UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CÂMPUS DE FRANCISCO BELTRÃO
CURSO DE LICENCIATURA EM INFORMÁTICA

GABRIELLY KOSLOVSKI PICOLOTTO

SIMULADOR INTERATIVO PARA O ENSINO DE SEGURANÇA DA INFORMAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO

FRANCISCO BELTRÃO
2020

GABRIELLY KOSLOVSKI PICOLOTTO

SIMULADOR INTERATIVO PARA O ENSINO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Informática da Universidade Tecnológica Federal do Paraná, como requisito para a obtenção do título de Licenciado em Informática.

Orientador: Prof. Me. Wellton Costa de Oliveira

FRANCISCO BELTRÃO
2020

TERMO DE APROVAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO - TCC

SIMULADOR INTERATIVO PARA O ENSINO DE SEGURANÇA DA INFORMAÇÃO

Por

Gabrielly Koslovski Picolotto

Monografia apresentada às 19 horas 30 min. do dia 28 de outubro de 2020 como requisito parcial, para conclusão do Curso de Licenciatura em Informática da Universidade Tecnológica Federal do Paraná, Câmpus Francisco Beltrão. A candidata foi arguida pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação e conferidas, bem como achadas conforme, as alterações indicadas pela Banca Examinadora, o trabalho de conclusão de curso foi considerado **APROVADO**.

Banca examinadora:

Prof. Dr. Rafael Wild	Membro
Profª. Me. Elaine de Paula Witt	Membro
Prof. Me. Wellton Costa de Oliveira	Orientador
Prof. Dr. Adair Jose Rohling	Professor Responsável TCC

O Termo de Aprovação assinado encontra-se na Coordenação do Curso.

AGRADECIMENTOS

Gostaria de agradecer primeiramente aos meus pais que sempre me apoiaram e me ajudaram quando precisei, e que desde pequena diziam que eu podia ser o que eu quisesse, desde que eu nunca desistisse de estudar. Sou muito grata ao meu namorado Rodrigo, a quem eu amo muito, que sempre acreditou em mim nos momentos em que nem eu mesma acreditava, e que nunca saiu do meu lado nos momentos de duvidas, ansiedade e até de desespero durante o processo deste trabalho, só tenho agradecer por toda a ajuda e apoio.

Agradeço também aos colegas que fizeram parte da minha caminhada acadêmica, dos quais compartilhamos momentos de alegria, estresse e diversão. Aos professores, que trouxeram diversos ensinamentos para a minha vida, fazendo cada um possuir um papel importante no meu desenvolvimento acadêmico. Agradeço principalmente ao professor Wellton que aceitou ser meu orientador, e que me ajudou e aconselhou durante o processo de desenvolvimento do trabalho.

"Não é o que o mundo reserva para você, mas o que você traz para o mundo." (MONTGOMERY, Lucy Maud, 1939).

RESUMO

KOSLOVSKI PICOLOTTO, Gabrielly. Simulador interativo para o ensino de segurança da informação. 2020. 29 f. Trabalho de Conclusão de Curso – Curso de Licenciatura em Informática, Universidade Tecnológica Federal do Paraná. Francisco Beltrão, 2020.

Diversas tecnologias são utilizadas pelas pessoas todos os dias, e muitas dessas são voltadas para o compartilhamento de informações e exposições pessoais, gerando um grande fluxo de dados sensíveis e sigilosos na internet. Consequentemente, a informação passou a ter um grande valor, tornando-a um alvo de indivíduos mal intencionados e também de empresas e corporações. Pessoas que não possuem conhecimentos sobre conceitos de segurança no ambiente virtual são as mais afetadas, não somente por golpes, mas também por manipulação. No trabalho será abordado os perigos e crimes voltados para o roubo de dados pessoais, enaltecendo a importância da educação das pessoas voltada para a área de segurança da informação. Por meio disso, foi desenvolvido um vídeo interativo que simula um ataque de roubo de dados, onde o usuário realiza escolhas utilizando seu conhecimento de segurança na internet.

Palavras-chave: Segurança. Tecnologia. Educação. Vídeo interativo.

ABSTRACT

KOSLOVSKI PICOLOTTO, Gabrielly. Interactive simulator for teaching information security. 2020. 29 f. Trabalho de Conclusão de Curso – Curso de Licenciatura em Informática, Universidade Tecnológica Federal do Paraná. Francisco Beltrão, 2020.

Several technologies are used by people every day, and many of these are aimed at sharing information and exposing personal files, generating a large flow of sensitive files and sensitive data on the internet. Consequently, the information has become of great value, making it a target for malicious individuals and also for companies and corporations. People who no have knowledge about security concepts in the virtual environment are the most affected, not only by scams, but also by manipulation. At this paper, the dangers and crimes related to the theft of personal data will be approached, highlighting the importance of educating people focused on the area of information security. Through this, was developed an interactive video that simulates a data theft attack, where the user makes choices using his knowledge of internet security.

Keywords: Security. Technology. Education. Interactive video.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

HTML	HyperText Markup Language
IP	Internet Protocol

SUMÁRIO

1 INTRODUÇÃO

Com o advento da internet e a criação das novas tecnologias, as pessoas de todo o mundo estão conectadas através de seus computadores, celulares, eletrodomésticos e até mesmo carros. Isto forneceu aos criminosos uma porta de entrada para um novo universo de crimes, os cibercrimes, ou também conhecidos como crimes virtuais.

As tecnologias, por mais inovadoras e modernas que possam ser, não possuem uma segurança cem por cento garantida, sempre há a possibilidade de haver alguma vulnerabilidade, uma falha ou de encontrar um ponto fraco que possa ser explorado por estes criminosos.

Com a internet, as pessoas passaram a cada vez mais expor suas vidas nas redes sociais, informando seus dados pessoais para variados sites, cadastrando cartões de crédito em lojas online e acessando suas contas do banco de modo virtual. No entanto, muitas pessoas não percebem os perigos que esta exposição pode gerar, ainda mais agora em que a informação se tornou um dos direitos mais necessário e valioso existente na nossa sociedade atual (BRAGA, 2000).

Todos os dados e informações ficam circulando nessa grande rede que se conecta com todo o mundo. Quando um indivíduo mal intencionado consegue ter acesso a esses dados, sejam eles dados que estavam visíveis através do consentimento do usuário ou que foram pegos de maneira ilegal, o criminoso pode utilizar essas informações para prejudicar a vítima ou ganhar dinheiro vendendo os dados recolhidos para outras pessoas ou instituições.

Acredita-se que é necessário conhecer e aprender como uma pessoa mal intencionada age para saber como se proteger, por isso destaca-se a importância da segurança da informação, não somente para o indivíduo, como também, para as empresas.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Demonstrar de maneira simulada e interativa conceitos de cibersegurança, mostrando os perigos existentes e as consequências das escolhas do usuário diante de uma determinada situação.

