



UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA

JACSON MACENA SOUZA CRUZ
ROMIVAL BARBOSA DA SILVA

**A VULNERABILIDADE DOS INTERNAUTAS NA
FORMAÇÃO SOCIAL DOS ALUNOS DE 12 A 15 ANOS
DA ESCOLA ESTADUAL DE ENSINO MEDIO
PROFESSORA ELZA MARIA CORREA DANTAS**

MARABÁ, PA.
2014

JACSON MACENA SOUZA CRUZ
ROMIVAL BARBOSA DA SILVA

**A VULNERABILIDADE DOS INTERNAUTAS NA
FORMAÇÃO SOCIAL DOS ALUNOS DE 12 A 15 ANOS
DA ESCOLA ESTADUAL DE ENSINO MEDIO
PROFESSORA ELZA MARIA CORREA DANTAS**

Trabalho de Conclusão de Curso – (TCC)
apresentado a Coordenação Acadêmica do Curso de
Licenciatura em computação da Universidade
federal Rural da Amazônia Campus Universitário de
Marabá – em parceria com o Plano Nacional de
Formação dos Professores da Educação Básica –
PAFOR como requisito primordial para a obtenção
do Título de Licenciada em Computação.

Orientadora: Dra. Leila Weitzel Coelho da Silva

MARABÁ, PA.
2014

JACSON MACENA SOUZA CRUZ
ROMIVAL BARBOSA DA SILVA

**A VULNERABILIDADE DOS INTERNAUTAS NA
FORMAÇÃO SOCIAL DOS ALUNOS DE 12 A 15 ANOS
DA ESCOLA ESTADUAL DE ENSINO MEDIO
PROFESSORA ELZA MARIA CORREA DANTAS**

Trabalho de conclusão do curso de licenciatura em
Computação sendo-lhe atribuída à nota “7,0” (sete),
pela banca examinadora formada por:

Dra. Prof.^a Leila Weitzel Coelho da Silva
Presidente: professor Orientador

Dr. Prof.^o Aurecilio Guedes
Membro: Supervisor de Campo

Prof.^a Rosanny Lima
Membro: Profissional na Área

AGRADECIMENTOS

Jacson Macena Souza Cruz

Agradeço em primeiro lugar a Deus que iluminou o meu caminho durante esta caminhada. Agradeço também a meu pai, RAIMUNDO SOUZA CRUZ FILHO, quem eu rogo todas as noites a minha existência, que de forma especial e carinhosa me deu força e coragem, me apoiando nos momentos de dificuldades, agradeço também aos meus avós RAIMUNDO E SEBASTIANA, que sempre acreditaram no meu potencial, quero agradecer também os meus filhos, CAMILO e JUAN, que embora não tivessem conhecimento disto, mas iluminaram de maneira especial os meus pensamentos me levando a buscar mais conhecimentos. E não deixando de agradecer de forma grata grandiosa a ROMIVAL, PEDRO JUNIOR, ANTONIO ROGERIO E toda minha turma em licenciatura da computação, pois vivemos momento de muito sacrifício em uma luta árdua mais que conseguimos nossos objetivos. A orientadora Leila, pela força, incentivo e empenho dedicado à elaboração deste trabalho.

Romival Barbosa da Silva

Esse trabalho a minha família, em especial a minha mãe Raimunda e minha filha Jeovana pelo apoio que me dedicaram ao longo dessa caminhada, dedicatória muito importante em memória de meu saudoso pai Luiz, que antes de partir me ensinou muitas coisas sobre os valores éticos da vida. Dedico também a todos os professores que passaram durante esses três anos.

Quero também agradecer em primeiro lugar a Deus por ter me dado saúde e força para superar as dificuldades, que surgiram ao longo do curso. A minha filha por entender a minha ausência. A minha mãe por todo apoio e incentivo, por estar do meu lado em todas as dificuldades, quem sempre esteve presente mesmo na minha ausência. Aos professores, sem exceção, poderia citar e listar cada um, trazendo sempre um novo aprendizado, enriquecendo nosso conhecimento. A orientadora Leila, pela força, incentivo e empenho dedicado à elaboração deste trabalho. Ao meu pai que apesar de todas as dificuldades, de sua doença que acabou lhe tirando a vida, me fortaleceu e que para mim foi muito importante. E como não poderia de deixar meus, agradecimentos aos meus amigos de curso, que durante esse tempo construímos uma bela amizade, e em especial Jacson Macena meu parceiro de trabalho, Pedro Junior e Antônio Rogerio.

Sumário

1 INTRODUÇÃO.....	7
1.1 PROBLEMATIZAÇÃO E JUSTIFICATIVA	9
2 A RELAÇÃO SEGURANÇA VS O JOVEM	9
3 REFERENCIAL TEÓRICO	15
4 PRINCIPAIS AMEAÇAS NA INTERNET	18
5 METODOLOGIA	25
6 RESULTADOS	33
7 DISCUSSÃO	36
REFERÊNCIAS BIBLIOGRÁFICAS	38

A VULNERABILIDADE DOS INTERNAUTAS NA FORMAÇÃO SOCIAL DOS ALUNOS DE 12 A 15 ANOS DA ESCOLA ESTADUAL DE ENSINO MEDIO PROFESSORA ELZA MARIA CORREA DANTAS

RESUMO

Este artigo mostra as principais vulnerabilidades dos alunos pré-adolescentes no uso da *internet* na sua formação política, cultural e social. Visto que a aquisição de computadores, celulares e *tablet* com acesso a *Internet* hoje é uma realidade em todo o mundo. Então jovens buscam informações, desde pesquisas escolares até conhecer pessoas de outros lugares do mundo. Com tanta facilidade de acessos devemos nos preocupar com os perigos que a internet nos oferece e pensando nesses perigos desenvolvemos nosso trabalho de conclusão de curso. Buscando também mostrar o papel que a escola deve desempenhar na formação destes alunos no sentido de oferecer uma formação adequada. E em busca desta preparação e identificação social e cultural, acabam recorrendo à rede mundial de computadores que é a *internet*, acessando principalmente redes sociais. E procuramos enfatizar os maiores perigos encontrados na rede mundial de computadores.

Palavras-chaves: Vulnerabilidades; Internet; Cuidados.

ABSTRACT

This article shows the main vulnerabilities of students preteens in using the Internet in their political training, cultural and social. Since the acquisition of computers, cell phones and tablet with access to the Internet today is a great reality worldwide. These young people seek information of all genres since school research, till to meet people from other places in the world. With such ease of access we must be concerned with the dangers that it offers us and thinking about these dangers developed our work course conclusion. Seeking also show the role that schools should play in the formation of these preteens in order to provide adequate training for their preparation mainly for the labor market. And in search of this preparation and social identification and cultural, 7 end up using the world wide web that is the internet, mainly accessing social networks.

So we tried to emphasize the largest the dangers found emphasizing more malware known as viruses, Trojan and worms. So we conducted this work with preteens first year of high school, taking view that is a very vulnerable age group.

Keywords: Vulnerabilities; the Internet; Care.

1 INTRODUÇÃO

Um trabalho que tem análise sobre a vulnerabilidade dos internautas na formação social dos alunos de 12 a 15 anos da Escola Estadual de Ensino Médio Professora Elza Maria Correa Dantas, em consideração às novas tendências tecnológicas e o papel da escola no desenvolvimento desses jovens. Pretende-se ainda mostrar a importância da escola em parceria com a sociedade. Em última análise o que se quer com a pesquisa é mostrar que a maioria dos jovens está procurando uma identificação social, política e também econômica.

A inclusão do ensino médio no âmbito da educação básica e o seu caráter progressivamente obrigatório demonstram o reconhecimento da importância política e social que ele possui. O País já não suporta tamanha desigualdade educacional. Trata-se de uma demanda crescente de escolarização diante da desvalorização dos diplomas em virtude da expansão do ensino e da necessidade de competir no exíguo mercado laboral, bem como de socializar a população em uma nova lógica do mundo do trabalho. “Confundir informação com conhecimento tem sido um dos grandes problemas da nossa educação” (KARNAL, 2008, p. 22).

A construção da cidadania somente ocorrerá se forem cultivados valores que formarão a base de sustentação do comprometimento a escola deve ter como tarefa a formação da Cidadania e ganha seu sentido pleno num contexto democrático, é fundamental verificar a Situação educacional existente hoje no Brasil.

