/cadernohumanas/article/view/2013. Acesso em: 29 jun. 2022.

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 set. 2022.

AZAUSTRE, Carlos. **Aprendiendo JavaScript: Desde cero hasta ECMAScript 6**. carlosazaustre. es, 2016.

BARROS, S. D. P; LEITE, P. T. A terceira idade frente aos desafios impostos pela tecnologia: a necessidade do aprendizado para um uso ético e seguro. [SI]: Decima Octava Conferencia Iberoamericana en Sistemas, Cibernética e Informática, 2019, Orlando. **Memorias**, v. 3., p. 23-28, 2019.

BASILE, Felipe R. M.; LOPEZ, Leonardo Juan R.. Estrategia formativa en defensa digital para adolescentes: experiencia en el Instituto Federal de São Paulo. Revista Científica General José María Córdova, v. 18, n. 30, p. 271-287, 2020.

BORGES, Luiz Eduardo. **Python para Desenvolvedores**. 2. ed. Rio de Janeiro: Edição do autor, 2010.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. VLibras. Brasília, 2019.

CARDOSO, Natanael Silva et al. Um estudo comparativo entre os principais frameworks de desenvolvimento web em linguagem python. 2019.

CECÍLIO, RICARDO. DESENVOLVIMENTO DO SITE WEBGD ACESSÍVEL. 2010.

CGI.br - Comitê Gestor da Internet no Brasil. 2020, **Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil**: TIC Kids Online Brasil 2019. São Paulo: CGI.br. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123093344/tic_kids_online_2019_livro_eletronico.pdf. Acesso em: 19 jun. 2022.

CHARÃO, Júlia. Os crimes cibernéticos na legislação brasileira e os procedimentos de investigação. 2017.

COSTA, A. C. Í.; ANDRADE, S. A. I. HTML5 - Por que usá-lo?. **Revista eletrônica da FANESE,** v. 4, n. 1, p. ?, 2015. Disponível em: https://app.fanese.edu.br/revista/wp-content/uploads/ARTIGO-01-Aluno-Ricardo-ArtigoHTML5.pdf. Acesso em: 14 jun. 2022.

COUTO, E. S. A infância e o brincar na cultura digital. **Perspectiva**, [S. l.], v. 31, n. 3, p. 897-916, 2013. DOI: 10.5007/2175-795X.2013v31n3p897. Disponível em:

https://periodicos.ufsc.br/index.php/perspectiva/article/view/2175-795X.2013v31n3p897. Acesso em: 19 jun. 2022.

CRAIGEN, Dan; DIAKUN-THIBAULT, Nadia; PURSE, Randy. Defining cybersecurity. **Technology Innovation Management Review**, v. 4, n. 10, 2014.

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.

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, 2009. DOI: 10.18617/liinc.v5i1.297. Disponível em: https://revista.ibict.br/liinc/article/view/3189. Acesso em: 9 jun. 2022.

DA SILVA, Rogério Oliveira; SILVA, Igor Rodrigues Sousa. Linguagem de Programação Python. **TECNOLOGIAS EM PROJEÇÃO**, v. 10, n. 1, p. 55-71, 2019.

DHAWAN, S. What's new in CSS 3. *In:* Medium. **Beginner's Guide to Mobile Web Development**. [*S. l.*], 13 mai. 2018. Disponível em: https://medium.com/beginners-guide-to-mobile-web-development/whats-new-in-css-3-dcd7fa6122e1. Acesso em 14 jun. 2022.

EIS, D. Uma breve história do CSS. **Tableless,** [*S.l*], 2005. Disponível em: https://tableless.com.br/uma-breve-historia-do-css/. Acesso em: 14 jun. 2022.

FERRAZ, Amanda Raquel da Rocha Sarmento. A utilização da internet feita por crianças com idade entre 5 e 10 anos. 2019. 74 f. Trabalho de Conclusão de Curso (Licenciatura Plena em Pedagogia) - Centro de Educação, Curso de Pedagogia, Universidade Federal de Alagoas, Maceió, 2019. Disponível em: http://www.repositorio.ufal.br/jspui/handle/riufal/5072. Acesso em: 19 jun. 2022.