1.1.2 Objetivos Específicos

Para a conclusão do projeto de pesquisa proposto os seguintes objetivos específicos foram desenvolvidos.

Levantar informações sobre os cibercrimes mais comuns atualmente e quais as "estratégias" por trás dos golpes e ataques utilizados na internet.

Procurar literaturas disponíveis sobre cibersegurança, os principais problemas que os crimes virtuais causam e leis que ajudam a proteger as vítimas destes tipos de crimes.

Desenvolver vídeos interativos de cunho educacional para auxiliar no ensino e aprendizagem na área de segurança da informação.

Criar uma interface interativa dentro do vídeo com o usuário, por meio de escolhas.

1.2 JUSTIFICATIVA

Atualmente, os crimes virtuais, como o roubo de dados, ataques de negação de serviços, venda e compartilhamento de objetos e conteúdos ilegais, se tornaram cada vez mais comuns. Observa-se nos noticiários, por meio de mídias como a televisão e a internet, grande parte da população ainda não possui instruções de como agir em determinadas situações, principalmente sendo elas voltadas para questões de segurança em ambientes virtuais, dificultando assim, a capacidade do indivíduo de se prevenir de golpes e ataques cibernéticos.

Tornando importante ressaltar também, que a polícia que deveria ser a responsável por lidar com esses crimes, muitas vezes não tem a preparação adequada, possuindo conhecimentos insuficientes para agir nas variadas situações que o universo cibernético pode trazer e na dificuldade de instruir as vítimas para lidar com a situação e até mesmo para prevenir que o crime aconteça novamente.

Sendo que, algumas inconsistências ainda existem dentro da legislação brasileira no que tange os crimes cibernéticos. Segundo Santos, Martins e Tybucsh (2017) o Brasil ainda não possui leis que abranjam todos os diferentes tipos que crimes cibernéticos que ocorrem no dia a dia e que vemos nas mídias.

Pode-se verificar que há uma necessidade de criar mecanismos para a educação destas pessoas tanto sobre tais crimes cibernéticos, quanto como são feitos e qual o propósito por trás. Conhecer o *'backstage'* desse mundo é uma das formas de se proteger e evitar ser vítima deste crimes. Foi através disto que partiu o interesse de criar uma série de vídeos simulando de forma interativa os diversos tipos de golpes existentes.

A tecnologia utilizada para a elaboração desses vídeos é baseada na tecnologia do filme *Black Mirror: Bandersnatch* feito pela Netflix, utilizando HTML5 e Javascript, onde o usuário que está assistindo faz as escolhas entre as opções que surgem durante o vídeo, levando-o para caminhos diferentes dependendo de suas escolhas.

Os vídeos buscarão simular uma navegação do usuário pela internet, fazendo-o se deparar com algumas estrategias de golpes utilizadas pelos criminosos, e através das escolhas o usuário pode cair no golpe ou conseguir sair seguro. A interação faz com que a pessoa se sinta envolvida e pense nas suas ações e nas consequências que isto pode trazer, pois são as suas escolhas que irão determinar o fim do vídeo.

1.3 ESTRUTURA DO TRABALHO

No próximo capítulo serão explorados fatores relevantes ao trabalho, tais como, o grande fluxo de dados pessoais na internet devido ao aumento do uso de tecnologias, acesso de

indivíduos e empresas a dados pessoais de maneira ilegal, legislações abordando crimes virtuais e direito de privacidade, o uso das TICs e sua importância na educação, e a utilização de vídeos como uma ferramenta para o ensino. No terceiro capítulo serão descritos os materiais e métodos utilizados para o desenvolvimento do vídeo. O desenvolvimento do sistema interativo será apresentado no capítulo quatro. Por fim, no capítulo cinco a conclusão será apresentada.

2 REVISÃO DE LITERATURA

2.1 CIBERCRIMES E O AVANÇO DAS TECNOLOGIAS

A internet de acordo com Saini, Rao e Panda (2012) é um local onde todos aproveitam e desfrutam dos benefícios de seu uso, mas que existe também um outro lado, em que as pessoas utilizam a internet com más intenções, que são os chamados cibercrimes. Segundo Oliveira et al. (2017) podemos dizer que os cibercrimes ou crimes virtuais são delitos cometidos por indivíduos que possuem conhecimento avançado em informática, que agem especificadamente através de um computador conectado com a internet.

No entanto, acredito que estes crimes não se limitam somente se praticados em um computador, pois os criminosos podem também se utilizar de celulares ou outros equipamentos próprios para determinados tipos de ataque. É importante lembrar que todos os dispositivos tecnológicos que possuem acesso a internet podem de alguma forma serem alvos ou serem atacantes.

O termo "cibercrime" surgiu por volta de 1990, em Lyon, na França, após uma reunião de um subgrupo das nações G8, onde foi discutido sobre os crimes feitos através de aparelhos eletrônicos ou internet. O subgrupo conhecido como "Grupo de Lyon", se utilizou deste mesmo termo para descrever qualquer tipo de crime praticado por meio da internet ou redes de telecomunicação.

Os primeiros criminosos começaram a surgir por volta de 1960, estudando e desvendando as tecnologias que faziam parte dos computadores e da internet. Utilizando os conhecimentos adquiridos para ter acesso a informações sigilosas tanto de usuários comuns como de empresas.

> Com o aperfeiçoamento dos computadores e a evolução da internet e dos meios digitais de acesso a ela, a atuação dos criminosos foi modificando-se ao longo dos anos e os crimes virtuais ganharam uma nova roupagem, não apenas para prática de espionagem e sabotagem das máquinas, mas em manipulações bancárias, pirataria em programas de computador, pornografia infantil, racismo, abuso sexual, dentre outros (SILVEIRA; SOUSA; MELO, 2017).

O ciberespaço se tornou um suporte tecnológico para muitos serviços e infraestruturas das quais dependemos diariamente, tornando-as dependentes. Esta crescente dependência trás um grande risco a sociedade, pois a expõe a novas vulnerabilidades. Os ataques feitos para prejudicar o funcionamento de redes e sistemas de informação tem aumentado, não somente na quantidade mas também no impacto produzido. Por isso, firma-se a preocupação na segurança não somente do Estado mas da comunidade também (NUNES, 2012).

2.2 SEGURANÇA DA INFORMAÇÃO

Por consequência, os países passaram a realizar ações para prevenir ataques e garantir sua segurança, criando leis e investindo em profissionais de segurança da informação. Ao pensar em segurança da informação, devemos levar em conta os seus três pilares: confidencialidade, integridade e disponibilidade.

