1. **INTRODUÇÃO**

Este capítulo expõe o tema abordado, a motivação e a justificativa do trabalho, relaciona os objetivos e apresenta a estrutura do trabalho.

* 1. CONTEXTUALIZAÇÃO

Quando a internet chegou ninguém imaginava as proporções que essa criação tomaria, além de somente as universidades terem acesso para o compartilhamento de documentos, ela transformou-se na rede mundial de computadores e tornou-se uma ferramenta essencial para todos que têm acesso a ela.

Com a globalização da internet os riscos também se tornaram maiores e mais frequentes. *Hackers*[[1]](#footnote-1), *malwares*[[2]](#footnote-2), fraudes, entre outras causas fazem com que a navegação se torne perigosa. Para adultos já é difícil compreender e distinguir do que é seguro e o que não é na *web*, para crianças isso se torna ainda mais complicado, pois assim como os as crianças e adolescentes são orientados, por seus pais, a não conversar nem aceitar nada de estranhos na rua, isso vale também para o ambiente virtual (VASCONCELOS, 2012).

Com as crianças além dos riscos citados acima, ainda existem outras formas de ameaça no ambiente virtual, sendo elas: o c*yberbullying*[[3]](#footnote-3), predadores *online*[[4]](#footnote-4), a superexposição e ainda divulgar dados importantes de seus pais, como endereço, número do cartão de crédito e local de trabalho (PALFREY; GASSER, 2011).

Para isso se faz necessária a intervenção para que essas crianças sujeitas a ameaças, saibam como se defender em ambientes hostis na internet.

* 1. PROBLEMA

A SaferNet Brasil é uma Organização Não Governamental [(ONG)](#_bookmark0) que recebe e trata de denúncias de crimes que acontecem na internet juntamente com a Policia Federal. Dados de 2016 mostram que as principais denúncias feitas pelos usuários brasileiros são de intimidação, discriminação ou ofensa, exposição intima, problemas com dados pessoais, conteúdo de ódio e fraudes (SAFERNET, 2016).

O aumento significativo de acesso à internet pelas crianças gerou algumas preocupações, pois assim como no mundo real, no mundo virtual existem ameaças, porém nem sempre que uma criança está mergulhada nesse mundo há supervisão de algum adulto responsável.

Logo, o problema consiste em saber como as crianças e adolescentes da Escola Básica Municipal (EBM) Prefeito Henrique Schwarz navegam na internet e analisar o nível de conhecimento dos mesmos quanto aos perigos, regras e leis da internet brasileira.

* 1. JUSTIFICATIVA

A internet pode trazer muitos perigos, pois no mundo virtual não há como ter certeza de quem realmente é a pessoa por trás do computador. Essa pessoa pode estimular crianças e adolescentes a acessar *sites*[[5]](#footnote-5) inadequados para a idade, enviar fotos íntimas ou informações que possam coloca-las em perigo.

(PRESS, 2017) mostra que em 2016 mais de 42 milhões de pessoas no brasil foram vítimas de crimes cibernéticos e isso pode ter gerado mais de dez milhões de dólares de prejuízo para os brasileiros.

Outra questão é a falsa ideia de que estão anônimas e julgarem ter o poder de praticar *bullying*[[6]](#footnote-6), preconceito e espalhar mensagens de ódio.

Chats, *e-mails* [[7]](#footnote-7)e redes sociais podem levar ao contato com pessoas estranhas e mal-intencionadas, essas podem convida-las para um encontro, um emprego ou um jogo. Os criminosos geralmente pedem para os jovens não contar aos pais sobre o convite que pode trazer muitos riscos, como: aliciamento de menores para o crime, sequestros e violência sexual ou física (KOVACS, 2016).

Números divulgados pelo Disque-Denúncia Nacional, mostram que mais de 17,5 mil crianças e adolescentes foram vítimas de violência sexual, violência psicológica também faz parte desse levantamento, esse número indica que foram feitas quase 50 denúncias por dia com relação a isso (VILLELA, 2016). Na internet além de ser possível identificar e punir ospredadores *online*, a criança ou adolescente que praticar um ato ilícito poderá ser responsabilizada pela sua conduta.

