UNIVERSIDADE FEDERAL DO ACRE

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

LUCAS CAMPELO VIEIRA

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE INFLUÊNCIAS E COMPORTAMENTOS NO USO DA INTERNET, SOB UM CONTEXTO DE SEGURANÇA, NA GERAÇÃO MILÊNIO

RIO BRANCO

2019

LUCAS CAMPELO VIEIRA

TRABALHO DE CONCLUSÃO DE CURSO

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE INFLUÊNCIAS E COMPORTAMENTOS NO USO DA INTERNET, SOB UM CONTEXTO DE SEGURANÇA, NA GERAÇÃO MILÊNIO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título Bacharel em Sistemas de Informação, do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Acre.

Orientador: Prof. Me. Wilker Luiz Gadelha Maia

RIO BRANCO

2019

Ficha catalográfica elaborada pela Biblioteca Central da UFAC

V658s Vieira, Lucas Campelo, 1994 -

Segurança da informação: um estudo sobre influências e comportamentos no uso da internet, sob um contexto de segurança, na geração Milênio / Lucas Campelo Vieira; orientador: Prof. Me. Wilker Luiz Gadelha Maia. - 2019.

73 f.: il.; 30 cm.
Monografia (Graduação) - Universidade Federal do Acre, Centro de Ciências Exatas e Tecnológicas, Curso de Bacharelado em Sistemas de Informação. Rio Branco, 2019.
Inclui referências e apêndice.

1. Segurança da informação 2. Tecnologia 3. Internet - riscos I. Maia, Wilker Luiz Gadelha (orientador) II. Título

CDD: 004

Ficha catalográfica elaborada pela bibliotecária Kezia Santos CRB-11/508

TERMO DE APROVAÇÃO

LUCAS CAMPELO VIEIRA

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE INFLUÊNCIAS E COMPORTAMENTOS NO USO DA INTERNET, SOB UM CONTEXTO DE SEGURANÇA, NA GERAÇÃO MILÊNIO

Esta monografia foi apresentada como trabalho de conclusão de curso de bacharelado em sistemas de informação da universidade federal do acre, sendo aprovado pela banca constituída pelo professor orientador e membros abaixo mencionados.

Compuseram a banca:

Prof. Wilker Luis Gadelha Maia, Me.
Curso de Bacharelado em Sistemas de Informação

Prof. Jean Gonzaga Souza de Oliveira, Me.
Curso de Bacharelado em Sistemas de Informação

Prof. Laura Costa Sarkis, Dra.
Curso de Bacharelado em Sistemas de Informação

Rio Branco, 21 de fevereiro de 2019.

AGRADECIMENTOS

Primeiramente a Deus por ter me proporcionado todas as condições necessárias para cursar este curso e realizar este trabalho. Á minha família, principalmente minha mãe e minha vó que sempre estiveram presentes em todas as necessidades. À minha namorada que ajudou diretamente nos estudos deste curso. Ao meu orientador, que apesar dos problemas particulares procurou atender as necessidades solicitadas. A esta universidade, seu corpo docente, direção e administração que possibilitou realizar o sonho de cursar o curso de Sistemas de Informação. E a todos os demais que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

O avanço tecnológico vem interferindo diretamente com os seres humanos, um exemplo disso é a internet, através dela é possível se relacionar com pessoas em qualquer lugar do mundo, fazer compras, realizar vendas, assistir vídeos, ouvir músicas, ler livros, se profissionalizar, acompanhar notícias e muitas outras possibilidades que o mundo digital oferece. Por outro lado, também existem perigos no mundo digital, há sempre pessoas querendo se aproveitar de pessoas descuidadas, leigas ou até inocentes na internet, que estão sempre em busca de acessar dados pessoais para divulgação ou proveito financeiro. O objetivo do presente trabalho é demonstrar conceitos de boas práticas de utilização da Internet e avaliar o nível de conhecimento dos concluintes do ensino fundamental a respeito dos riscos de segurança atrelados ao uso da Internet, assim como divulgar uma cartilha com orientações de boas práticas tanto para os estudantes entrevistados como para a sociedade em geral. Também foi considerado de grande importância expor conceitos de inclusão digital, fator que contribui para o avanço contínuo no acesso à tecnologia. Embora existam ferramentas que auxiliam na prevenção de ataques, elas não são suficientes perante as avançadas técnicas utilizadas pelos criminosos, por isso se faz necessário ter conhecimento sobre os riscos, e assim tomar medidas preventivas para evitá-los. O desenvolvimento da cartilha com orientação digital tornou-se possível através da pesquisa de conceitos técnicos e da análise dos resultados da pesquisa quantitativa.