A confidencialidade é não permitir que outras pessoas além das pessoas autorizadas tenham acesso a informação. A integridade é evitar que a informação seja alterada, ela deve permanecer verdadeira. E por último, a disponibilidade é garantir que as pessoas autorizadas tenham acesso as informações sempre que desejarem, elas devem estar sempre disponíveis para o usuário (CALDAS; FREIRE, 2013).

Se um destes pilares for quebrado, significa que a informação está em risco, por isso, os profissionais de segurança da informação devem impedir que isto aconteça e devem garantir que os pilares permaneçam seguros.

De acordo com uma pesquisa feita pela ISACA *(Information Systems Audit and Control Association)* sobre o estado da segurança em 2019, somente 29% dos candidatos para uma vaga de trabalho em cibersegurança possuem qualificações para o cargo e 40% dos alunos graduados em um curso de cibersegurança não estão preparados para os desafios que enfrentarão no trabalho. Isto mostra as dificuldades enfrentadas na busca de profissionais qualificados e com competência para trabalhar na área.

No entanto, por mais protegido que um sistema esteja a sua maior vulnerabilidade é o usuário.

> Os usuários são, portanto, um dos elementos que pode provocar vulnerabilidades e eventuais danos nos SI, pelo que é pertinente verificar se estão sensibilizados para a utilização de práticas corretas e seguras no desempenho das suas tarefas. (PIMENTA; QUARESMA, 2013).

Para atingir esse ponto fraco que está por trás de todos os sistemas, que é o ser humano, os criminosos utilizam a chamada Engenharia Social. A engenharia social é a utilização de conhecimentos com o fim de manipular e persuadir uma pessoa para obter informações, muitas vezes as pessoas nem percebem que estão sendo vítimas de um golpe e acabam passando informações privadas para o engenheiro social, pois este geralmente se passa por alguma pessoa que possui influência sobre a vítima, alguém em que ela confie (SILVA et al., 2012).

Esta acaba se tornando uma maneira muito mais prática e rápida de se conseguir as informações necessárias para se ter acesso a um sistema, sem precisar utilizar meios técnicos e conhecimentos avançados em tecnologia para realizar a invasão.

Atualmente, os principais ataques de roubo de dados são feitos utilizando esta técnica, pois, mesmo a sociedade sendo alertada e orientada a tomar os devidos cuidados, a engenharia social é tão eficaz que até os mais cuidadosos podem ser enganados e acaberem virando vítimas.

Segundo Oliveira et al. (2017) o Brasil a algum tempo atrás não possuía nenhuma legislação voltada especificamente para crimes virtuais. No entanto, em 2012, foi criada a lei

nº 12.737 que ficou conhecida como "lei Carolina Dieckmann", pois em maio deste mesmo ano, a atriz teve seus dados acessados por meio de um link infectado que os criminosos enviaram por e-mail, e assim, teve suas fotos intimas roubadas.

O caso relatado teve uma grande repercussão pelo país, principalmente por se tratar de uma figura pública, mas é importante salientar que muitos outros casos deste tipo já haviam ocorrido com outras pessoas. Esta lei torna crime qualquer invasão em dispositivos eletrônicos, seja com a finalidade de roubar, adulterar ou destruir dados sem a devida autorização.

> A pena para esse tipo de crime prevê de seis meses a dois anos de reclusão, conforme o art. 154-A do código penal: "Aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos."(OLIVEIRA et al., 2017).

2.3 MERCADO DE DADOS PESSOAIS E PRIVACIDADE NO AMBIENTE VIRTUAL

Ao pensar em cibercriminosos, percebe-se frequentemente que existe uma imagem que foi enraizada por influência da cultura vinda de filmes, séries e muitas vezes dos noticiários, de um individuo de capuz em um quarto escuro, utilizando um computador e que possui um extremo conhecimento em tecnologia.

Quando nos deparamos com alguma notícia de crime virtual, como por exemplo, roubo e utilização ilegal de dados, essa é uma das primeiras imagens que o subconsciente cria na mente das pessoas, fazendo-nos esquecer as vezes que empresas e instituições também violam os direitos de privacidade do cliente, e os utilizam sem autorização ou sem que o individuo tenha conhecimento disso. Sendo o próprio governo também um agente de risco, no que se refere ao direito de privacidade e violação de dados sigilosos do indivíduo.

Ao adentrar no assunto de utilização de dados pessoais por empresas e corporações, é necessário primeiramente abordar a existência do mercado de dados pessoais, este que possui grande relevância em nossa sociedade atual. A compra e venda de dados se tornou algo comum, pois, por meio de dados pessoais é possível construir o perfil de uma pessoa, com seus gostos, personalidade, relacionamentos, entre outras informações.

> Conforme o texto da Organisation for Economic Co-operation and Development (OECD) sobre tais mercados, os dados são normalmente utilizados para servir melhor os clientes, melhorar a eficiência das transações e a qualidade dos produtos, bem como para identificar as macrotendências em um número de diferentes setores, incluindo saúde, transporte e segurança (OECD, 2013, p. 4). (SILVEIRA; SOUSA; MELO, 2017).

Esse se tornou um discurso aparentemente comum ao empresas e corporações serem questionadas sobre o uso de dados pessoais. Observa-se que questões sociais e o pensamento em relação ao indivíduo são pouco consideradas nesse contexto. O que nem todas as pessoas percebem é o poder que informações pessoais possuem, e uma delas é o poder de manipulação que oferecem em relação a um indivíduo.

A valorização e o poder da informação fica evidenciada no uso de serviços online gratuitos, muitos desses serviços necessitam que você realize um pagamento para utilizá-lo, não se referindo a dinheiro, pois o pagamento é feito por outro tipo de moeda, os dados pessoais do indivíduo. Esta troca mostra como a informação se tornou um bem econômico em nossa sociedade atual (SILVEIRA; SOUSA; MELO, 2017).

Nesta era da informação, onde a informação e a tecnologia ocupam um espaço importante na vida das pessoas, é de grande necessidade pensar nos direitos de privacidade do indivíduo neste mundo globalizado. No Brasil foi criada a Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709/2018, essa Lei busca aplicar regras para regulamentar a forma como os dados pessoais podem ser armazenados por empresas ou até mesmo por outras pessoas físicas. Possuindo como objetivo proteger os direitos de liberdade e privacidade para o desenvolvimento livre da personalidade do indivíduo.

Na internet, todo dia são feitas transações bancárias, compartilhamento de arquivos, postagem de fotos, compras online, comunicação entre as pessoas, entre muitos outros. Perante inúmeros benefícios, existe também os desafios. Quando colocamos algo na web, é praticamente impossível reaver o que foi exposto, já que pessoas podem salvar e repassar para outros.