FERREIRA, Elisabete Zimmer et al. Internet influence on the biopsychosocial health of adolescents: an integratitive review. **Revista Brasileira de Enfermagem [online]**, 2020, v. 73, n. 2 [Acess 19 June 2022] , e20180766. Available from: <https://doi.org/10.1590/0034-7167-2018-0766>. Epub 30 Mar 2020. ISSN 1984-0446. https://doi.org/10.1590/0034-7167-2018-0766.

FLATSCHART, Fábio. **HTML 5-Embarque Imediato**. Brasport, 2011.

FONTES, Edison. **Praticando a segurança da informação**. Brasport, 2008.

FRANÇA, S. dos S. WEB DESIGN RESPONSIVO: CAMINHOS PARA UM SITE ADAPTÁVEL. **Interfaces Científicas - Exatas e Tecnológicas**, [S. l.], v. 1, n. 2, p. 75–84, 2015. DOI: 10.17564/2359-4942.2015v1n2p75-84. Disponível em: https://periodicos.set.edu.br/exatas/article/view/2220. Acesso em: 19 jun. 2022.

FRÓES, Gabriel; WEBER, Vanessa. **SQLite (O Banco de Dados de Bolso)** // Dicionário do Programador. Youtube, 19 jul. 2021. Disponível em: <https://www.youtube.com/watch?v=xOODmm-NdUc>. Acesso em 19 jun. 2022.

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

ISHIYAMA, Y. B.; TANAKA, Q. F. Democratização da web e liberdade para gerar conteúdo: a tecnologia como meio para geração de impacto social. *In:* Grupo PET - Sistemas de Informação - EACH/USP. **Coruja Informa.** [*S. l.*], 31 mai. 2017. Disponível em http://www.each.usp.br/petsi/jornal/?p=1790. Acesso em: 9 jun. 2022.

KASPERSKY - Kaspersky Lab. Proteja os idosos também no mundo online. Pesquisa da Kaspersky identificou que 44% dos internautas têm parentes idosos que já foram vítimas de ciberameaças. *In:* Kasperski - Kaspersky Lab. **Comunicado à imprensa.** [S. *l.*], 31 mar. 2020. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_proteja-os-idosos-tamb-m-no-mundo-online. Acesso em: 10 mai. 2022.

MACHADO, Leticia Rocha et al. Competência digital de idosos: mapeamento e avaliação. **Educação Temática Digital**, v. 21, n. 4, p. 941, 2019.

MACIEL, Ariane Durce. O lugar das mulheres: Gênero e inclusão digital. **P2P e inovação**, v. 2, n. 1, p. 66-85, 2015.

MALENKOVICH, Serge. Caso Morris Worm completa 25 anos. *In:* Kasperski daily - Kaspersky Lab. **Kaspersky daily.** [S. *l.*], 4 nov. 2013. Disponível em: https://www.kaspersky.com.br/blog/caso-morris-worm-completa-25-anos/1632/. Acesso em: 10 mai. 2022.

MARIOTO, Rita Roberta; BASILE, Felipe Rodrigues Martinez. Escrita para terceira idade com o uso de tecnologias digitais: relato de experiência. **Revista Internacional de Formação de Professores**, v. 5, 2020.

MILANI, André. **PostgreSQL-Guia do Programador**. Novatec Editora, 2008.

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.

MORAIS, E. A.; AMBRÓSIO, Ana Paula L. Ferramentas de busca na Internet. **Relatório Técnico: Universidade Federal de Goiás**, 2007.

NEVES, Barbara Coelho et al. Se estou no Google, logo existo: técnicas de alavancagem e visibilidade de um periódico científico em motores de busca por meio de técnicas de SEO. **Informação & Informação**, [S.l.], v. 25, n. 4, p. 402-430, dez. 2020. ISSN 1981-8920. Disponível em: https://www.uel.br/revistas/uel/index.php/informacao/article/view/39512. Acesso em: 17 jun. 2022. doi:http://dx.doi.org/10.5433/1981-8920.2020v25n4p402.