* 1. OBJETIVOS
     1. **Objetivo Geral**

O objetivo desse trabalho é conscientizar as crianças da [EBM](#_bookmark1) Prefeito Henrique Schwarz para uma navegação segura e consciente na internet.

* + 1. **Objetivos Específicos**

Para o desenvolvimento desse trabalho tem-se os seguintes objetivos específicos:

- Realizar revisão bibliográfica sobre o tema de segurança na internet para crianças e adolescentes;

- Expor o conteúdo para a turma do nono ano do ensino fundamental;

- Coletar dados da turma para análise; e

- Apresentar os resultados obtidos

* 1. CONTRIBUIÇÃO

Esse trabalho se caracteriza como um trabalho de extensão universitária, uma vez que possibilita a socialização dos conhecimentos adquiridos na universidade com a comunidade.

Contribuirá com o maior entendimento das crianças, pais e educadores para uma navegação mais consciente e segura na internet, além de expor os perigos e as oportunidades que essa ferramenta possui.

* 1. ESTRUTURA DO TRABALHO

Este trabalho de conclusão de curso será estruturado em cinco capítulos. No primeiro capítulo será feita uma introdução e justificativa do tema, com dados reais e notícias em relação a segurança das crianças e adolescentes na internet. O segundo capítulo trará uma pesquisa bibliográfica, para base teórica na aplicação de questionários e entrevistas que foram feitas. No terceiro capítulo será exposto o processo metodológico para a pesquisa de campo e coleta de dados, bem como a sua análise. O quarto capítulo trata da análise qualitativa dos dados que foram coletados dos participantes da pesquisa. No quinto capítulo será exposta a conclusão do trabalho e as considerações finais.

1. **FUNDAMENTAÇÃO TEÓRICA**

Este capitulo aludes sobre as principais formas de uso da informática dentro e fora do ambiente escolar. Práticas relacionadas ao seu uso educacional e outras formas, como uso de redes sociais e as possíveis vantagens de uso da informática na escola.

* 1. AS TECNOLOGIAS DA INFORMAÇÃO E A EDUCAÇÃO ESCOLAR

Está claro que nos dias atuais as Tecnologias Digitais de Informação e Comunicação (TDIC), estão presentes no dia-a-dia das crianças e adolescente, porém nem sempre o uso dessas ferramentas é feito de forma adequada.

“É papel da educação escolar capacitar o indivíduo para a vida”, (COX, 2008, p.25), a autora ressalta a necessidade que as escolas têm de educar os alunos para o mundo cada vez mais desenvolvido tecnologicamente e incentivar os alunos a ter uma postura mais crítica com as matérias abordadas em sala de aula

Para Cox (2008), a informática educacional trata-se de utilizar a informática para a educação como ferramentas de aprendizado e não apenas ensinar ferramentas como processadores de texto, planilhas eletrônicas ou apresentações de *slides*. Mas sim como forma de incentivar a pesquisa, e aprender com a prática.

Então chegamos nas formas de utilização das tecnologias em sala de aula, para proporcionar um aprendizado de qualidade para os alunos, e ajudar os professores a lecionar determinado assunto. Para isso a autora nos traz seis diferentes formas de utilizar a tecnologia,

Cox (2008) traz seis sugestões para utilização das TDCI em sala de aula, para proporcionar um aprendizado de qualidade para os alunos e ajudar os professores a lecionar um determinado assunto. São elas: jogos, simulação, comunicação, *softwares* educacionais, *softwares* comerciaise para ensino a distância.

* + 1. **Jogos**

Aproveitando os recursos de entretenimento que as TDCI oferecem, são desenvolvidos vários jogos eletrônicos com caráter educativo. Fazendo uso das cores, animações e sons disponíveis, essa é uma maneira de prender a atenção das crianças ao conteúdo que está sendo passado.

Esses jogos estão disponíveis em várias plataformas (computadores, smartphones e tablets). Exemplos de jogos desse tipo são fáceis de encontrar de forma gratuita na loja de aplicativos para Android, o Google Play.