No entanto, o limite entre a liberdade de informação e a privacidade é algo bastante delicado, e é necessário realizar um grande esforço para que ambos coexistam harmonicamente.

2.4 O USO DE TICs NA EDUCAÇÃO

Apesar de todos os problemas que a falta de segurança no ambiente virtual podem causar e dos meios criados que buscam garantir nossa segurança e punir criminosos, acredita-se que a educação pode ser uma das formas mais práticas e efetivas de se evitar algum problema ou de criar uma solução.

Segundo, Machado (2019), estamos vivendo em uma época cheia de mudanças que afetam toda a sociedade e sua maneira de viver, e essas mudanças exigem atualizações e inovações na educação. A educação é um meio para o indivíduo formar uma nova visão do mundo e gerar um processo constante de rompimento e reorganização de velhos conhecimentos.

Com o surgimento do computador nas mais variadas formas e tipos de acessibilidade, e das tecnologias que surgiram após o seu advento, muitas atividades realizadas pelas pessoas foram se modificando, e no âmbito escolar não foi diferente, sendo, as Tecnologias da Informação e Comunicação (TICs), utilizadas na educação como uma nova maneira para a realização do processo de ensino-aprendizagem.

As TICs, assim como todas as coisas, possui um lado bom e um lado ruim. De acordo com Leite e Ribeiro (2012) para uma inclusão tecnológica de forma positiva, é necessário que o professor possua o domínio sobre as tecnologias existentes e saber utilizá-las na prática, sendo essencial que haja uma boa formação acadêmica deste profissional, e também, que a escola possua uma boa infraestrutura para abrigar estas tecnologias possibilitando o seu uso durante as aulas. Lembrando que, como as tecnologias estão em constante evolução é importante que

os professores também se atualizem, que se motivem a aprender e a inovar.

Por meio das diversas ferramentas tecnológicas disponíveis nos dias de hoje, a informática, se bem utilizada proporciona uma nova visão para a área pedagógica, podendo gerar uma grande melhora nas metodologias de ensino, possibilitando também, trazer uma gama de inovações, mediante a sua aplicação, para as salas de aula.

2.5 UTILIZAÇÃO DE CONTEÚDO AUDIOVISUAL NA EDUCAÇÃO

Uma das TICs muito utilizada em sala de aula nos últimos anos são os vídeos. Os conteúdos audiovisuais passaram a ser bastante procurados com a finalidade não somente de entretenimento, mas também, como fonte de aprendizado, pois, esses tipos de conteúdos passaram a ser de fácil acesso e se tornaram uma grande fonte de informações.

Um dos principais motivos para a procura de vídeos para o aprendizado pode ser o fato dele ser algo visual, tornando mais atrativo e interessante do que somente escutar ou ler sobre um determinado assunto.

> O uso dos recursos midiáticos, em especial o vídeo, inegavelmente, possibilita o despertar da criatividade à medida que, estimula a construção de aprendizados múltiplos, em consonância com a exploração da sensibilidade e das emoções[. . .](SILVA; OLIVEIRA, 2016).

Muitos filmes são utilizados em sala de aula como uma proposta para o ensino, se tornando um complemento ao tema abordado pelo professor. No entanto, com o grande consumo de vídeos e com os estudos sobre a eficácia de seu uso no âmbito educacional, o conteúdo audiovisual passou a possuir uma nova categoria, o de vídeos educacionais.

Nos dias de hoje ao procurar na internet algum tema do qual se deseja aprender, é muito provável que encontre um vídeo relacionado para se utilizar como uma fonte de conhecimento. Porém, é de grande importância o indivíduo saber filtrar os vídeos que trazem um conteúdo de qualidade de um que pode estar trazendo assuntos mal fundamentados ou que até mesmo esteja espalhado mentiras.

O mesmo se aplica ao professor, quando este decide utilizar algum vídeo como uma ferramenta de apoio em sala de aula. Sendo necessário uma boa formação deste profissional para realizar um trabalho pedagógico de qualidade, trazendo benefícios tanto para ele, como também, para seus alunos.

O vídeo como um meio educacional trouxe inovação para o processo de ensino-aprendizagem, ele abriu uma porta para o mundo externo, transportando o usuário através de imagens e sons, para as mais variadas realidades existentes, sem precisar se locomover, só sendo necessário uma tela para conseguir enxergar todas essas possibilidades que os vídeos podem trazer.

3 MATERIAIS E MÉTODOS

Neste capítulo são apresentadas as ferramentas que foram utilizadas para o desenvolvimento do trabalho, e o método usado durante o processo.

3.1 MATERIAIS

O Objetivo é desenvolver um software que consiga dar maior interação para o estudante, possibilitando controlar o vídeo educativo que ele está assistindo, similar ao *Black Mirror: Bandersnatch*[1].

Para atingir este objetivo foi necessário a utilização de diversos materiais e ferramentas. Cada uma possuindo uma função específica e de importância dentro no projeto.

A realização das escolhas do projeto foi baseado em um código livre em domínio público que está hospedado na plataforma GitHub [2]. O GitHub, é uma plataforma de hospedagem de código-fonte e arquivos.

As ferramentas utilizadas para o desenvolvimento da história para o vídeo foram: O Twine, uma plataforma gratuita para criação de histórias interativas em formato de páginas web. O Google Drive [3], um serviço de armazenamento em nuvem da Google que possui integração com o Google Docs, permitindo a criação de seus próprios arquivos online.

Na parte de gravação, edição e formatação de vídeo foi usado o HandBrake [4], um *software* de código aberto para conversão de arquivos de vídeos. O *software* gratuito de edição de vídeos, DaVinci Resolve 16[5]. E também, XRecorder [6], um aplicativo para gravação e capturas de tela em dispositivos móveis.

Para fazer alterações nos códigos do sistema interativo foi utilizado o Sublime Text [7], que possui como objetivo possibilitar a visualização e edição de código-fonte.

Foi utilizado o sistema operacional Kali Linux [8], uma distribuição GNU/Linux baseada no Debian, desenvolvida pela Offensive Security, possuindo várias ferramentas para realizar testes de penetração e *Ethical Hacking*. Porém, seu uso de deu por meio de uma máquina virtual criada no Virtual Box [9], um *software* gratuito de virtualização de sistema operacionais.

Por meio do sistema operacional Kali Linux, algumas ferramentas foram utilizadas, sendo elas: The Social-Engineer Toolkit (SET) [10], uma ferramenta de código aberto para

[1] https://www.netflix.com/br/title/80988062
[2] https://github.com/joric/bandersnatch/
[3] https://www.google.com.br/drive/
[4] https://handbrake.fr
[5] https://www.blackmagicdesign.com/br/products/davinciresolve/
[6] https://play.google.com/store/apps/details?id=videoeditor.videorecorder.screenrecorderhl=pt$_BR$
[7] https://www.sublimetext.com
[8] https://www.kali.org
[9] https://www.virtualbox.org
[10] https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

realização de testes de penetração voltados para a engenharia social. Ettercap [11], uma abrangente ferramenta para ataques *man-in-the-middle*.