Palavras-chave: 1. Segurança. 2. Internet. 3. Riscos. 4. Tecnologia. 5. Informação.

ABSTRACT

The technological advance is interfering directly with human beings, an example of this is an internet, through it is possible to relate to people anywhere in the world, to make purchases, to make sales, to watch videos, to listen to music, to read books, to resemble, What is the digital world offers? On the other hand, there are also dangers in the digital world, there are people who want to benefit from careless, careless, careless or even innocent people on the internet, who are always looking for personal data for advertising or financial gain. The Internet Information Program is the use of the Practices of the risk of knowledge of the Internet is the risk of knowledge of the fundamental risk in the risked the risk to use the Internet cards the students interviewed as for a society in general. It was also considered of great importance to expose concepts of digital inclusion. There are tools that help prevent gun trafficking, which can be used as advanced precautions for criminals so that they can become more aware of the risks as well as take preventive measures to prevent them. The development of the primer with digital orientation became possible through the research of technical concepts and the analysis of the results of the quantitative research.

Keywords: 1. Security. 2. Internet 3. Risks 4. Technology. 5. Information

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A busca por informação sempre foi uma característica do ser humano, sempre buscando ficar atualizado todos os dias, desde do primeiro sistema de comunicação chamado rádio por meio das frequências (AM e FM) até os meios de comunicações mais atuais como a televisão que transmitem som e imagem em alta frequência.

As pessoas sempre buscam novas formas de socializar e trocar informações e conhecimentos não se contentam apenas com os sistemas já existentes. Talvez por isto mesmo, deu-se o surgimento de um dos maiores avanços da humanidade até hoje, relacionado a comunicação chamado internet.

No Brasil, o surgimento da internet deu início com modems ligados às linhas telefônicas, por ser uma infraestrutura básica e que já era existente. Esse modelo tornou-se conhecido como banda estreita pois sua velocidade era bastante reduzida e atingia apenas 56 Kbps apenas.

Com os atuais avanços da tecnologia, existem as redes de fibra óptica, que já estão em fase de testes no Brasil. Essa tecnologia resolve problemas de velocidade e distância por utilizar um sistema um filamento de vidro transparente com alto grau de pureza.

Com a chegada dos celulares conhecidos como "*smartphones"* cresceu bastante o número de pessoas com acesso a internet, pois anteriormente o acesso era feito através de um computador pessoal, que tinha um custo elevado e era necessária uma rede fixa com telefone para assim obter acesso à internet, enquanto hoje em dia vários estabelecimentos oferecem acesso gratuito à internet.

Com tanta tecnologia à disposição e pessoas conectadas surgiram vários problemas com a segurança dos dados destas pessoas. Nesse sentido, o trabalho aborda questões que cercam o uso da Internet, as ameaças atuais as quais os usuários são expostos, assim como formas para prevenção e boas práticas de utilização desse recurso. Também foi realizada uma pesquisa através de um questionário, com a intenção de

mensurar o nível de conhecimento dos alunos concluintes do ensino fundamental da região de Rio Branco - Acre sobre os riscos de segurança que o uso da Internet de forma desorientada pode causar. Por fim, com o resultado da pesquisa em mãos, foi desenvolvida e divulgada uma cartilha com as boas práticas de uso da Internet e segurança digital.

1.1 JUSTIFICATIVA

O avanço tecnológico vem interferindo diretamente com os seres humanos, um exemplo disso é a internet, através dela é possível se relacionar com pessoas em qualquer lugar do mundo, fazer compras, assistir vídeos, acompanhar notícias e muitas outras possibilidades que o mundo digital oferece. Por outro lado, também existem perigos no mundo digital, há sempre pessoas querendo se aproveitar de pessoas descuidadas, leigas ou até inocentes na internet, sempre em busca de acessar dados pessoais para divulgação ou proveito financeiro.