O ensino médio representa apenas os três ou quatro últimos anos da educação básica, mas talvez sejam os mais controvertidos e os que trazem dificuldades no momento de definir políticas para essa etapa da escolarização. Fala-se da perda da identidade, quando na verdade o ensino médio nunca teve uma identidade muito clara, que não fosse o trampolim para a universidade ou a formação profissional.

Segundo MORAN (2013, p 53), “o acesso às Tecnologias da Informação e Comunicação - TIC está relacionado com os direitos básicos de liberdade e de expressão, portanto os recursos tecnológicos são as ferramentas contributivas ao desenvolvimento social, econômico, cultural e intelectual”.

O avanço tecnológico de hardwares e softwares tem proporcionado o barateamento de produtos do ramo da informática, e conseqüentemente estimulado o uso de computadores e outros dispositivos que se conectam à Internet. A Internet causou uma revolução como ferramenta de comunicação, e a cada dia cresce cada vez mais o número de pessoas que usam a Internet como fonte de informação e pesquisa. Informações que em alguns anos atrás só poderiam ser obtidas em materiais impressos, como livros e revistas. Diante deste cenário, a liberdade para produção de conteúdo digital também aumentou, onde qualquer pessoa publicar sobre qualquer assunto.

O incremento do acesso à rede aumentou também, infelizmente, os casos de violações dos direitos humanos pela *Internet* e tem exposto crianças e adolescentes a novas modalidades de risco. Esses novos riscos incluem a violência sexual, como abuso, aliciamento e disseminação de pornografia infanto-juvenil on-line, e ao *cyberbullying*. Criada em 2005 com a missão de promover e proteger os direitos humanos na Internet, a *SAFERNET*¹ trabalha em conjunto com a Polícia Federal e o Ministério Público Federal. As três entidades operam a **CENTRAL NACIONAL DE DENÚNCIAS DE CRIMES CIBERNÉTICOS**², em cooperação com o Ligue 100, da **SECRETARIA ESPECIAL DE DIREITOS HUMANOS - SEDH**. O próprio site da *SAFERNET* abriga esse canal de denúncias, totalmente anônimo, pelo qual recebe relatos apenas sobre violações cometidas em sites, blogs, redes de relacionamento e demais conteúdos on-line (ESTEFENON, 2008).

É possível perceber que as vulnerabilidades existem. Você pode ter os mais perfeitos produtos de segurança, mas eles não serão nada se você não tiver consciência que eles serão gerenciados e utilizados por pessoas, isto nos faz refletir sobre a necessidade de uma infraestrutura de segurança. A exposição a riscos na Internet não resulta necessariamente em dano se os indivíduos estão cautelosos e conscientes dos riscos (LIVINGSTONE et al, 2011).

1 www.safernet.org.br

2 www.denunciar.org.br

1.1 PROBLEMATIZAÇÃO E JUSTIFICATIVA

Percebendo que o aluno está usando a Internet sem um direcionamento adequado, para sua formação cultural, sócia e política, nessa análise percebe-se que estão usando a Internet com jogos, redes sociais e não voltada para sua educação.

Com objetivo de direcionar o aluno de ensino médio adequadamente em relação ao bom uso da *Internet* na formação cultural, sócia e política, colocando a importância da escola que estar integrada com a sociedade e mostrando que a maioria dos jovens está procurando uma identificação social, política e também econômica.

Acredita-se que a orientação dada aos alunos de ensino médio em relação ao bom uso da Internet vem colaborar no seu aprendizado, pois do período de 2005 onde foi implantado o laboratório de informática, podemos analisar que de 2005 até hoje os alunos estão sabendo mais como usar esta a *internet*, que estamos vendo o uso também na sua formação cultural, social e política. Visto que a Internet hoje é uma ferramenta de pesquisa importante na Educação.

2 A RELAÇÃO SEGURANÇA VS O JOVEM

A segurança da informação está relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada

informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade **CIA** - *Confidentiality Integrity Availability* em português **CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE**, representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade e a autenticidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação³.

- **Confidencialidade** - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- **Integridade** - propriedade que garante que a informação mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
- **Disponibilidade** - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Inicialmente, grande parte dos acessos à *Internet* eram realizados por meio de conexão discada com velocidades que dificilmente ultrapassavam 56 Kbps. O usuário, de posse de um *modem* e de uma linha telefônica, se conectava ao provedor de acesso e mantinha esta conexão apenas pelo tempo necessário para realizar as ações que dependessem da rede. Desde então, grandes avanços ocorreram e novas alternativas surgiram, sendo que atualmente grande parte dos computadores pessoais ficam conectados à rede pelo tempo em que estiverem ligados e a velocidades que podem chegar a até 100 Mbps. Conexão à Internet também deixou de ser um recurso oferecido

³ <http://cartilha.cert.br/redes/>

apenas a computadores, visto a grande quantidade de equipamentos com acesso à rede, como dispositivos móveis, TVs, eletrodomésticos e sistemas de áudio.

Independentemente do tipo de tecnologia usada, ao conectar o seu computador à rede ele pode estar sujeito a ameaças, como:

- **FURTO DE DADOS:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador.
- **USO INDEVIDO DE RECURSOS:** um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar *spam*, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante.
- **VARREDURA:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades.
- **INTERCEPTAÇÃO DE TRÁFEGO:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia.
- **EXPLORAÇÃO DE VULNERABILIDADES:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como *modems* e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para *sites* fraudulentos.
- **ATAQUE DE NEGAÇÃO DE SERVIÇO:** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar.

- **ATAQUE DE FORÇA BRUTA:** computadores conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.
- **ATAQUE DE PERSONIFICAÇÃO:** um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

A *Internet* e as novas tecnologias de informação trouxeram um sem-fim de novidades e possibilidades para uma grande parcela da população mundial. Segundo dados da **UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES** (ITU, na sigla em inglês), divulgados no fim de 2008, naquela época já eram mais de 1,5 bilhão de usuários de Internet, entre redes fixas e móveis, em todo o planeta.

O Ibope Inteligência fez um levantamento para traçar o perfil do público brasileiro de *internet*. A pesquisa, realizada entre julho e de dezembro de 2014, mostra que 53% dos usuários são mulheres.

O estudo considerou a população acima de 16 anos e identificou que a maior parcela (52%) de internautas é da classe C. Os números mostram que 34% são da classe B, 10% das classes D/E e 4% da classe A.

Em um panorama geral, 53% dos brasileiros são ativos na *internet*, considerando quem acessou conteúdo online nos três meses anteriores ao estudo. Ao avaliar as regiões, o levantamento concluiu que a região Sudeste 49% dos internautas do país, seguida pelo Nordeste, com 22%, e Sul, com 14%. Centro-Oeste e Norte possuem 8% e 7%, respectivamente.

O acesso é mais comum entre pessoas com escolaridade alta. Dos que concluíram ensino superior, 90% têm acesso à rede. Para os que concluíram o ensino médio, a taxa cai para 71%. Na parcela da população que possui o ensino fundamental, apenas 24% usam a *internet*.

Surpreendentemente, os brasileiros entre 35 e 54 anos são os que mais acessam a internet (representam 34% dos acessos totais do país), logo atrás estão aqueles entre 25 e 34 anos, representando 32% das pessoas que acessam a rede, www.Ibope.inteligencia.org.

Conforme dito anteriormente, o incremento do acesso à rede aumentou também, infelizmente, os casos de violações dos direitos humanos pela Internet e tem exposto crianças e adolescentes a novas modalidades de violência sexual, como abuso, aliciamento e disseminação de pornografia infanto-juvenil on-line, e ao *cyberbullying*. A SAFERNET oferece, oficinas para a formação de educadores, distribuição de kits pedagógicos com conteúdo que ajudam a inclusão do tema nas salas de aula, concurso e projetos engajando os próprios jovens internautas para que se mobilizem em prol da segurança deles mesmos e dos seus pares – como concursos de vídeos e desenhos – e campanhas, a exemplo do Dia Nacional da Internet Segura (9 de fevereiro), ao lado de outras organizações.