3.2 MÉTODOS

Para o desenvolvimento deste projeto foi utilizado o método estudo de caso, dentro do método qualitativo. De acordo com, Oliveira (2008), quando o pesquisador estiver interessado em realizar uma pesquisa focada em algo em particular e com delimitações bem definidas, orienta-se utilizar o estudo de caso.

O objeto de pesquisa deste trabalho foi a área de segurança da informação, onde se fez um levantamento de informações e foi realizada uma análise dos dados acerca de suas problemáticas no que se refere a pessoas leigas neste assunto.

Tornando necessário também adentrar no tema de cibercrimes, em que foi feita uma vasta pesquisa no que tange os ataques e golpes mais utilizados por cibercriminosos, e também os riscos e as consequências que as falhas e a falta de conhecimento em segurança da informação podem causar.

O método qualitativo não demonstra preocupação na quantidade de dados obtidos sobre um determinado assunto, pois seu principal objetivo é obter a compreensão e entender o significado do objeto estudado, isto sendo feito principalmente por meio da observação e da análise.

Em razão disso, a pesquisa realizada teve seu foco na obtenção de informações a respeito do objeto estudado, trazendo vertentes do assunto que se tornaram necessárias durante o processo, para assim, buscar uma melhor compreensão sobre o tema.

Durante o estudo de caso ocorreu levantamento de questões, onde acabou se tornando fundamental a busca por possíveis soluções para os problemas encontrados. Sendo o tema deste projeto uma ideia adquirida a partir de um desses questionamentos, tornando possível levar o conhecimento de segurança da informação para diversas pessoas, se utilizando de um método diferenciado, que possui como atrativo a utilização do meio visual, que são os vídeos, e a interação com o mesmo, levando o poder de escolha para o usuário.

[11] https://www.ettercap-project.org

4 DESENVOLVIMENTO DO SIMULADOR INTERATIVO

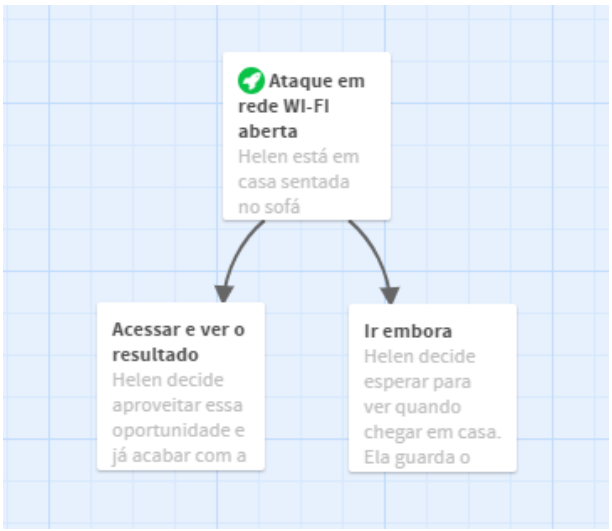
Neste capítulo são apresentadas as partes do processo de desenvolvimento do simulador interativo, sendo elas: a história, a gravação e edição e a implementação do sistema interativo.

4.1 HISTÓRIA

Para a criação da história dos vídeos foi utilizada a plataforma gratuita Twine. Ela serviu para escrever as histórias de uma forma interativa e bastante visual, onde conforme escrevemos, podemos ver os diagramas das histórias e as suas possíveis escolhas, podendo também visualizá-las em uma página web, possibilitando interagir com as escolhas da história que escrevemos.

Abaixo, na figura 1 é possível visualizar a imagem da história criada no Twine, em que possui o formato de diagramas.

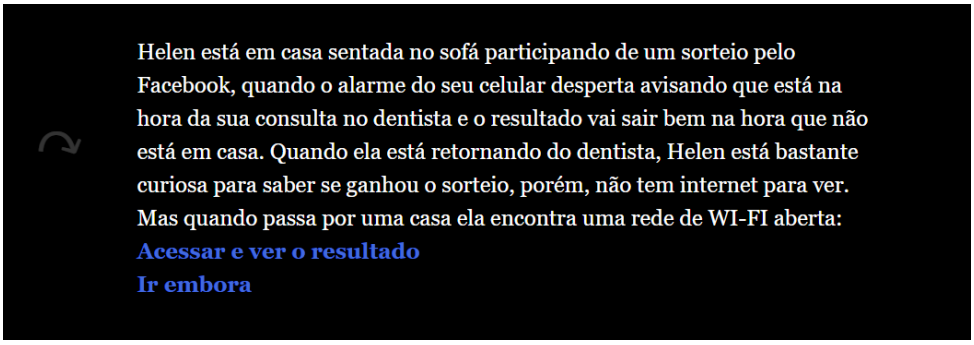
Figura 1 – Twine



Fonte: O autor.

Na Figura 2, é apresentado por meio da página web a história com as suas possíveis escolhas, que se encontram na cor azul, onde o usuário pode interagir clicando no caminho escolhido para ler sua história.

Figura 2 – Twine versão web



Fonte: O autor.

Finalizando a ideia geral no Twine, foi necessário criar o roteiro de cada ação e falas que seriam usadas nas gravações do vídeo. Esta parte foi elaborada no Google Drive, por ser uma plataforma em que os arquivos já ficam salvos automaticamente na nuvem.

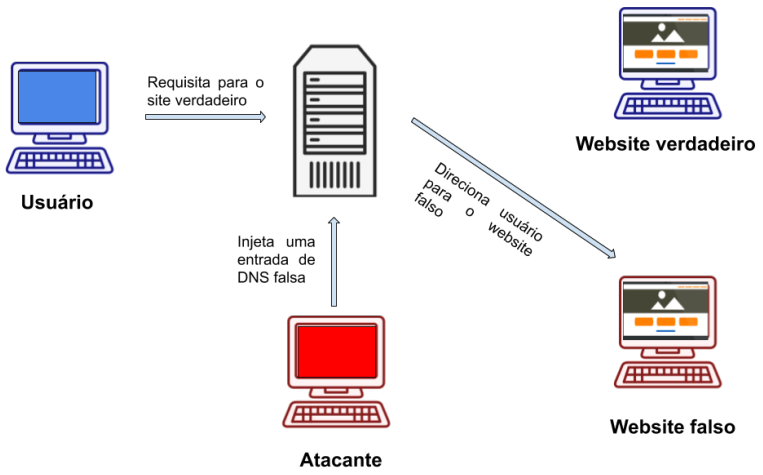
4.2 GRAVAÇÃO E EDIÇÃO

Após elaborada a história e o roteiro, iniciou-se o processo de gravação do vídeo. Para este projeto, foi elaborada a ideia de um possível ataque em uma rede Wi-Fi aberta, conhecido como DNS *cache poisoning* ou DNS *spoofing*.