Então é necessário buscar meios de se proteger e a melhor maneira é conhecer quais são os perigos que existem na internet e como fazer para evitá-los, todavia o primeiro passo é detectá-los.

Para Cassanti (2014, p.22), “Não haverá o mínimo de possibilidade em obter êxito na luta contra os crimes virtuais, se quem pretender vencê-los primeiramente não puder entendê-los”.

O estudo desse trabalho se justifica pela necessidade do autor em auxiliar adolescentes que estão usando a internet, na maioria das vezes sem controle dos responsáveis ou até mesmo falta de conhecimento sobre os perigos que existem no uso da internet. Também será possível avaliar o conhecimento de uma parcela de estudantes na maioria entre 13 e 14 anos, para buscar entender como estão usando a internet, verificando quais ações que esses adolescentes estão cometendo que possam gerar algum risco para ele ou até mesmo para sua família.

1.2 OBJETIVOS

Nos dois tópicos a seguir serão explorados os objetivos que devem ser atingidos ao final desse trabalho, separando o objetivo geral e os específicos respectivamente.

1.2.1 **Objetivo geral**

Demonstrar conceitos de boas práticas de utilização da Internet e avaliar o nível de conhecimento dos concluintes do ensino fundamental a respeito dos riscos de

segurança no uso da Internet, assim como divulgar uma cartilha com orientações de boas práticas, tanto para os estudantes, como para a sociedade em geral.

1.2.2 **Objetivos específicos**

Este trabalho tem como objetivos específicos:

a) Descrever os principais ataques virtuais;
b) Demonstrar formas de prevenção para esses ataques;
c) Exemplificar boas práticas para um uso seguro;
d) Desenvolver questionário sobre o uso da internet;
e) Coletar os dados e analisa-los;
f) Criar e divulgar uma cartilha de boas práticas;

1.3 ESTRUTURA DO TRABALHO

No Capítulo 2 é apresentado o embasamento teórico utilizado para formulação do trabalho, o qual está dividido em seções representando cada tópico da pesquisa. As seções são, antecedentes históricos da internet e suas ameaças, que inclui a história da internet no Brasil e no mundo, mostrando dados e estatísticas do uso da internet. Na sequência será visto como ocorre a inclusão digital no Brasil, mostrando as diferentes maneiras de incluir a população no mundo digital. Em seguida é visto como ocorre a gestão da informática na educação, mostrando de que forma a informática é vista nas escolas, mostrando como os gestores trabalham essa ferramenta com os alunos. Na seção sobre a nova realidade da rede mundial de internet, mostra-se as principais ações contra a comunidade infanto-juvenil que acontece na internet. Em seguida, será mostrado as principais ameaças que existem na internet, mostrando como são conhecidas essas ameaças, o que elas fazem e quem as comete. Algumas ferramentas que auxiliam na proteção do usuário, serão expostas, detalhadas e como elas trabalham. Para finalizar, apresenta-se os cuidados necessários que as pessoas devem tomar ao usar a internet, para não caírem nas “armadilhas” da rede mundial de internet.

No capítulo 3 é exposta a pesquisa elaborada para avaliar o conhecimento em segurança digital dos alunos concluintes do ensino fundamental nas escolas de Rio Branco-AC, assim como a análise, os gráficos e os demais resultados obtidos.

No capítulo 4, são demonstradas as conclusões obtidas neste trabalho, a partir dos questionários e a divulgação de ideias para trabalhos futuros.

Por fim o trabalho possui dois apêndices que corresponde ao trabalho realizado nas escolas, no apêndice A é exposto o questionário utilizado para obter as informações

dos alunos, por fim no apêndice B é exposta a cartilha de segurança elaborada com o objetivo de ajudar os alunos e também a comunidade em geral.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo subdivide-se basicamente em 6 partes, onde a primeira parte é dedicada a expor a histórias das ameaças virtuais, conhecendo as primeiras ameaças e seus criadores. Na sequência, o trabalho foca na inclusão digital do Brasil, onde mostra-se que o abismo entre incluídos e excluídos ainda é bastante grande. A terceira parte deste capítulo tem como foco a gestão escolar na rede pública, expondo os desafios e projetos que o governo implementou ao longo dos anos. Na sequência é exposto os riscos que o público infanto-juvenil corre ao usar a internet, onde é exposto que as crianças são as vítimas mais vulneráveis desta teia de comunicação. Na quinta parte deste capítulo é exposto os riscos e crimes que são cometidos na internet, onde é mostrado a causa dessas ameaças, a razão delas acontecerem, especificando as causas. Na última parte é apresentado as ferramentas e práticas usadas para prevenir e tratar essas ameaças citadas na quinta parte deste capítulo.