* + 1. **Simulação**

(COX, 2008) sugere o uso de simulações da seguinte maneira:

Com essas estratégias de uso dos recursos computacionais, um professor de química, por exemplo, pode simular um conjunto de substâncias a serem misturadas pelos alunos para análise das reações resultantes. Com isso o aluno pode experimentar suas ideias, elaborar conclusões e consequentemente aprender. ([COX, 2008,](#_bookmark29) p.36)

Um exemplo prático de simulação que está no mercado há algum tempo é o Virtual Lab, ele possui vários recursos de um laboratório físico, porém está tudo virtualizado, como representa a [Figura 1.](#_bookmark16)

Figura 1 – Virtual Lab



Fonte: [(PEARSON, 2017)](#_bookmark33)

* + 1. **Comunicação**

O avanço da internet e das enciclopédias *online* possibilitou um grande avanço no compartilhamento das informações, sendo possível consulta-las a partir de qual- quer dispositivo com acesso à rede.

E essa comunicação está associada também às redes sociais. Elas começaram a se popularizar a partir de 2006 com o Orkut, rede essa que já se encerrou [(DIAS; CAVALCANTI, 2016)](#_bookmark30). Atualmente as redes sociais Facebook, WhatsApp e Messenger são as preferidas dos brasileiros. O Facebook, a rede social mais utilizada no Brasil, com cerca de 103 milhões de usuários ativos, é a maior rede social do mundo e também a que tem o maior público do país. Trinta por cento da população brasileira utiliza o WhatsApp diariamente e este está presente em aproximadamente 70% dos *smartphones* do país. O Messenger é o aplicativo para troca de mensagens em tempo real do Facebook, ele se destaca por não precisar entrar no *feed,* mantendo assim mais foco em suas tarefas, o aplicativo possuí mais de 48 milhões de download na loja de aplicativos da Google (RIBEIRO, 2017).

* + 1. ***Softwares* Educacionais**

Os *softwares* educacionais são voltados especificamente para determinados temas, como histórias interativas que promovem a interação das crianças com as personagens envolvidas na trama.

Há aplicativos de exercícios de determinadas matérias que ajudam na aprendizagem pela prática e acabam por agir como um estudo dirigido. Um exemplo de software desse tipo é o Scratch, um projeto do Massachusetts Institute of Technology [(MIT),](#_bookmark2) que ajuda os jovens a pensar de forma criativa, raciocinar e trabalhar de forma colaborativa. Com o Scratch pode programar suas próprias animações, histórias interativas e jogo. [(MIT, 2017)](#_bookmark31).

* + 1. ***Softwares* comerciais**

“São *softwares* com objetivos mais práticos do que educacionais: editar um texto, preencher uma planilha de cálculo e armazenar, classificar e pesquisar dados” (COX, 2008, p.45). Os *softwares* comerciais podem ser uteis para o aprendizado dos alunos, como um editor de texto que facilita a modificações e correção de redações, um editor de planilhas para o armazenamento de dados e auxiliar em equações.

* + 1. **Educação à distância**

A Educação a Distância (EAD) é uma alternativa a educação tradicional (presencial), possibilita que o aluno assista aulas em locais fisicamente distante dos colegas e professores por meio de tecnologia que permita a comunicação entra as partes (MENDONÇA, 2012).

(COX, 2008) aponta as vantagens que as TDCI oferecem quando empregados a essa finalidade:

É valido ainda ressaltar que, quando o computador é usado na aplicação da EAD, as mensagens podem ser compostas por animações, cores, imagens, textos e ilustrações, o que pode enriquecer significativamente o material educativo usado e possivelmente favorecer o processo de aprendizagem (COX, 2008, p.44).

* 1. O USO DA INTERNET PELAS CRIANÇAS E ADOLESCENTES

A internet atinge 50% da população global, sendo que 37% faz uso de redes sociais e 9% de todos os usuários tem entre treze e dezessete anos (KEMP, 2017).