Uma pesquisa realizada pela Organização Não-Governamental (ONG) SAFERNET, a fim de identificar vulnerabilidades ouviu 1,4 mil crianças, jovens e pais de todo o País. O estudo foi divulgado pelo MINISTÉRIO PÚBLICO FEDERAL, no dia 9 de outubro de 2011, e revelou que 53% das crianças e adolescentes já tiveram contato com conteúdo agressivo e impróprio na Internet. "Existem muitos pais que não acompanham os filhos na hora em que eles acessam a rede mundial". E complementa, "sem limites, a Internet se torna perigosa. As crianças ficam vulneráveis à ação de criminosos". A pesquisa ainda revelou que 64% dos jovens navegam pela web no próprio quarto, ou seja, os pais não adotam políticas de segurança para orientação dos filhos. Também foi constatado que 87% dos adolescentes afirmam não ter restrições para o uso da *Internet*⁴.

O CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO⁵ lançou o livro *TIC Kids Online Brasil 2012*, resultado de uma pesquisa que mapeou oportunidades e riscos associados ao uso da Internet por crianças e adolescentes brasileiros.

O levantamento de dados foi realizado durante o ano de 2012 com 1.580 entrevistas de crianças e adolescentes entre 9 e 16 anos e mostra como eles acessam e utilizam a *Internet* e os riscos que enfrentam on-line. Além disso, a pesquisa investiga as experiências, práticas e preocupações dos pais relacionadas ao uso da Internet por parte dos seus filhos. O livro também conta com artigos de especialistas de diversas universidades brasileiras na relação entre crianças e *Internet*, que analisam em detalhes alguns indicadores da pesquisa. Os autores afirmam que “não se deve estimular uma visão amedrontada da *Internet* e nem mesmo um encantamento excessivo com esses novos nativos digitais”. O livro também destaca a importância da formação dos professores para educar a nova geração, que já tem a Internet envolvida em suas vidas.

Hoje, quando se fala em crianças e tecnologia, as preocupações quase sempre giram em torno dos dados e do conteúdo. Julgar por sucessivos alertas de especialistas, talvez fosse uma boa ideia dar mais atenção para o próprio acesso a aparelhos, norte-americana COMMON SENSE MEDIA, especializada em questões da família, divulgou ano de 2012, 38% das crianças com menos de dois anos nos EUA já usam dispositivos móveis. Não há números para o Brasil, mas uma pesquisa recente da empresa de segurança AVG mostrou que 97% dos meninos e meninas entre 6 e 9 anos e que têm pais que acessam a Internet também estão conectados. E ainda, a média de horas que os jovens passam na Rede Social *FACEBOOK*, no *Tablets*, *smartphones* e PCs é o triplo da média mundial podem e devem estar presentes no lazer e na educação. Mas é preciso moderação (ESTEFENON, 2008). Pode-se inferir portanto que as crianças brasileiras também são usuárias frequentes de aparelhos eletrônicos. Não se trata de deixar as crianças à margem de uma sociedade cada vez mais tecnológica.

De acordo com a *SAFERNET*, alguns cuidados devem ser tomados com relação ao uso das TICs, são eles:

1. Sempre conversar sobre os sites mais apropriados de acordo com o desenvolvimento e a maturidade de cada um. Aproveitar oportunidades de palestras em escolas ou conversas com amigos sobre a importância da supervisão constante e a proteção sobre os perigos da rede;
2. Estabelecer regras e limites bem claros para a entrada e permanência em salas de bate-papo e serviços de mensagens eletrônicas. Cuidado com envio de fotos e informações particulares para pessoas desconhecidas;

4 www.fisepe.pe.gov.br/cepe/materias2008/out/legi09211008.htm

5 www.cetic.br

3. Denunciar qualquer mensagem esquisita, amedrontadora, obscena, humilhante, inapropriada ou que contenha imagens ou conteúdo pornográfico, no disque 100 ou www.denuncia.org.br;
4. Nunca fornecer sua senha virtual a quem quer que seja, nem aceitar brindes ou prêmios ou convites oferecidos para viagem ou estadas em cidades turísticas ou em qualquer lugar;
5. Limitar o tempo de uso do computador para prestigiar a convivência familiar entre todos, especialmente, manter os hábitos e as horas de sono para descanso cerebral e corporal;
6. Usar filtros de segurança e sistema de segurança on-line atualizado, com bloqueadores de mensagens proibidas ou inseguras para crianças e adolescentes;
7. Ficar atento aos sinais de riscos e características do uso impróprio, exagerado ou doentio do computador e de outras tecnologias, especialmente aos problemas de abuso, pornografia, pedofilia ou exploração comercial sexual de crianças e adolescentes;
8. Participar das redes de proteção social para crianças e adolescentes nas escolas ou comunidades, estimulando a prática de mensagens saudáveis e boicotando e denunciando sites ou empresas que não são considerados "amigos" de crianças e adolescentes.

3 REFERENCIAL TEÓRICO

As novas tecnologias vêm modificando significativamente as relações do homem com o mundo, visto que em cada segmento social encontramos a presença de instrumentos tecnológicos. A escola não pode ficar excluída desta realidade, devendo apropriar-se dos avanços tecnológicos e incorporá-los a prática educativa.

Segundo Lévy (1996), a era atual das tecnologias da informação e comunicação estabelece uma nova forma de pensar sobre o mundo que vem substituindo princípios, valores, processos, produtos e instrumentos que mediam a ação do homem com o meio. Ainda conforme Lévy (1999), pela primeira vez na história da humanidade, a maioria das competências adquiridas por uma pessoa no começo de seu percurso profissional estará obsoleta ao fim de sua carreira.

Com a chegada dos recursos tecnológicos nas escolas, exige-se dos educadores uma nova postura frente à prática pedagógica. Conhecer as novas formas de aprender, ensinar, produzir, comunicar e reconstruir conhecimento, é fundamental para a formação de cidadãos melhor qualificados para atuar e conviver na sociedade, conscientes de seu compromisso, expressando sua criatividade e transformando seu contexto.

Segundo MORAN (2013, p 53), “o acesso às Tecnologias da Informação e Comunicação - TIC está relacionado com os direitos básicos de liberdade e de expressão, portanto os recursos tecnológicos são as ferramentas contributivas ao desenvolvimento social, econômico, cultural e intelectual”.

Integrar as tecnologias como apoio ao ensino aprendizagem é um grande desafio para a educação, especialmente na rede pública de ensino para dar igualdade de condições aos educandos. O educador necessita buscar ferramentas eletrônicas pra atender a necessidade e a curiosidade dos educandos. São necessárias novas competências e atitudes para que o processo ensino-aprendizagem seja significativo.

São vários os recursos tecnológicos que podem facilitar o processo de aprendizagem. O computador, o principal produto das TICs, ganha destaque e importância neste quesito. Rico em recursos audiovisuais possibilita o entrecruzamento de imagens, sons, textos e diversos softwares educativos de apoio aos conteúdos curriculares que podem estimular os alunos para a aprendizagem.

Segundo Mercado (1999, p. 27) as novas tecnologias criam novas chances de reformular as relações entre alunos e professores e de rever a relação da escola com o meio social, ao diversificar os espaços de construção do conhecimento, ao revolucionar os processos e metodologias de aprendizagem, permitindo à escola um novo diálogo com os indivíduos e com o mundo.

Mesmo destacando as vantagens da utilização dos recursos tecnológicos, Mercado (1999, p. 27) considera necessário, além de uma preparação adequada dos professores, um projeto educacional que articule o trabalho do professor ao uso destas tecnologias para que estas possam concretizar seus objetivos, do contrário, corre-se o risco de se confrontar com velhas práticas, mais caras e com um caráter pretensamente moderno ou uma utilização de forma inadequada por parte dos alunos, haja vista que a simples introdução da tecnologia não é capaz de modificar as concepções do professor acerca das questões pedagógicas. O acesso às tecnologias de informação e comunicação amplia as transformações sociais e desencadeia uma série de mudanças na forma como se constrói o conhecimento

As consequências da evolução das novas tecnologias, centradas na comunicação de massa, na difusão do conhecimento, ainda não se fizeram sentir plenamente no ensino como previra *McLuhan* já em 1969, pelo menos na maioria das nações, mas a aprendizagem à distância, sobretudo a baseada na *Internet*, parece ser a grande novidade educacional neste início de novo milênio. A educação opera com a linguagem escrita e a nossa cultura atual dominante vive impregnada por uma nova linguagem, a da televisão e a da informática, particularmente a linguagem da *Internet*. A cultura do papel representa talvez o maior obstáculo ao uso intensivo da *Internet*, em particular da educação a distância com base na *Internet*. Por isso, os jovens que ainda não internalizaram inteiramente essa cultura adaptam-se com mais facilidade do que os adultos ao uso do computador. Eles já estão nascendo com essa nova cultura, a cultura digital.