2.1 ANTECEDENTES HISTÓRICOS DA INTERNET E SUAS AMEAÇAS

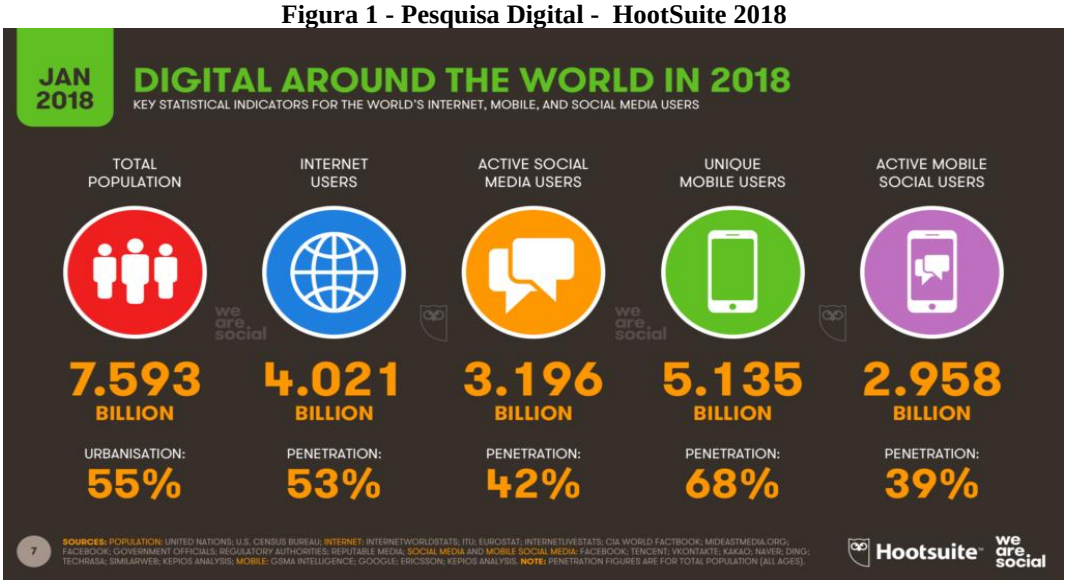
2.1.1 **Internet no Mundo**

Segundo pesquisa divulgada no We Are Social em parceria com o aplicativo HootSuite, em 2017 mais de 4,3 bilhões de pessoas acessaram a internet através de um smartphone através de uma banda larga, ou seja, quase dois terços da população mundial. Nesta mesma pesquisa, mostrou que 71% dos jovens entre 14 e 24 anos, no mundo, usa internet, onde 39% desses jovens são chineses ou indianos.

Já no ano de 2018, na primeira pesquisa da We Are Social, mostrou que a penetração média da internet no mundo é de 53%, os países com maior índice de penetração são Catar e Emirados Árabes Unidos, ambos com 99% da população online.

A seguir, a figura 1 apresenta mais dados da pesquisa realizada em janeiro de 2018 pela We Are Social:

Figura 1 - Pesquisa Digital - HootSuite 2018



Fonte: https://hootsuite.com/pt/pages/digital-in-2018#

Na figura 1 é possível observar que dos mais de 7 bilhões de pessoas no mundo, 53% deles, totalizando mais de 4 bilhões de pessoas conectados na internet, um número que pode ser considerado razoável, onde pode-se observar que ainda existe muita exclusão digital, porém vale destacar que a pesquisa mostra que mais de 5 bilhões de pessoas tem acesso a dispositivos móveis, totalizando 68% da população mundial, o número bastante expressivo.

Mas se tratando apenas do Brasil, a seguir será abordado o histórico da internet em solo brasileiro.