“Uma rede social é uma estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações [...]” [(BERNARDO, 2011).](#_bookmark28) Essa é uma definição quanto as redes sociais no âmbito físico, por exemplo a vizinhança ou colegas de escola.

(TORRES, 2009, p.113), caracteriza as redes sociais digitais da seguinte forma: “[...] *sites* na internet que permitem a criação e o compartilhamento de informações e conteúdos pelas pessoas e para pessoas, nas quais o consumidor é ao mesmo tempo produtor e consumidor de informação”.

Redes sociais digitais são ambientes dinâmicos, com participação na produção e veiculação de informação, de incentivo a participação e assim como em ambientes não virtuais, tais redes também podem tem momentos de conflito e lutas de interesse (ROCHA, 2005).

Existe um ponto em comum entre as redes sociais que é o compartilhamento de informações, conhecimentos e interesses. As redes sociais integram membros com interesses e ideologias, semelhantes ou não, e proporcionam a interatividade entre eles através da comunicação e compartilhamento de conteúdo (BERNARDO, 2011).

A agência de marketing digital We Are Social, realiza pesquisas anuais sobre como a população mundial se comporta na internet. Dados de 2017 mostram que 58% da população brasileira possuem perfis ativos em redes sociais e gastam em média 3:43 horas por dia (KEMP, 2017).

A [ONG](#_bookmark0) SaferNet disponibiliza indicadores de denúncias realizadas durante o ano por usuários e mostra que os principais casos, como pornografia infantil, tráfico de pessoas e incitação à violência são os crimes mais denunciados no Brasil e no mundo. Todas as redes sociais preferidas pelos brasileiros aparecem no ranking dos dez sites mais denunciados em 2016 (SAFERNET, 2016).

No quarto capítulo do livro “Nascidos na Era Digital” (PALFREY; GASSER, 2011), é abordado sobre o assunto de segurança dos nativos digitais na internet. Pesquisas realizadas por eles em países do mundo todo, mostram que isso é uma das maiores preocupações dos pais quanto aos filhos na internet, isso se dá em parte porque os nativos digitais estão passando mais tempo na internet. Em países como a Coréia do Sul, já existem centros de tratamento para jovens viciados em internet.

O *bullying* além de estar presente nas salas de aula e pátios da escola se tornou mais fácil de ser praticado *online*, pois o anonimato que a internet proporciona, faz com que pessoas digam coisas para ferir seus colegas, difamando e promovendo zombarias. Até mesmo as crianças que sofrem o *bullying* na escola, se tornam bulidores na internet (PALFREY; GASSER, 2011).

Outro problema enfrentado na internet é o contato indesejado com pessoas estranhas. Isso acontece quando a criança entra na rede social e não mantém as configurações de privacidade de forma adequada. Os estranhos podem serpredadores *online* e influenciar os jovens a fazer algo que não seja adequado para uma criança ou adolescente, antecipação de imagens fortes e pornografia (PALFEY; GASSER, 2011, p. 108-114).

Vale ressaltar também (PALFREY; GASSER, 2011), citam que a internet não é a causa de todos os problemas que estão relacionados a segurança dos nativos digitais, e sim um meio no qual os problemas que já existiam estão se propagando. Não devemos ficar com medo das novas tecnologias por causa desses problemas e sim tomar atitudes e realizar projetos para prevenção e capacitação dos jovens para uma navegação mais segura e consciente.

Existem algumas organizações que tratam do assunto de segurança na internet para crianças e adolescentes. O Quadro 1 destaca as principais organizações de língua portuguesa, suas parcerias e ações.