A educação no Brasil está passando por várias transformações estruturais no que se refere aos aspectos sociais e interacionistas, agregado a isso é possível encontrar as soluções que resolvam ou amenizem as dificuldades encontradas na área no que tange ao melhor conhecimento e aprendizagem dos alunos e a descoberta de práticas consistentes que viabilizem uma educação de qualidade em todas as áreas do ensino.

É possível perceber que as vulnerabilidades existem. Você pode ter os mais perfeitos produtos de segurança, mas eles não serão nada se você não tiver consciência que eles serão gerenciados e utilizados por pessoas, isto nos faz refletir sobre a necessidade de uma infraestrutura de segurança. A exposição a riscos na Internet não resulta necessariamente em dano se os indivíduos estão cautelosos e conscientes dos riscos (LIVINGSTONE et al, 2011).

4 PRINCIPAIS AMEAÇAS NA INTERNET

O termo *malware* é proveniente do inglês *malicious software*; é um *software* destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não).

Vírus de computador incluem as classes: *worms*, *trojan horses* (cavalos de troia) e *spywares* são considerados *malware*. Também pode ser considerada *malware* uma aplicação legal que por uma falha de programação (intencional ou não) execute funções que se enquadrem na definição supra citada.

Entre as principais formas de ação do *malwares* se destacam o Monitoramento de URLs, alteração da Página Inicial do *Browser* do usuário, monitoramento e armazenamento das teclas digitadas e armazenamento da posição do cursor do mouse, mas existem outras formas de atuação. As principais características dos *malwares* mais conhecidos:

Adware: normalmente é um aplicativo que exhibe ou baixa sem autorização, anúncios na tela do computador. Em muitos casos, esse *malwares* vem incorporado a softwares e serviços, como o MSN *Messenger* por exemplo. Não causam danos, na maioria das vezes;

Backdoor: é, na verdade, uma porta de entrada para *malwares*. “Porta dos fundos” – traduzindo literalmente – são falhas no sistema operacional ou em aplicativos que permitem que *crackers* tenham controle remoto sobre o equipamento infectado;

Bots e Botnets: são programas capazes de se propagar utilizando brechas nos softwares em um computador. Permitem comunicação com o invasor, e, portanto, são controlados remotamente;

Cavalo de Tróia – Trojan Horse: são softwares projetados para serem recebidos como “presentes”, um cartão virtual, por exemplo. Além de executar as funções para as quais foram programados, eles executam outras sem o conhecimento do usuário;

Keyloggers: capturam e armazenam as teclas digitadas no computador infectado. Assim, as informações de um *e-mail* ou senhas bancárias, por exemplo, correm riscos;

Spywares: designa uma categoria de malwares que têm como objetivo principal monitorar as atividades de um sistema, enviando os dados e as informações coletadas;

Rootkits: é um conjunto de programas que permite que um invasor se esconda e tenha acesso contínuo ao computador infectado. Esses programas, de modo geral, dificultam a localização do invasor, pois o escondem em usuários e *backdoors*, por exemplo;

Worms: é um tipo de *malware* capaz de se propagar automaticamente por meio de redes, enviando cópias de si para outros computadores, a partir de brechas e falhas em softwares instalados incorretamente, fonte: www.psafes.com/blog

Um vírus é um programa com fins maliciosos, capaz de causar transtornos com os mais diversos tipos de ações: há vírus que apagam ou alteram arquivos dos usuários, que prejudicam o funcionamento do sistema operacional danificando ou alterando suas funcionalidades, que causam excesso de tráfego em redes, entre outros. Os vírus, tal como qualquer outro tipo de *malwares*, podem ser criados de várias formas. Os primeiros foram desenvolvidos em linguagens de programação como C e *Assembly*. Hoje, é possível encontrar inclusive ferramentas que auxiliam na sua criação.

Os vírus recebem esse nome porque possuem características de propagação que lembram os vírus reais, isto é, biológicos: quando um vírus contamina um computador, além de executar a ação para o qual foi programado, tenta também se espalhar para outras máquinas, tal como fazem os vírus biológicos nos organismos que invadem. Os dez piores vírus criados para PC desde o CIH (também conhecido como *Chernobyl*), de 1988, até o *Sasser*, criado por um adolescente alemão em 2004. Estes programas causaram danos econômicos importantes, chegando a bilhões de dólares em alguns casos, além de ocasionarem a perda de uma quantidade considerável de dados e deixarem um grande número de máquinas danificadas. Exemplos de Vírus mais conhecidos.

CIH: Liberado em *Taiwan* em junho de 1988, o CIH infectava *Windows 95*, *98* e arquivos executáveis do *ME*. Ficava residente na memória do *PC* e podia sobrescrever dados no *HD*, tornando-o inoperante. Também conhecido como "*Chernobyl*", o vírus deixou de ser maligno devido à grande migração dos usuários para o *Windows 2000*, *XP* e *NT*, que não são vulneráveis a ele. Os danos causados pelo CIH foram estimados em entre *US\$ 20 milhões* e *US\$ 80 milhões*, além dos dados destruídos fonte: www.psafe.com/blog.

MELISSA: O *W97M/Melissa* tornou-se manchete de tecnologia em março de 1999. Vírus de macro para documentos *Word*, se espalhou rapidamente e forçou empresas como *Intel* e *Microsoft*, entre outras, a fechar seus sistemas de e-mail para conter a praga, que se disseminava via *Outlook*. O vírus, além de se enviar pela *Internet*, modificava documentos do *Word* colocando falas do programa de televisão *Os Simpsons*. Causou danos estimados em *US\$ 300 milhões* a *US\$ 600 milhões*.

ILOVEYOU: Também conhecido como *Loveletter* e *The Love Bug*, o *ILOVEYOU* era um *script* de *Visual Basic* com uma mensagem amorosa e foi detectado pela primeira vez em maio, em *Hong Kong*. Era transmitido via e-mail e continha o anexo *Love-Letter-For-You.TXT.vbs*. Assim como o *Melissa*, o vírus se espalhava via *Outlook*. O programa malicioso sobrescrevia arquivos de música, imagem e diversos outros com uma cópia sua. Como o autor do vírus é filipino e na época naquele país não havia leis contra criação de vírus, ele nunca foi punido. A estimativa dos danos financeiros causados pelo *ILOVEYOU* ficou entre *US\$ 10 bilhões* e *US\$ 15 bilhões*.

CODE RED: O *Code Red* em 2001 era um *worms* que foi liberado em servidores de rede em 13 de julho. Era um bug particularmente perigoso por causa do seu alvo: servidores rodando *Microsoft's Internet Information Server (IIS)*. O *worms* explorava uma vulnerabilidade no sistema operacional do *IIS*. Também conhecido como *Body*, o *Code Red* foi criado para causar o máximo de danos. Na infecção, sites controlados por um servidor atacado exibiram a mensagem "*HELLO! Welcome to http://www.worm.com! Hacked By Chinese!*". *PCs* controlados pelo vírus dirigiram ataques a determinados endereços *IP*, incluindo a *Casa Branca*. Em menos de uma semana, o vírus infectou quase 400 mil servidores pelo mundo. As estimativas dão conta de um milhão de computadores infectados, e danos de *US\$ 2,6 bilhões*.

SQL Slammer: O SQL Slammer em 2003, também conhecido como *Sapphire*, apareceu em 25 de janeiro. Como foi lançado em um sábado, o dano foi baixo em termos de dólares. Ele atingiu 500 mil servidores em todo o mundo e deixou a Coreia do Sul fora do ar por 12 horas. Seu alvo não eram os usuários finais, mas os servidores. Ele infectou 75 mil computadores em 10 minutos e atrapalhou enormemente o tráfego online.