2.1.2 Internet no Brasil

No Brasil, a primeira experiência com a Internet foi realizada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), em 1988, que realizou a primeira conexão à rede através de uma parceria com o *Fermi National Accelerator Laboratory* (FERMILAB), sendo considerado um dos mais importantes centros de pesquisa dos Estados Unidos. Seguindo a mesma rota, a Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC) também se conectaram. Em 1992, foi a vez do governo federal, com a criação da Rede Nacional de Pesquisas (RNP) que criou uma enorme infraestrutura para suportar a rede mundial de computadores que recebia o link internacional e o espalharia pelas principais capitais do país (VIEIRA, 2003).

O uso da Internet fora dos meios acadêmicos somente teve início com a criação do Instituto Brasileiro de Análises Sociais e Econômicas (IBASE), através de um serviço de correio eletrônico chamado Alternex. Nos anos seguintes ocorreu um crescimento gradual no uso da Internet nos meios acadêmicos e, em 1994, o governo

resolve apoiar esse crescimento, associando a experiência e infraestrutura obtida pela RNP com a exploração comercial por parte da Embratel (VIEIRA, 2003).

Ao que tudo indicava, a Embratel teria o monopólio da Internet, porém em 1995 o presidente Fernando Henrique Cardoso ao assumir o cargo de presidente da república declarou que as operadoras estatais não poderiam oferecer o serviço de Internet ao consumidor final, pois isso estaria sob-responsabilidade da iniciativa privada. As operadoras estatais, por sua vez, ficariam limitadas a oferecer a infraestrutura necessária para o mercado corporativo (VIEIRA, 2003).

2.1.3 **Primeiras ameaças**

Existem divergências quanto ao registro do primeiro delito informático. Para alguns autores, foi no âmbito do Massachusetts Institute of Technology (MIT), no ano de 1964, onde um aluno de 18 anos teria sido advertido por ter cometido um ato classificado como cibercrime. Outros autores referenciam um ato realizado na Universidade de Oxford, em 1978, onde um estudante invadiu e copiou uma prova de uma rede de computadores (JESUS, 2016).

Em 1982, Richard Skrenta, com apenas quinze anos, criou o Elk Cloner, que foi considerado por muitos como o primeiro vírus desenvolvido para infectar computador, embora o termo "vírus de computador" tivesse sido criado somente em 1984 por Fred Cohen. Em 1986, surgiu o vírus chamado Brain, criado por dois irmãos paquistaneses, que atingia o setor de inicialização de disco e tinha por finalidade detectar o uso não autorizado de um software médico de monitoramento cardíaco que haviam desenvolvido. O código sofreu alterações maliciosas e passou a espalhar um vírus causando lentidão nas operações de sistemas e ocupando espaço na memória (WENDT; JORGE, 2013).

Nas décadas de 1980 e 1990 houve um grande crescimento de crimes virtuais, outro caso a ser destacado foi o de John Draper, que conseguiu realizar ligações gratuitamente utilizando um apito para produzir o tom de 2.600 Hz, capaz de enganar o sistema telefônico americano. Nessa época, os atos mais comuns eram disseminação de vírus, pornografia infantil, invasão de sistemas e pirataria. Também foi nessa época que se iniciou um movimento para conscientização acerca da segurança de sistemas (JESUS, 2016).

Já com a utilização do celular, em 2004 surgiu o seu primeiro vírus, oriundo das Filipinas. Chamado de *Cabir*, ele foi criado para infectar sistemas operacionais

Symbian, com o objetivo de descarregar toda a bateria de celulares que eram infectados através do *Bluetooth* (WENDT; JORGE, 2013).

2.2 INCLUSAO DIGITAL NO BRASIL

Para que se possa entender o fator inclusão digital, é preciso conhecer também o seu oposto, a exclusão digital. A exclusão digital caracteriza-se por privar o cidadão do acesso a instrumentos básicos como computador, linha telefônica e provedor de acesso (SILVEIRA, 2001 apud LEMOS, 2007, p.17).

A distância entre incluídos e excluídos digitais é enorme no Brasil e, embora haja programas do governo, o principal complicador é o alto índice de pobreza e analfabetismo. Para haver inclusão digital é necessário que além de computadores e internet, haja profissionais no âmbito educacional, garantindo a construção da cidadania (LEMOS, 2007).