Quadro 1 – Organização de língua portuguesa de segurança na internet para crianças e adolescentes (Continua)

|  |  |  |  |
| --- | --- | --- | --- |
| **Nome da Organização** | **Descrição** | **Parcerias** | **Ações preventivas** |
| Família mais segura na internet | Movimento para a formação de usuários digitalmente corretos para a construção de um ambiente virtual mais ético, seguro e legal | Sistema Positivo, Ministério da Educação, TV Escola e MediaPost. | Cartilhas sobre uso ético e legal da tecnologia. Aplicativo iStart, petição *online* para incluir a disciplina de “ética e cidadania digital” nas escolas do Brasil. |
| SeguraNet | O SeguraNet é da responsabilidade da Direção Geral da Educação / Equipe de Recursos e Tecnologias Educativas. Faz Parte do consórcio público-privado Centro Internet Segura. | Fundação para a Ciência e Tecnologia, Instituto Português do Desporto, Microsoft Portugal, cofinanciado pela União Europeia. | Formação, desafios SeguraNet, conteúdos e materiais de sensibilização, dia da internet mais segura, recursos educativos digitais, selo de segurança digital e líderes digitais. |
| SaferNet Brasil | Associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 2005 por um grupo de cientistas da computação, professores, pesquisadores e bacharéis em direito, a organização surgiu para materializar ações concebidas ao longo de 2004 e 2005, quando os fundadores desenvolveram pesquisas e projetos sociais para o combate à pornografia infantil na internet brasileira. | Polícia Federal Ministério Público Federal, Secretaria de Direitos Humanos, Comitê Gestor da Internet no Brasil e Conselho Nacional de Procuradores Gerais. | Cartilhas sobre uso seguro da internet, canal de orientação *online* para crianças e adolescentes, fórum de debates, como denunciar sobre situações de suspeita de violações de direitos humanos de crianças e adolescentes. |

Quadro 1 – Organização de língua portuguesa de segurança na internet para crianças e adolescentes (Conclusão)

|  |  |  |  |
| --- | --- | --- | --- |
| **Nome da Organização** | **Descrição** | **Parcerias** | **Ações preventivas** |
| Childhood Brasil | Certificada como Organização da Sociedade Civil de Interesse Público (OSCIP), trabalha para influenciar a agenda de proteção da infância e adolescência no país, seja em parceria com empresas, com a sociedade civil ou com o governo. A organização tem o papel de garantir que assuntos relacionados ao abuso e a exploração sexual sejam pauta de políticas públicas e privadas oferecendo informação, soluções e estratégias para diferentes setores da sociedade. | Ministério da Educação, Unicef, Senac, Futura e Instituto Votorantim. | Programa na Mão Certa, Programas Grandes Empreendimentos, Programa Turismos, Depoimento Especial, Programa Proteção em Rede, Projeto especial “Grandes Eventos e Infância”. |

Fonte: Elaborado pelo autor, com base nos *sites* das organizações.

A organização Família Mais Segura na Internet é uma organização portuguesa que preza pelas crianças de sua região, enquanto as demais são organizações brasileiras, com muito apoio e respeito das autoridades. O foco principal é o abuso sexual e a superexposição das crianças.

* 1. CRIMES CIBENÉTICOS

Os primeiros relatos relacionadas a esse tipo de ameaça são datadas do final da década de 1950, com programas que se auto replicavam nos computadores das vítimas e inutilizava a memória dos mesmos. Em 1984 Fred Cohen criou o termo “vírus de computador” que denomina arquivos maliciosos, nocivos ao sistema. No ano de 1986 dois irmãos paquistaneses desenvolveram um vírus chamado Brain, que tinha como objetivo detectar o uso não autorizado de um *software* médico para monitoramento de informações cardíacas, porém o código sofreu modificações e se espalhava por disquetes infectados, ele causava lentidão nas operações do sistema e ocupava vários kilobytes da memória dos computadores. Em 1988 foi criado, na Indonésia, o primeiro antivírus para computador, que se preocupava principalmente com o Brain. Relatos mostram que em 2004 surgiram os primeiros vírus para celular, eram transmitidos por Bluetooth e descarregava rapidamente a bateria do celular (WENDT; JORGE, 2013, p. 8-17).

Podemos definir crimes cibernéticos como: “[...] decidimos utilizar o termo “crimes cibernéticos” para definir os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral) (WENDT; JORGE, 2013, p.18)”.