BLASTER: No verão (no Hemisfério Norte) de 2003, os profissionais de TI testemunharam, em rápida sucessão, o aparecimento dos *worms Blaster* e *Sobig*. O *Blaster*, também conhecido com *Lovsan* ou *MSBlast*, foi o primeiro. Detectado em 11 de agosto, ele se espalhou rapidamente. Explorava uma vulnerabilidade dos Windows 2000 e XP, e quando ativado, apresentava o usuário com uma mensagem avisando que uma queda do sistema era iminente. Em seu código havia instruções para um ataque DDoS contra o site *windowsupdate.com*, programado para o dia 15 de abril. Centenas de milhares de PCs foram infectados, e os danos ficaram entre US\$ 2 bilhões e US\$ 10 bilhões.

SOBIG.F: O Sobig surgiu em seguida ao *Blaster*, transformando agosto de 2003 num mês para usuários corporativos e domésticos de PC. A variante mais destrutiva foi a *Sobig.F*, que se espalhou tão rápido a partir do dia 19 que chegou a estabelecer um recorde, gerando mais de um milhão de cópias em apenas 24 horas. Em 10 de setembro, o vírus se desativou e deixou de ser uma ameaça. A *Microsoft* chegou a oferecer uma recompensa de US\$ 250 mil para quem identificasse o criador do Sobig.F, mas até hoje ninguém foi apanhado. Os danos foram estimados entre US\$ 5 a US\$ 10 bilhões, com mais de um milhão de PCs infectados.

BAGLE: Um *worm* clássico e sofisticado, o *Bagle* foi posto em ação em 18 de janeiro. Ele infectava os sistemas pelo método tradicional - vinha anexado a um *email* - e vasculhava arquivos do *Windows* em busca de endereços de e-mail que pudesse utilizar para se replicar. O verdadeiro perigo do *worm*, também conhecido com *Beagle*, e suas 60 a 100 variantes é que, ao infectar o PC, ele abria uma porta que permitia o controle total e a distância do sistema. O *BAGLE.B* foi desenhado para parar de se espalhar depois de 28 de janeiro do mesmo ano, mas numerosas outras variantes

continuam a incomodar até hoje. Os danos foram estimados em dezenas de milhões de dólares, e a contagem continua.

MyDoom: Por um período de quatro horas em 26 de janeiro de 2004, o choque do *MyDoom* pôde ser sentido em todo o mundo enquanto o *worm* se espalhava numa velocidade sem precedentes pela *Internet*. A praga, também conhecida como *Norvarg*, se espalhou em um arquivo anexado que parecia ser uma mensagem de erro, com o texto "*Mail transaction failed*", e via compartilhamento de arquivos entre os usuários da rede P2P *Kazaa*. A sua replicação foi tão bem-sucedida que especialistas em segurança de PCs calcularam que uma em cada dez mensagens de *email* enviadas durante as primeiras horas da infecção continham o vírus. Ele estava programado para parar de agir depois de 12 de fevereiro 2004, mas em seu auge chegou a diminuir em 10% a performance global da *Internet* e aumentar o tempo de carregamento dos sites em 50%.

SASSER: Criado por um adolescente alemão (17 anos de idade), o *Sasser* surgiu em maio de 2004 começou a se espalhar em abril do mesmo ano, e foi destrutivo o bastante para deixar fora do ar o satélite de comunicações para algumas agências de notícias da França. Também resultou no cancelamento de vários vôos da *Delta Airlines* e na queda do sistema de várias companhias ao redor do mundo. Diferente da maioria dos *worms* que o antecederam, o *Sasser* não era transmitido por *email* e não precisava de nenhuma ação do usuário para se instalar. Ele explorava uma falha de segurança em sistemas rodando *Windows 2000* e *XP* desatualizados. Quando conseguia se replicar, procurava ativamente por outros sistemas desprotegidos e se transmitia a eles. Os sistemas infectados experimentavam quedas repetidas e instabilidade. Como o autor ainda era menor de idade quando criou o vírus, um tribunal alemão considerou-o culpado por sabotagem de computadores, mas suspendeu a sentença. O *Sasser* causou dezenas de milhões de dólares em prejuízos.

Um **Worms** é uma classe de vírus (verme, em português) é um programa auto replicante. O *Worms* é um programa completo e não precisa de outro para se propagar. Um *worms* pode ser projetado para tomar ações maliciosas após infestar um sistema, além de se autorreplicar, pode deletar arquivos em um sistema ou enviar documentos por *e-mail*. A partir disso, o *worms* pode tornar o computador infectado vulnerável a outros ataques e provocar danos apenas com o tráfego de rede gerado pela sua

reprodução – o *Mydoom*, por exemplo, causou uma lentidão gerada na rede de computadores mundial nos níveis mais alto de seu ataque. O primeiro *worms* que atraiu grande atenção foi o *Morris Worms*, escrito por Robert T. Morris Jr no Laboratório de Inteligência Artificial do MIT. Ele foi iniciado em 2 de novembro de 1988, e rapidamente infectou um grande número de computadores pela *Internet*. Ele se propagou através de uma série de erros no BSD Unix e seus similares. *Morris* foi condenado a prestar 400 horas de serviços à comunidade e pagar uma multa de US\$10.000.

Os *worms Sobig e Mydoom* instalaram *backdoors* (brechas) nos computadores, tornando-os abertos a ataques via *Internet*. Estes computadores "zumbis" são utilizados para enviar *emails* (spams) ou para atacar endereços de sites da *Internet*. Acredita-se que *spammers* (pessoas que enviam *spams*) pagam para a criação destes *worms*, e criadores de *worms* já foram apanhados vendendo listas de endereços IP de máquinas infectadas. Outros tentam afetar empresas com ataques DDOS (Ataque de Negação de Serviço) propositais. As brechas podem também ser exploradas por outros worms, como oDoomjuice, que se espalha utilizando uma brecha aberta pelo Mydoom.

Os *worms* podem ser úteis: a família de worms Nachi, por exemplo, tentava buscar e instalar *patches* do site da Microsoft para corrigir diversas vulnerabilidades no sistema (as mesmas vulnerabilidades que eles exploravam). Isto eventualmente torna os sistemas atingidos mais seguros, mas gera um tráfego na rede considerável — frequentemente maior que o dos worms que eles estão protegendo — causam reboots da máquina no processo de aplicação do patch e, talvez o mais importante, fazem o seu trabalho sem a permissão do usuário do computador. Por isto, muitos especialistas de segurança desprezam os worms, independentemente do que eles fazem.

O **Cavalo de Tróia ou Trojan Horse** é um tipo programa malicioso que podem entrar em um computador disfarçados como um programa comum e legítimo. Ele serve para possibilitar a abertura de uma porta de forma que usuários mal intencionados possam invadir seu PC. Seu nome surgiu devido à história da guerra de Tróia e que culminou com a destruição desta. O cavalo de Tróia, um grande cavalo de madeira, fora supostamente oferecido como um pedido de paz por parte dos gregos. Sendo um presente para o rei, os troianos levaram o cavalo para dentro das muralhas da cidade.

Durante a noite, quando todos dormiam, revelou-se uma armadilha e os soldados gregos que se escondiam dentro da estrutura oca de madeira do cavalo saíram e abriram os portões para que todo o exército entrasse e queimasse a cidade. Assim como na história, um Trojan se passa por um programa que simula alguma funcionalidade útil quando de fato ele esconde um programa que pode causar malefícios aos computadores e seus usuários, como abrir portas e possibilitar invasões ou roubar senhas de usuário. A principal forma de propagação destes é pela internet, onde são oferecidos como ferramentas com funções úteis – ou até mesmo vitais – para os computadores. Os dois tipos mais comuns de Trojans são os *Keyloggers* (que normalmente são utilizados para roubar senhas) e os *Backdoors* (arquivos que possibilitam aberturas de portas para invasão). Diferente dos Vírus e *Worms*, eles normalmente não se auto copiam, não necessitam infectar outros programas para executar suas funções: eles são autônomos necessitando apenas ser executados, costumam instalar-se com arquivos que quando apagados podem gerar perda de dados.