Em 20 de setembro de 2005, foi decretado pelo presidente da república Projeto Cidadão Conectado – computador para todos, com o objetivo de:

> [...] promover a inclusão digital mediante a aquisição em condições facilitadas de soluções de informática constituídas de computadores, programas de computador (software) neles instalados e de suporte e assistência técnica necessários ao seu funcionamento, observadas as definições, especificações e características técnicas mínimas estabelecidas em ato do Ministro de Estado a Ciência e Tecnologia.(Planalto.gov.br, 2005, sem paginação).

Neste tempo em questão, existia uma enorme discussão entre as pessoas sobre o que significa incluir? Por quê? E para quem? Visto que existia vários problemas mais graves, como saúde, educação, saneamento e segurança. O desafio era apresentar à comunidade que a inclusão lhes proporcionaria diversos benefícios, abrindo caminhos para a profissionalização e inclusão em um mercado de trabalho cada vez mais necessitado de profissionais capacitados, além de promover a cultura do indivíduo. A inclusão digital sempre esteve diretamente ligada com as políticas de inclusão social, adquirindo grande atenção do governo, que chegou a prever uma meta de ter seis mil telecentros no país até o ano de 2007 (LEMOS, 2007).

Existem duas formas distintas de inclusão digital, que são classificadas como espontânea e induzida, que serão explicadas nas seções 2.2.1 e 2.2.2, respectivamente.

2.2.1 **Inclusão digital espontânea**

É desenvolvida através de processos comuns de evolução da sociedade na era da informação, não havendo necessidade de qualquer formação para seu uso. Atividades do cotidiano são cada vez menos analógicas e mais digitais, como por exemplo, o uso de

caixas eletrônicos, urnas eletrônicas, terminais de autoatendimento, celulares, câmeras digitais, entre outros, são consideradas como formas de evolução natural e populares (BONILLA; PRETTO, 2011).

2.2.2 **Inclusão digital induzida**

A inclusão digital induzida caracteriza-se por serem executadas por universidades, empresas privadas, instituições governamentais e/ou não governamentais, sendo necessários recursos e habilidades para sua execução. São separadas em três categorias: técnica, econômica e cognitiva (BONILLA; PRETTO, 2011).

A categoria técnica trata do incentivo do capital técnico para o uso do computador, seus sistemas e o acesso à Internet. Inclui-se nessa categoria os cursos básicos para atividades diárias como mandar e-mails, editar documentos, acessar a internet e cursos em manutenção para reparo de peças e instalação de redes (BONILLA; PRETTO, 2011).

Já a categoria econômica está relacionada aos custos de comprar e manter equipamentos informáticos e pagamento necessário para acesso à internet e softwares. Também está vinculada a inclusão de micro e pequenas empresas fazendo uso de formas para alavancar os negócios, como comércio eletrônico, integração de transações e facilidade de comunicação com fornecedores e clientes, mudando assim a forma de administrar a economia e proporcionando redução de custos (BONILLA; PRETTO, 2011).

Por fim, a categoria cognitiva é a que se refere ao processo de aquisição de conhecimento, onde é analisado mais do que o ter ou não ter, e sim o que o processo poderá trazer de diferença na vida do indivíduo, analisando as atribuições e necessidades de cada um. O processo cognitivo se torna tão ou mais importante que o técnico, pois é a partir do conhecimento que o uso das novas ferramentas poderá ganhar o status de necessidade básica a todos, mudando assim a sua qualidade de vida (BONILLA; PRETTO, 2011).

2.3 A GESTÃO DA INFORMÁTICA NA EDUCAÇÃO

Gestão da informação pode ser conceituado como um conjunto de estratégias que visa identificar as necessidades informacionais, mapear os fluxos formais de informação nos diversos ambientes da organização, assim como sua coleta, filtragem, análise, organização, armazenagem e disseminação, com o objetivo de apoiar o

desenvolvimento das atividades diárias e a tomada de decisão no ambiente corporativo. (VALENTIM, 2002).

Em um ambiente escolar pode se ter diferentes formas de gestão de informática, nas seções 2.3.1, 2.3.2 e 2.3.3 são destacadas estas formas.