Os crimes cibernéticos são divididos em crimes cibernéticos abertos, que são aqueles que podem ser praticados com ou sem o auxílio de um computador e os crimes exclusivamente cibernéticos são caracterizados por somente serem praticados a partir de um computador ou outros recursos que permitem o acesso a internet. O Quadro 2 expõe alguns exemplos desses crimes.

|  |  |
| --- | --- |
| Quadro 2 – Condutas indevidas praticadas por computador | |
| **Crimes cibernéticos abertos** | **Crimes exclusivamente cibernéticos** |
| Crimes contra a honra;  Ameaça;  Pornografia infantil;  Estelionato;  Furto mediante fraude;  Falsa identidade;  Concorrência desleal;  Tráfico de drogas. | Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir dados sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidade para obter vantagem ilícita;  Interceptação telemática ilegal;  Pornografia infantil por meio de sistema de informática;  Corrupção de menores em sala de bate papo;  Crimes contra urna eletrônica. |

Fonte: Adaptado de WENDT; JORGE (2013).

Esses exemplos são de crimes que já possuem legislação no Brasil, algumas outras ações prejudiciais como a invasão de computador sem o fim de obter, adulterar ou excluir dados e informações e a difusão de *phishing scam* [[8]](#footnote-8)ainda não são caracterizados como crimes.

Os crimes supracitados são comumente praticados em lojas virtuais e *sites* de hotéis falsos e em redes sociais. Nas redes sociais os crimes mais praticados são os crimes de calúnia, insultos, difamação, divulgação de material confidencial, ato obsceno, apologia ao crime, perfil falso, preconceito ou discriminação e pedofilia (POZZEBOM, 2016).

O *site* Direitos Brasil (2017) sugere três importantes passos para a denúncia de um crime cibernético, a Figura 2, traz as ações necessárias para tal.

Figura 2 – Passos para denúncia de crime cibernético

Fonte: Adaptado de Direitos Brasil (2017).

1. **METODOLOGIA DE PESQUISA DO TEMA DO TRABALHO**
   1. PESQUISA BIBLIOGRÁFICA

Para (MARCONI; LAKATOS, 2009) “a pesquisa bibliográfica, [...] abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico etc. [...].

A finalidade da pesquisa bibliográfica é colocar o pesquisador em contato com o que já foi escrito, dito ou filmado sobre o assunto (MARCONI; LAKATOS, 2009).

Os tipos de fontes bibliográficas para esse trabalho foram imprensa escrita, material cartográfico e publicações. Para imprensa escrita foram consultadas algumas notícias com dados e números relevantes para o trabalho, o material cartográfico foi utilizado com o mapa dos indicadores de denúncias de crimes virtuais (SAFERNET, 2016) e as publicações são artigos e livros consultados.

* 1. MÉTODO SURVEY

1. Indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um hacker frequentemente consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento "normal" dos sistemas como previstos pelos seus criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados. [↑](#footnote-ref-1)
2. Abreviação em inglês de “*malicious software”* que significa programa malicioso destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações. [↑](#footnote-ref-2)
3. Prática que envolve o uso de tecnologias de informação e comunicação para dar apoio a comportamentos deliberados, repetidos e hostis praticados por um indivíduo ou grupo com a intenção de prejudicar o outro. [↑](#footnote-ref-3)
4. Nesse sentido *online* significa conectado e/ou compartilhando em sistemas de computadores, especialmente na Internet. [↑](#footnote-ref-4)
5. Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações em multimídia. [↑](#footnote-ref-5)
6. Situação que se caracteriza por agressões intencionais, verbais ou físicas, feitas de maneira repetitiva, por um ou mais alunos contra um ou mais colegas. O termo bullying tem origem na palavra inglesa *bully*, que significa valentão, brigão. [↑](#footnote-ref-6)
7. Correio eletrônico. [↑](#footnote-ref-7)
8. O termo "phishing" faz alusão à palavra inglesa "fishing", que significa "pescaria", em tradução livre. A associação com esta atividade não é mero acaso: o Phishing Scam é uma tentativa de fraude pela internet que utiliza "iscas", isto é, artifícios para atrair a atenção de uma pessoa e fazê-la realizar alguma ação. [↑](#footnote-ref-8)