O DNS *cache poisoning*, como sua tradução já diz, é um ataque de envenenamento de cache DNS. Os servidores DNS (*Domain Name System*), são responsáveis por estabelecer nomes para os endereços IP, tornando possível ao usuário acessar um site digitando seu nome, sem que seja necessário lembrar-se do endereço IP.

Este ataque se aproveita de uma vulnerabilidade dos servidores DNS, possibilitando ao atacante redirecionar usuários que ao acessar um site, como por exemplo o *Facebook*, são levados para uma página falsa, muito semelhante a original, ou seja, os endereços IP dos servidores DNS da vítima são alterados para apontar servidores maliciosos. Fazendo com que muitos nem percebam que estão acessando uma página clone, e acabam por fornecer dados pessoais para o atacante.

Figura 3 – Ataque DNS *cache poisoning*



Fonte: O autor.

Para reproduzir este ataque no vídeo, foi utilizado o sistema operacional Kali Linux, por meio de uma máquina virtual, sendo esta criada através do Virtual Box. Este sistema operacional foi escolhido por já fornecer diversas ferramentas para o uso em testes de penetração, sendo algumas destas ferramentas, as necessárias para a realização do DNS *cache poisoning*.

Antes de iniciar as gravações, foi necessária a criação de uma rede Wi-Fi aberta no roteador. Em razão disso, por meio da página web, foi acessado a interface de configuração do roteador Wi-Fi, na opção chamada *Guest Network* ou Rede de Convidados foi criada uma nova rede sem senha, nomeada de "Wifi do João".

Após essa etapa, iniciou-se o processo de criação de uma página clone do *Facebook*, feita por meio da ferramenta The Social-Engineer Toolkit (SET). Esta ferramenta possui várias funções para a realização de ataques de engenharia social, no entanto, foi utilizada apenas a sua função de capturar credenciais, como por exemplo senhas e logins de usuário, por meio de uma página web falsa.

Finalizada a página clone do *Facebook*, o Ettercap foi utilizado para fazer o ataque DNS *cache poisoning*. Sendo ele o responsável por direcionar para a página falsa o usuário que acessar o site do *Facebook*. Configurando o Ettercap para realizar esta ação com todos os dispositivos conectados na rede.

Com tudo configurado e pronto para a realização do ataque, iniciou-se o processo de filmagem, onde as ações e falas elaboradas no roteiro foram postas em prática.

As gravações foram feitas pelo celular em resolução 4K, no entanto, foi necessário converter para a resolução full HD pelo software gratuito e opensource HandBrake, pois o editor de vídeo não suportava a resolução 4K. Em algumas cenas foi necessário gravar a tela do celular e para isso foi utilizado o aplicativo XRecorder.

Na parte de edição dos vídeos, o *software* escolhido para esse função foi o DaVinci Resolve 16. Por se tratar de um *software* gratuito e bastante completo, trazendo todas as ferramentas fundamentais para a edição final do vídeo.

Foram utilizadas músicas, transições, efeitos de aceleração de vídeo, cortes e muitos outros elementos, voltados para a melhoria do vídeo. A narração presente no vídeo, foi gravada pelo gravador de áudio já disponível no celular, sendo este, incorporado ao vídeo posteriormente.

4.3 SISTEMA INTERATIVO

Por fim, foi criada a interface interativa, que será por meio dela que ocorrerá toda a interatividade do vídeo, permitindo que o usuário faça suas escolhas entre as opções oferecidas no vídeo. Fazendo com que cada escolha leve a um final diferente.

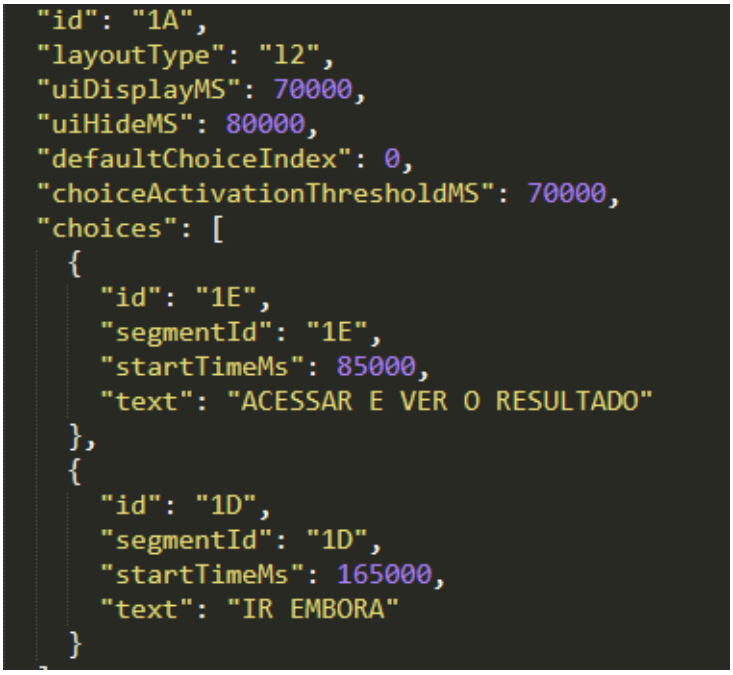
Para o desenvolvimento desta interface foi utilizado HTML5 e arquivos com linguagem de programação Javascript. O usuário para ter acesso ao vídeo de forma interativa deverá abrir a página em HTML5, na qual, por meio do código, chama o vídeo e realiza a leitura dos códigos feitos em Javascript.

No arquivo HTML possui toda a programação da interface visual, contendo todos os elementos visuais, como a localização das opções de escolhas, a barra de tempo, as cores das fontes, as configurações de tamanho da imagem, o arquivo do vídeo gravado e a as opções de controle de vídeo.

As ações de controle no vídeo são realizadas por meio de teclas específicas do teclado do computador, sendo elas: A letra "F" para deixar o vídeo em tela cheia; "R" para reiniciar o vídeo; "Espaço" para pausar; Seta da direita para pular para o próximo momento de interação e da esquerda para pular para o momento de interação anterior.

No arquivo Javascript denominado "bandersnatch.js" foi modificado os nomes das opções de escolha, da primeira interação do código com id "1A", que foi utilizada no vídeo. Sendo a primeira escolha, com id "1E", modificada para ser a opção "Acessar e ver o resultado" e a segunda escolha, com id "1D", passou a ser "Ir embora".