NIC.br - Núcleo de Informação e Coordenação do Ponto BR ; W3C Brasil - Consórcio World Wide Web Brasil; CGI.br - Comitê Gestor da Internet no Brasil; MPSP - Ministério Público do Estado de São Paulo. 2016. **Cartilha de Acessibilidade na Web (Fascículo II).** Disponível em:

https://www.w3c.br/pub/Materiais/PublicacoesW3C/cartilha-w3cbr-acessibilidade-web-fasciculo-II.pdf.. Acesso em: 9 jun. 2022.

NIC.br - Núcleo de Informação e Coordenação do Ponto BR. 2021. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: pesquisa TIC Domicílios (Edição COVID-19 - Metodologia adaptada)**, ano 2020. Disponível em: https://cetic.br/pt/arquivos/domicilios/2020/domicilios/. Acesso em: 9 jun. 2022.

NIC.br - Núcleo de Informação e Coordenação do Ponto BR; W3C Brasil - Consórcio World Wide Web Brasil; CGI.br - Comitê Gestor da Internet no Brasil; MPSP - Ministério Público do Estado de São Paulo. 2014. **Cartilha de Acessibilidade na Web (Fascículo I).** Disponível em: https://ceweb.br/media/docs/publicacoes/1/cartilha-w3cbr-acessibilidade-web-fasciculo-I.pdf. Acesso em: 9 jun. 2022.

OLIVEIRA, C. B.; SILVA NETO, P. C. Acessibilidade web em dispositivos móveis: uma proposta de métrica para desenvolvimento de conteúdo web móvel acessível a deficientes visuais. **Profiscientia**, n. 13, p. 08-24, 2019. Disponível em: http://www.profiscientia.ifmt.edu.br/profiscientia/index.php/profiscientia/article/view/209/147. Acesso em: 9 jun. 2022.

PANTOFA, Verônica Costa et al. Tecnologia da Informação e Comunicação e a Sociedade da Informação: uma contribuição para inclusão. 2008.

PELTIER, Thomas R. **Information security risk analysis**. CRC press, 2005.

PIEKARSKI, Joseli Inês. Vulnerabilidade digital de novas tecnologias: técnicas utilizadas através do meio digital que podem ser aplicadas em processo. **Gestão da Segurança da Informação-Unisul Virtual de espionagem e no cybercrime**, 2018.

PNAD - Pesquisa Nacional por Amostra de Domicílios, 2015. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv98887.pdf. Acesso em: 19 jun. 2022.

PRADO, Filipe. Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais. **IstoÉ Dinheiro.** [S. *l.*], 20 dez. 2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/. Acesso em: 10 mai. 2022.

RIBEIRO, Alysson de Sousa; ALBUQUERQUE, Walisson Francisco de. Análise de artefatos maliciosos em ambiente acadêmico. 2014.

SECTOR, STANDARDIZATION; ITU, O. F. ITU-Tx. 1205. **Overview of cybersecurity**, v. 10, n. 20-X, p. 49.

SERASA - Serasa Experian. Brasileiros sofrem uma tentativa de fraude a cada 8 segundos, revela levantamento da Serasa Experian. *In:* SERASA - Serasa Experian. **Análise de Dados.** [S. *l.*], 30 ago. 2021. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/brasileiros-sofrem-uma-tentativa-de-fraude-a-cada-8-segundos-revela-levantamento-da-serasa-experian/.

Acesso em: 10 mai. 2022.

SILVA, Andressa.; LÔBO, Ingrid.; MELLO, Marco Túlio. **Dona Ciência - Acessibilidade.** 32. ed. 2021. *E-book.* 19 p. Disponível em: https://institutodosono.com/dona-ciencia-edicao-32/#dearflip-df_7864/26/. Acesso em: 9 jun. 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.

TORRES, V. M. HTML e seus Componentes. **Revista Ada Lovelace,** [S. l.], v. 2, p. 99–101, 2018. Disponível em: http://anais.unievangelica.edu.br/index.php/adalovelace/article/view/4652. Acesso em: 14 jun. 2022.

WAI - W3C Web Accessibility Initiative. **Introduction to Web Accessibility**. WAI, 2005. Disponível em: https://www.w3.org/WAI/fundamentals/accessibility-intro/. Acesso em: 9 jun. 2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação**. Brasport, 2013.