Como eles são menos limitados podem ser potencialmente mais perigosos e as vezes não são identificados como ameaças. Assim, como uma forma de prevenção, arquivos executáveis desconhecidos ou de origem duvidosa, ainda que não sejam acusados como ameaças pelos antivírus, devem ser executadas com cautela. Uma medida de segurança simples, porém eficaz é tomar cuidado com arquivos executáveis vindos de terceiros. O ideal seria utilizá-los somente quando se tem certeza de sua procedência, para evitar incômodos futuros. E, como via de regra, é sempre recomendado manter um bom antivírus instalado e sempre em dia com as atualizações.

5 METODOLOGIA

Foi desenvolvida na Escola Estadual de Ensino Médio Professora Elza Maria Correa Dantas. Logo abaixo é apresentada a descrição da escola.

A Escola Estadual de Ensino Fundamental e Médio Prof^a. Elza Maria Corrêa Dantas foi fundada e entregue á população são-dominguense em 08 de março de 1991.

Localizada às margens da BR 230, especificamente à travessa Alacid Nunes, Qd. Especial, Bairro Novo São Domingos, na Cidade de São Domingos do Araguaia, CEP 68.520.000, com uma área de aproximadamente 8100 metros quadrados. Tendo como Unidade mantenedora a Secretaria Executiva de Estado de Educação do Pará- SEDUC, contemplada pelos recursos financeiros federais: Programa Dinheiro Direto na Escola – PDDE e PDE destinados a suprir as necessidades básicas da escola, através de parcelas anuais, administrados pelo Conselho Escolar e pela gestão da escola.

Inicialmente a escola ofertava as seguintes modalidades de ensino: 1ª a 8ª série do Ensino Fundamental e Ensino médio – Magistério.



Figura 1: Entrada Principal da Escola



Figura 2: Dependências Internas da Escola

Atualmente, com a municipalização do ensino Fundamental, a escola atende apenas o Ensino Médio, com uma demanda de 529 alunos na 1ª Série, 401 alunos na 2ª Série e 275 alunos na 3ª Série, totalizando 1205 alunos no ano letivo 2011, distribuídos em 32 turmas, nos três turnos, a saber, manhã, tarde e noite. Destacamos que parte dessa clientela é advinda da zona rural, por esse motivo há necessidade de utilização do transporte escolar, que é mantido pela prefeitura em parceria com o governo do estado, através do convênio PNATE, que é firmado anualmente através de termos de adesão entre as Secretarias Municipal e Estadual, junto ao MEC. Diante do contexto, os alunos da rede municipal, oriundos da zona rural dividem o transporte com os alunos da rede estadual.

Então escola e formada assim, os professores que trabalham na referida escola, tem as seguintes formações (ver tabela 1).

Tabela 1: Formação dos professores da escola

Nº DE SERVIDORES	CARGO FUNÇÃO	FORMAÇÃO	SEGMENTO
05	Professor	Lic. Letras	1ª a 3º Serie
02	Professor	Lic. Letras/Hab. Ling. Est.	1ª a 3º Serie
03	Professor	Lic. História	1ª a 3º Serie
04	Professor	Lic. Geografia	1ª a 3º Serie
01	Professor	Lic. Educ. Física	1ª a 3º Serie
03	Professor	Lic. Biologia	1ª a 3º Serie
04	Professor	Lic. Matemática	1ª a 3º Serie
02	Professor	LP. Pedagogia	1ª a 3º Serie
04	Professor	Lic. Sociologia	1ª a 3º Serie

Os turnos e as turmas são assim definidos (ver tabela 2).

Tabela 2- Distribuição dos turnos e turmas

SEGMENTO SERIE	Nº TURMAS	TURNOS	HORA
1ª Série	05	Manhã	07:00hs-12:00hs
2ª Série	03	Manhã	07:00hs-12:00hs
3ª Série	02	Manhã	07:00hs-12:00hs

1ª Série	04	Tarde	13:00hs-17:00hs
2ª Série	03	Tarde	13:00hs-17:00hs
3ª Série	02	Tarde	13:00hs-17:00hs
1ª Série	05	Noite	19:00hs-23:00hs
2ª Série	04	Noite	19:00hs-23:00hs
3ª Série	04	Noite	19:00hs-23:00hs

Em relação à estrutura física, podemos considerar que o espaço é apropriado, necessitando ainda da aquisição de um auditório para realização de eventos educativos e culturais na escola. O prédio encontra-se em perfeito estado de funcionamento, uma vez que, passou recentemente por uma reforma e ampliação com construção de dois ambientes: um laboratório de informática e um multifuncional. Além de uma cobertura na Quadra Poliesportiva, já existente na escola.

- **I PAVILHÃO:** Uma Biblioteca, uma sala da direção, uma sala de professores, uma sala de secretaria, dois banheiros para funcionários, uma sala de coordenação pedagógica e orientação educacional e uma sala de arquivos.
- **II PAVILHÃO:** Um laboratório de informática, uma sala de monitoramento, uma sala de laboratório multifuncional e uma quadra poliesportiva.
- **III PAVILHÃO:** um recreio coberto, um depósito para armazenamento da merenda escolar, uma sala para professores de educação física, uma sala de leitura, banheiro feminino para alunos, banheiro masculino, banheiro para alunos PNEE e um depósito de livros;
- **IV PAVILHÃO:** 04 salas de aula
- **V PAVILHÃO:** Térreo: quatro salas de aula e escadaria; 1ª andar: quatro salas de aula e escadaria.

Com um grande número de turmas a escola acolhe a mais diversa gama de alunos, migrantes das mais variadas regiões do país, compondo assim uma diversidade social, étnica, cultural e econômica bastante expressiva, com certa predominância do estado do Maranhão. O município não oferece tantas condições para que os jovens ingressem no mercado de trabalho formal.

A *Internet* junto com um conjunto de comportamento cultural, social e política dos alunos do ensino médio, além de interferir seriamente na questão disciplinar, provocam um índice bem expressivo de aprovação com dependência de estudos, evasão e até crises familiares abalando muito a estrutura pessoal e social do aluno.

Foi selecionada as turmas de 1º ano “A” e “B” no turno matutino com o objetivo de identificar as contribuições e a importância da *Internet* na formação cultural, social e política dos alunos do ensino médio na Escola Estadual Elza Dantas, dando ênfase aos perigos da *Internet*.

Durante o desenvolvimento do trabalho foi feito um levantamento das principais ameaças (vulnerabilidades) da *Internet* que pode afetar na formação social dos adolescentes que foram descritas no Capítulo 4.



Figura 3: Palestrante Jacson

No desenvolvimento do Trabalho foi elaborado um questionário para ser aplicado antes e depois de uma palestra. A estratégia da pesquisa é conforme especificada abaixo. Em um primeiro momento é aplicado um questionário sobre as vulnerabilidades que a *Internet* possui, com o intuito de verificar o conhecimento das pessoas sobre este tema. O questionário é então recolhido e logo a seguir é dada uma palestra que trata de mostrar para os alunos como proteger – se dentro da rede mundial de computadores. Na realidade a palestra é um alerta e uma aula sobre segurança na *Internet*, ou seja, como evitar os riscos e as vulnerabilidades.



Figura 4: Palestrante Romival

Momento da palestra no qual começamos a falar o que os vírus são capaz de fazerem nos computadores e celulares. Explicação para os alunos que os vírus podem destruir vidas e os criadores deles usam para furtar dados de outros usuários.



Figura 5: Alunos assistindo a palestra

Adolescente concentrados na palestra e tirando suas duvidas sobre o tema abordado.



Figura 6: Alunos dos 1º ano A e B

Adolescentes participando da palestra através de perguntas sobre Cavalo de Tróia, Vírus e outros *malwares*.



Figura 7: Encerramento da palestra

Alunos respondendo o questionário aplicado no final da palestra. O primeiro questionário contém perguntas de cunho pessoal e perguntas sobre o comportamento na Internet, estas perguntas são do tipo resposta fechada e as possibilidades de resposta são binárias – SIM e NÃO

Tabela 3: Primeiro questionário aplicado

PERGUNTA	RESPOSTA
Sexo	MASC. () FEM. ()

Você tem Computador em Casa?	SIM () NÃO ()
Sente-se seguro em usar o Computador?	SIM () NÃO ()
Tem Internet?	SIM () NÃO ()
Sente-se seguro em usar a Internet?	SIM () NÃO ()

Após a realização da palestra foi aplicado um novo questionário para vermos a opinião dos alunos sobre a política de segurança da Internet e os cuidados que os mesmos tinham em acessar a Internet, com as seguintes perguntas.