Figura 4 – Código com as escolhas



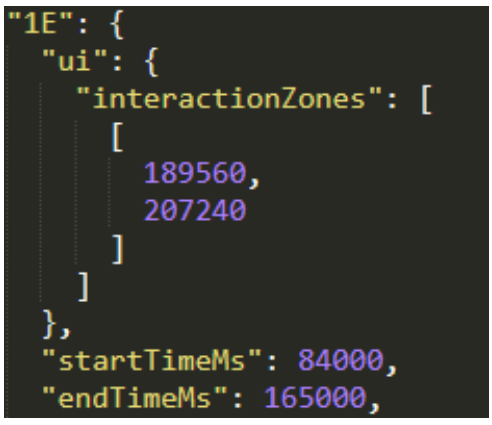
```
"id": "1A",
"layoutType": "12",
"uiDisplayMS": 70000,
"uiHideMS": 80000,
"defaultChoiceIndex": 0,
"choiceActivationThresholdMS": 70000,
"choices": [
  {
    "id": "1E",
    "segmentId": "1E",
    "startTimeMs": 85000,
    "text": "ACESSAR E VER O RESULTADO"
  },
  {
    "id": "1D",
    "segmentId": "1D",
    "startTimeMs": 165000,
    "text": "IR EMBORA"
  }
```

Fonte: O autor.

Já no arquivo Javascript "SegmenMap.js" é onde determinamos o tempo em milissegundos de quando será disparado as opções de escolhas, sendo definido também, o tempo do vídeo em que cada escolha levará.

Como apresentado na figura 5, a escolha com id "1E", que possui a opção "Acessar e ver o resultado", foi modificado no código o "startTimeMs" e o "endTimeMs". No "startTimeMs" foi definido que quando o usuário escolher a opção "Acessar e ver resultado", ele será direcionado para o tempo 84000ms, que convertendo daria 1,4 minutos do vídeo. E no "endTimeMs" é determinado o tempo em que o vídeo pertencente a essa escolha termina.

Figura 5 – Código da escolha "1E"



```
"1E": {
  "ui": {
    "interactionZones": [
      [
        189560,
        207240
      ]
    ]
  },
  "startTimeMs": 84000,
  "endTimeMs": 165000,
```

Fonte: O autor.

Na figura 6, a escolha com id "1D", que possui a opção "Ir embora", foi definido no "startTimeMs" que ao usuário escolher esta opção, ele será direcionado para o tempo 170000ms, que sendo convertido daria 2,83 minutos do vídeo. No "endTimeMs" foi definido o tempo em que o vídeo termina.

Figura 6 – Código da escolha "1D"

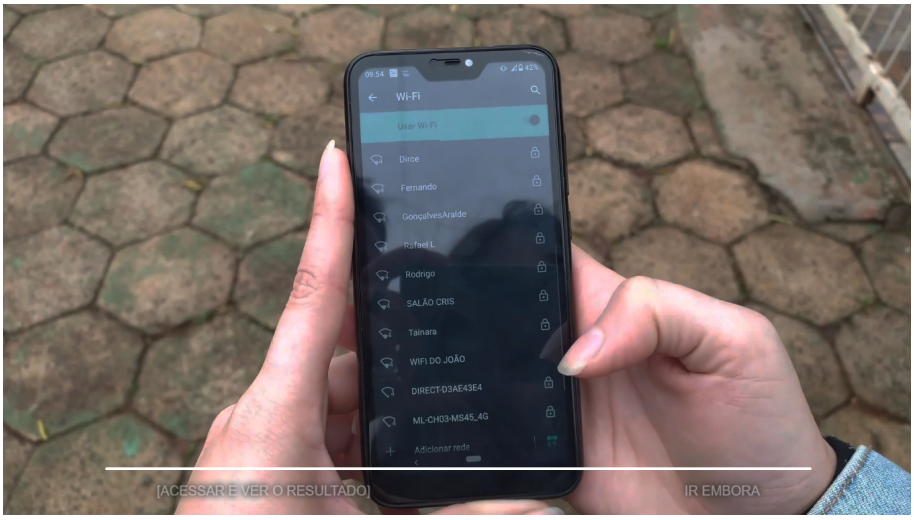
```
"1D": {
  "ui": {
    "interactionZones": [
      [
        189560,
        207240
      ]
    ]
  },
  "startTimeMs": 170000,
  "endTimeMs": 250000,
```

Fonte: O autor.

Após realizadas as devidas mudanças nos códigos, foi executado vários testes para confirmar que tudo estava funcionando bem e assim, garantir que cada escolha estava levando ao tempo certo do vídeo.

Abaixo, na figura 7 é possível visualizar a parte interativa do vídeo já finalizado, trazendo as possíveis escolhas, que são: "Acessar e ver o resultado" e "Ir embora". E também a barra de tempo que o usuário possui para fazer sua escolha, devendo clicar em cima da opção desejada, no entanto, se o tempo acabar e o usuário não tiver feito a sua escolha, a opção que está dentro dos colchetes, que no caso é "Acessar e ver o resultado", será escolhida automaticamente.

Figura 7 – Escolhas



Fonte: O autor.

5 CONCLUSÃO

Este trabalho apresentou os perigos que vivenciamos todos os dias ao utilizar a internet e os meios de comunicação atuais, evidenciando os tipos de ataques e como, por meio da engenharia social, podemos ser alvos fáceis para cibercriminosos.

Foi abordado o abismo existente entre as tecnologias ofertadas, no que se refere a precariedade e até mesmo a falta de ensino oferecido as pessoas comuns sobre como utilizar essas ferramentas de uma forma mais segura para si e sua empresa.

Os golpes aplicados por cibercriminosos estão cada vez mais avançados e acontecendo em maior número. Vivemos na era da informação onde os dados de como os usuários interagem nos sites que visitam, e também seu dados pessoais, são muito valorizados no mercado negro, se tornando um produto amplamente comercializado, muitas vezes, sem o conhecimento das pessoas que tiveram estes dados vazados.

Nesse trabalho foi explorado uma forma de auxiliar o ensino de cibersegurança para as pessoas leigas, através do desenvolvimento de um sistema interativo no formato de vídeo, onde a escolha realizada determina se o alvo será ou não atingido pelo cibercriminoso.

A plataforma de desenvolvimento e elaboração da história através do uso do software livre Twine, em conjunto com os códigos em HTML5 e JavaScript, se demonstraram fáceis de usar, conseguindo um resultado satisfatório de desenvolvimento das interações entre o vídeo e o usuário.

É importante ressaltar que o código em HTML5 e JavaScript, por ser um código livre permite um desenvolvimento e modificação simples e ao mesmo tempo com grandes possibilidades para projetos futuros.

Já o sistema operacional utilizado Kali Linux, se demonstrou completo em sua instalação base, que já possuí uma gama de ferramentas que possibilitam a realização de testes de penetração e de ataques de engenharia social, com poucos cliques, desde que se tenha algum conhecimento prévio.

O Kali linux não deve ser utilizado como distribuição principal em seu computador pessoal, ele é uma ferramenta potente para profissionais em cibersegurança. Seu uso sem o conhecimento adequado pode trazer grandes consequências para o usuário.

Na gravação da história, começaram a aparecer algumas dificuldades, ocorreram várias tomadas de vídeo para que saísse da forma correta, por ser um vídeo com cenas em lugares diferentes, foi necessário dedicar um período grande de tempo para a parte da edição realizada com o Davinci Resolve 16, que mesmo sendo utilizada sua versão gratuita, atendeu a demanda do vídeo sem maiores problemas.

No processo de estudo do código surgiram algumas dificuldades, na tentativa de adequar o código as interações colocadas no vídeo, com a mudança necessária de direção da história dependendo da escolha do usuário. Após o entendimento do código, foram realizadas

então, todas as alterações necessárias para que ao executar o vídeo, este se reproduzi-se de forma satisfatória.

Tendo em vista o objetivo principal desse projeto, o sistema interativo de vídeos facilita o ensino e aprendizagem de normas e bons hábitos de cibersegurança, sendo um modo interativo, que pode ser bem visto pelo usuários finais, por se tratar de uma abordagem dinâmica e de fácil entendimento, sobre um assunto que muitas vezes amedronta ou causa desconforto ao ser trabalhado com pessoas leigas.

5.1 TRABALHOS FUTUROS

O desenvolvimento do sistema interativo de vídeos para ensino de cibersegurança, engloba um método de ensino prático e interativo, a um assunto de extrema importância nos dias atuais.

Quanto maior é o nível de desenvolvimento da tecnologia utilizada pela sociedade, maior deve ser o conhecimento de seus usuários sobre o que pode ou não ser feito ao utilizar essas ferramentas.

O desenvolvimento desse projeto vai além de um trabalho de conclusão de curso, foi observado durante sua criação que o projeto tem uma grande área de extensão, visto que o ensino em questões de cibersegurança ainda é muito precário.

Como trabalho futuro, além de vídeos voltados para um público mais jovem, como foi elaborado neste trabalho, os vídeos interativos podem ser categorizados por idades, com conteúdos voltados a cibersegurança, mas que sejam adaptáveis a todas as idades, adaptando o conteúdo e desenvolvimento, a algo atrativo e que facilite o aprendizado, se utilizando de uma linguagem de comunicação específica para cada faixa etária.

Além do desenvolvimento de vídeos gravados com atores reais em situações do cotidiano, os vídeos podem ser desenvolvidos no formato de desenhos animados, com interações voltadas para o bom uso de tecnologia para crianças, ensinando os cuidados que devem ser tomados por eles, visto que essas já crescem se utilizando de celulares e computadores principalmente para jogos, sendo muitos desses online e sem restrição de idade, o que leva as crianças interagirem muitas vezes com pessoas mais velhas.

5.2 CONSIDERAÇÕES FINAIS

O campo de cibersegurança é muito amplo e ainda pouco explorado, tendo em vista a velocidade de crescimento das tecnologias que utilizamos, e o crescente aumento no roubo de dados. Este é um campo de estudo de extrema importância, não apenas para profissionais da área, mas para qualquer um que faz o uso dessas tecnologias.

O trabalho vem demonstrar um pouco dessa importância, além de ressaltar como estamos vulneráveis a ataques de cibercriminosos, ficando evidente a necessidade de se ter mais ferramentas de ensino nessa área, tanto para leigos quanto para profissionais de informática.

Visto que as empresas também estão vulneráveis a perda de dados importantes se não aplicado normas de segurança da informação baseados na ISO 27000.

Dentro de uma empresa, cada funcionário se torna um elo, que sem o acompanhamento e ensino adequado de como usar as ferramentas tecnológicas, pode se tornar uma porta para cibercriminosos.

Referências

BRAGA, A. A Gestão da Informação. **Millenium**, 2000. ISSN 1647-662X. Citado na página 10.

CALDAS, A.; FREIRE, V. Cibersegurança: das Preocupações à Ação. **Instituto da Defesa Nacional**, 2013. Citado na página 14.

LEITE, W. S. S.; RIBEIRO, C. A. d. N. A inclusão das TICs na educação brasileira: problemas e desafios. **Magis. Revista Internacional de Investigación en Educación**, 2012. Citado na página 16.

MACHADO, L. R. A importância da educação através da arte para construção de cidadania . **Núcleo do Conhecimento**, 2019. ISSN 2448-0959. Citado na página 16.

NUNES, P. F. V. A definição de uma estratégia nacional de cibersegurança. **Nação e Defesa**, 2012. Citado na página 13.

OLIVEIRA, B. M. de et al. Crimes virtuais e a legislação brasileira. 2017. Citado 3 vezes nas páginas 13, 14 e 15.

OLIVEIRA, C. L. de. Um apanhado teórico-conceitual sobre a pesquisa qualitativa: tipos, técnicas e características. **Revista Travessias ed. 04**, 2008. ISSN 1982-5935. Citado na página 19.

PIMENTA, A. M. S.; QUARESMA, R. F. C. A segurança dos sistemas de informação e o comportamento dos usuários. **Revista de Gestão da Tecnologia e Sistemas de Informação**, 2013. ISSN 1807-1775. Citado na página 14.

SAINI, H.; RAO, Y. S.; PANDA, T. Cyber-Crimes and their Impacts : A Review. **International Journal of Engineering Research and Applications**, 2012. Citado na página 13.

SANTOS, L. R. dos; MARTINS, L. B.; TYBUCSH, M. S. B. A. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. 2017. Citado na página 11.

SILVA, C. S. da et al. Engenharia Social: o elo mais frágil da segurança nas empresas. **Revista eletrônica do Alto Vale do Itajaí**, 2012. Citado na página 14.

SILVA, R. V. da; OLIVEIRA, E. M. de. As possibilidades do uso do vídeo como recurso de aprendizagem em salas de aula do 5º ano. **Pesquisa em Educação: Desenvolvimento, Ética e Responsabilidade Social**, 2016. ISSN 1981-3031. Citado na página 17.

SILVEIRA, N.; SOUSA, M. L. de; MELO, A. M. d. A. J. Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann. **Jus**, 2017. Citado 3 vezes nas páginas 13, 15 e 16.