Tabela 4: Segundo questionário aplicado

PERGUNTA	RESPOSTA
Você ainda se sente seguro com relação a usar o computador?	SIM () NÃO ()
Depois disto você pretende adotar mais medidas de segurança como antivírus atualizado?	SIM () NÃO ()

1 RESULTADOS

Os resultados do questionário tabulado em planilha eletrônica e ilustrados através de gráficos. Na Figura têm-se os dados tabulados do gênero dos entrevistados. Verifica-se que o sexo masculino é pequena maioria,



Figura 8: Tabulação do gênero dos entrevistados

Este gráfico mostra o gênero dos alunos entrevistado. Onde dos vinte alunos 55% eram masculino e 45% femininos.

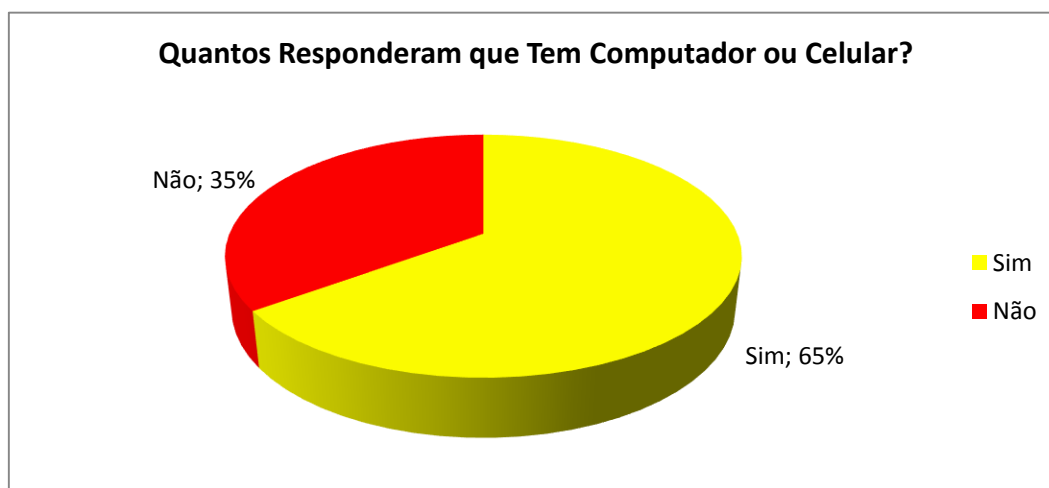


Figura 9: Quantos Responderam que Tem Computador ou Celular?

Dos vinte alunos entrevistados 65% responderam que tem computador ou celular em casa e 35% dizem que não possui computador e nem celular

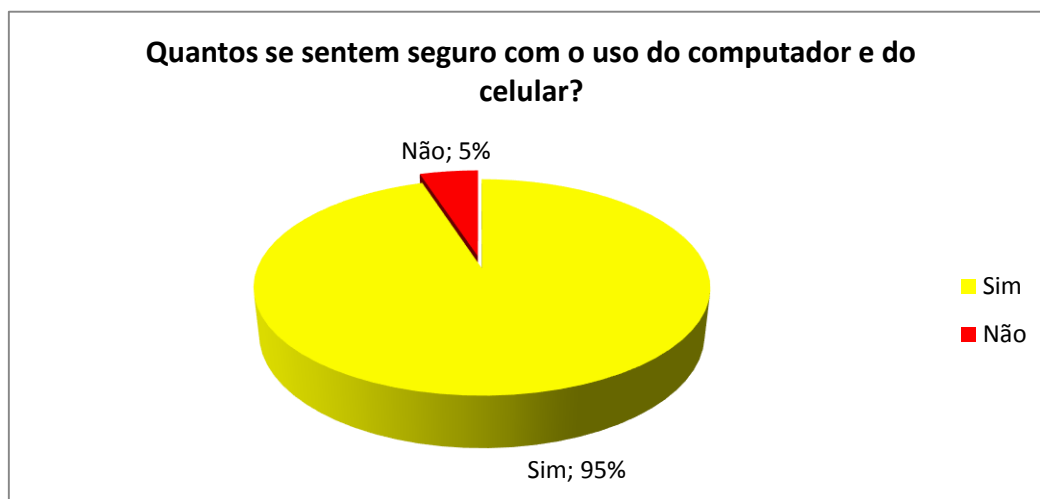


Figura 10: Quantos se sentem seguros com o uso do computador e do celular?

Nesta pergunta 95% responderam que se sentem seguros em usar o computador ou o celular e somente 5% dos entrevistados não se sentem seguros em usar esses equipamentos.

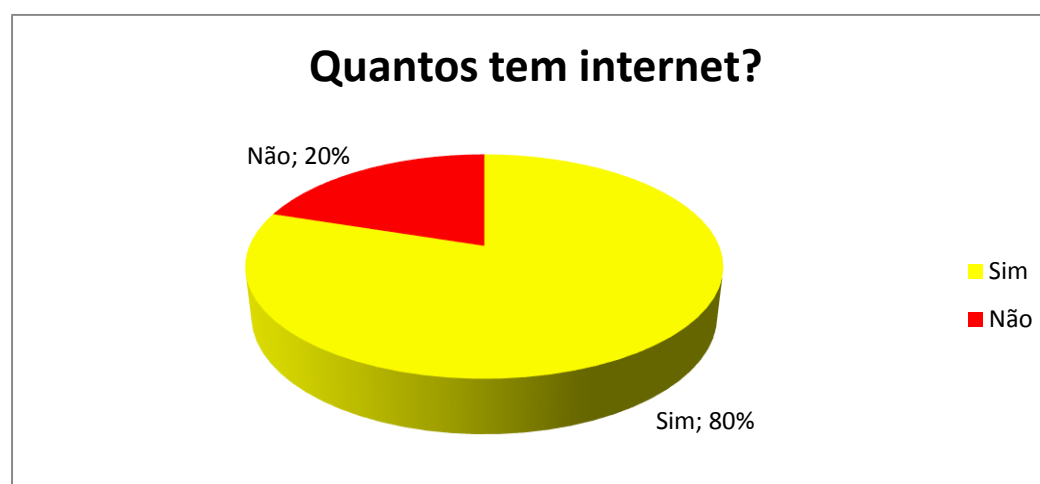


Figura 11: Quantos tem internet?

Aqui, nesta pergunta 80% dos alunos entre meninos e meninas responderam que tem Internet e 20% disseram que não possuem Internet.

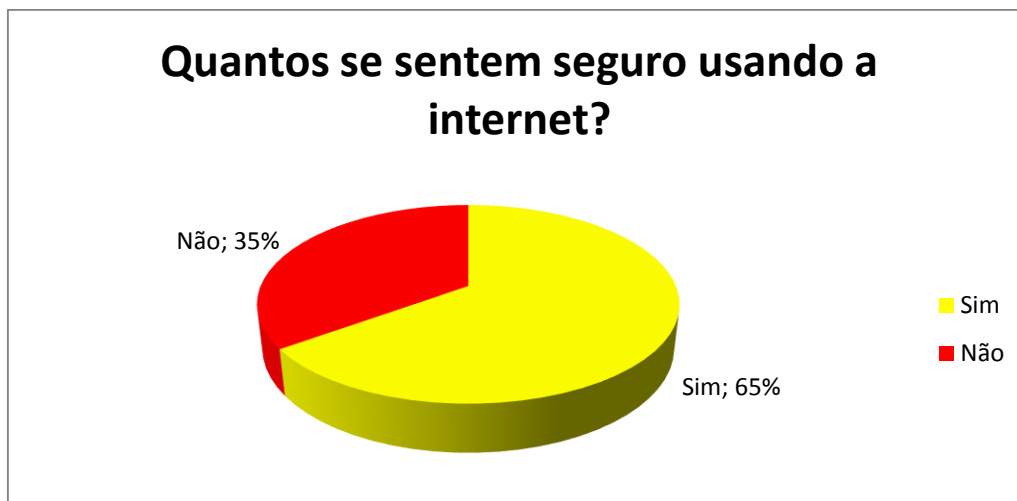


Figura 12: Quantos se sentem seguro usando a internet?

Dos que responderam o questionário 65% disseram que se sentem seguros em usar a Internet, já 35% não se sentem seguros.

Após realizarmos a palestra voltamos a fazer uma pesquisa em forma de questionário com os mesmo vinte alunos.

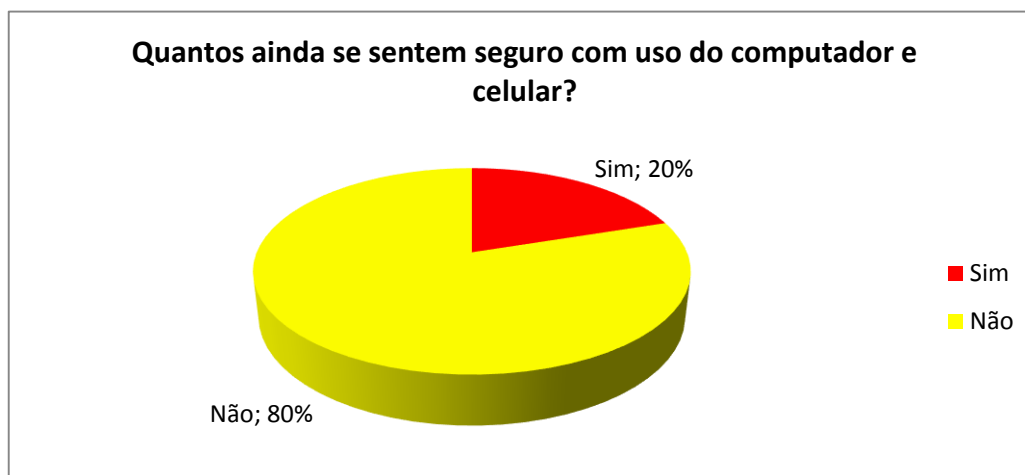


Figura 13: Quantos ainda se sentem seguro com uso do computador e celular?

Após nossa palestra podemos perceber que a opinião da maioria dos alunos mudou em relação ao uso de computadores e principalmente da Internet. Dos alunos entrevistados novamente somente 20% dos alunos continuam se sentindo seguros em relação ao uso da Internet, já 80% dos entrevistados não se sentem seguros em usar a Internet.

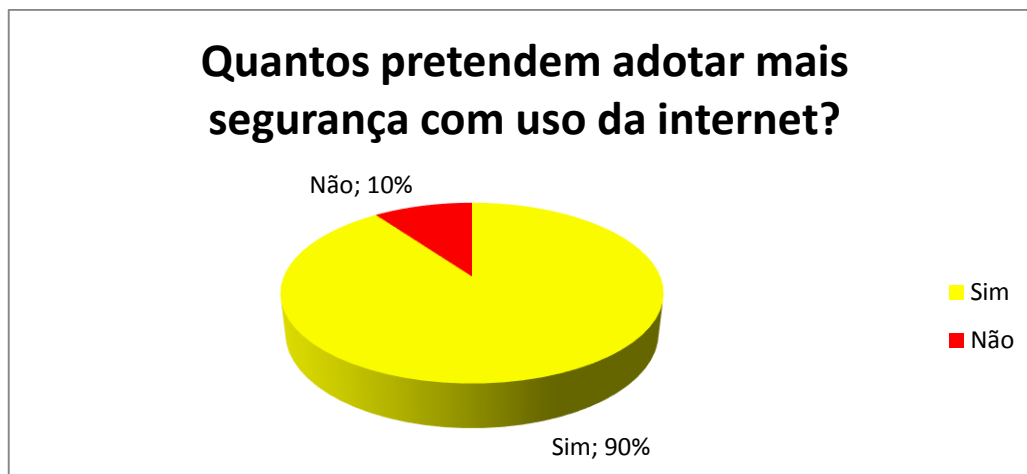


Figura 14: Quantos pretendem adotar mais segurança com uso da internet?

Dos que responderam o questionário 90% pretendem adotar uma maior segurança em relação ao uso da Internet, como antivírus atualizados e apenas 10% disseram que não tomariam nenhuma medida de segurança, pois já se sentem seguros.

A pesquisa proposta é de caráter qualitativo e exploratório visando elucidar o problema abordado.

No intuito de atingir os objetivos, são sugeridas as seguintes abordagens para a realização da presente pesquisa:

- Será feito um profundo estudo sobre o uso da Internet na formação cultural, social e política dos alunos de ensino médio.

As informações serão coletadas através de dados bibliográficos de livros, artigos relacionados à área de pesquisa e dados disponibilizados na Web. Para o TCC dos alunos do curso de Licenciatura em Computação.

7 DISCUSSÃO

Consideração às novas tendências tecnológicas e o papel da escola no desenvolvimento desses jovens. Fazer também um levantamento, mostrando as principais vulnerabilidades e as maiores ameaças que os alunos estão sujeitos.

Foi feito um levantamento bibliográfico sobre os perigos da internet e as vulnerabilidades que estamos sujeitos. Desta forma realizamos uma palestra com pré-adolescentes do 1º ano médio da Escola Elza Dantas em São domingos do Araguaia-Pará. Nesta palestra foram abordados os perigos ao qual estamos sujeitos e os males que podem nos causar se não tomarmos as devidas precauções.

Desta forma foi feito um breve histórico sobre os malware ou softwares maliciosos, dando destaque para os vírus, worms e Cavalo de Troia. Fazendo uma diferenciação entre eles e como cada um ataca, como você é infectado e por fim quais males provoca ao usuário.

No inicio da palestra foi aplicado um questionário para sabermos o que os adolescentes pensavam sobre o assunto, se sentem seguro ou usar o computador e consequentemente a internet.

Durante a palestra foram surgindo varias perguntas por parte dos adolescentes que se mostraram bastantes interessados no assunto, pois a maioria deles não tinham conhecimentos dos riscos que corriam em usar indiscriminadamente e sem nenhuma proteção a Internet.

Ao final foi aplicado um novo questionário para sabermos o que continuavam pensando sobre os perigos da Internet, e podemos perceber que a maioria deles mudaram de opinião sobre está ou não seguros ao usar a Internet.

Podemos ao final concluirmos que falta uma politica de educação voltada para essa nova geração de adolescentes, visto que os meios tecnológicos estão acessíveis a praticamente todo adolescente e a Internet é uma ferramenta presente na vida de cada um deles. E como não há uma politica de conscientização e de prevenção sobre os perigos que os mesmos correm ao acessarem a rede mundial de computadores, muitos acabam caindo em verdadeiras armadilhas e muitas vezes irreversíveis.

Assim podemos contribuir com nosso conhecimento e esclarecimentos sobre esses perigos e desta forma atentá-los para que possa se precaver dos malwares da Internet.

Enquanto acadêmicos tivemos um bom aprendizado, visto que conseguimos aplicar na sociedade o que foi aprendido em sala de aula. Também foi de fundamental importância para nosso aprendizado pessoal e profissional.

REFERÊNCIAS BIBLIOGRÁFICAS

BUFFA, Ester. **Educação e cidadania: quem educa o cidadão.** 3 ed. São Paulo: Cortez, 2003. 95 p.

FRANCO, M. L. P. B. **Ensino médio: desafios e reflexões.** 2.ed. São Paulo: Papirus, 2007.

KARNAL, Leandro. **História na sala de aula.** 5 ed. São Paulo: Contexto, 2008.

LIVINGSTONE, S., Haddon, L., Görzig, A., e Ólafsson, K. (2011). **Risks and safety on the Internet: The perspective of European children. Full findings.** LSE, London: EU Kids Online. Outros relatórios e detalhes técnicos em www.eukidsonline.net

MORAN, José Manuel. **Desafios da Internet para o professor.** Disponível em: <http://www.eca.usp.br/prof/moran/i>. Acesso em: 17. Julho. 2013.

ROSANI CARVALHO. **AS TECNOLOGIAS NO COTIDIANO ESCOLAR: POSSIBILIDADES DE ARTICULAR O TRABALHO PEDAGÓGICO AOS RECURSOS TECNOLÓGICOS.**

ESTEFENON SGB, Eisenstein E org.: **2008 Geração Digital: Riscos e Benefícios das Novas Tecnologias para Crianças e Adolescentes,** Rio de Janeiro, Ed Vieira & Lent, 222p