2.3.1 **Gestão educacional**

Segundo Frigeri (2009) gestão educacional pode ser:

> [...] o processo que envolve a coordenação das atividades relacionadas à educação englobando as três instâncias governamentais: federal, estadual e municipal. No cenário da gestão educacional, ocorre o gerenciamento e legitimação das políticas públicas e das leis para a educação, ou seja, é o canal de normatização de leis que gestam a educação brasileira. Desta gestão são elaborados os pareceres, portarias, decretos e leis como, por exemplo, a Lei de Diretrizes e Bases da Educação (LDB), essa legislação deve abranger toda área educacional do país).

Nos últimos anos muitas escolas em todo o país foram inseridas em programas com foco nas TIC's, como ProInfo Rural ou ProInfo Urbano, proporcionando o acesso as tecnologias digitais.

De acordo com o site oficial do MEC, o Programa Nacional de Tecnologia Educacional (ProInfo) é um programa educacional com o objetivo de promover o uso pedagógico da informática na rede pública de educação básica. O programa leva às escolas computadores, recursos digitais e conteúdos educacionais. Em contrapartida, estados, Distrito Federal e municípios devem garantir a estrutura adequada para receber os laboratórios e capacitar os educadores para uso das máquinas e tecnologias.

2.3.2 **Gestão escolar**

A gestão pode ser entendida como a arte de pensar, agir e fazer acontecer. Sendo assim, o gestor precisa articular para que cada indivíduo envolvido se sinta responsável no processo. Pode trabalhar para superar as diferenças, a fragmentação, a descontextualização e construir, através de um olhar abrangente e interativo, a visão e orientação de conjunto, e a partir do qual desenvolver ações articuladas e conscientes (FRIGERI, 2009).

"A gestão da escola passa a ser então o resultado do exercício de todos os componentes da comunidade escolar, sempre na busca do alcance das metas estabelecidas pelo projeto político-pedagógico construído coletivamente" (BARBOSA, 1999, p. 219).

2.3.3 **Gestão democrática**

Segundo Frigeri (2009) gestão da escola é:

> [...]nada mais é que um ato político, pois implica sempre uma tomada de posição dos atores sociais (pais, professores, funcionários, estudantes). Ou seja, a sua construção não pode ser individual, pelo contrário, coletiva, envolvendo os diversos segmentos na discussão e na tomada de decisões. Ela indica para os sistemas de ensino as normas para a gestão democrática, apontando dois instrumentos fundamentais: a elaboração do Projeto Político Pedagógico da escola, contando com a participação dos profissionais da educação; e a participação das comunidades escolar e local em CPM, Conselhos Escolares ou equivalentes.

Segundo Barbosa:

> A gestão democrática, assim entendida, exige uma mudança de mentalidade dos diferentes segmentos da comunidade escolar. A gestão democrática implica que a comunidade e os usuários da escola sejam os seus dirigentes e gestores e não apenas os seus fiscalizadores ou meros receptores de serviços educacionais (BARBOSA, 1999, p.219).

2.4 A REDE: UMA NOVA REALIDADE

Segundo Benevenuto (2008, p. 28):

> Diante da facilidade de acesso ao desenvolvimento de computadores em redes, a sociedade vem mudando seu modo de relacionar-se entre si. A vida compartilhada via sistemas de informações faz parte do cotidiano de um número cada vez maior de pessoas. Atividades relacionadas ao dia-a-dia como: compras, relacionamentos, diversão, trabalho, estudo e outras, tornam- se cada vez mais dependentes do uso das redes de comunicação.

A preocupação voltada as ameaças existentes na internet não é novidade, porém, a população ainda não reflete essa ideia. A inquietação em assegurar informações disponíveis em sistemas surgiu primeiramente relacionada aos governos e grandes empresas. Segundo Ferreira (2003, p. 70):

> No início da Internet, os especialistas em segurança estavam quase que totalmente focados nas ameaças vindas de fora. Eles estavam preocupados com hackers espiões industriais, ou mesmo, ameaças de governos estrangeiros.

Os riscos eminentes pertinentes a redes de comunicação estão presentes diariamente no cotidiano de todos os componentes da mesma, mas indubitavelmente as crianças são as vítimas mais vulneráveis desta teia de comunicação.

2.4.1 **A vulnerabilidade infanto-juvenil**

O mundo disponível na internet se torna muito atrativo ao público infanto-juvenil, uma vez que esse mundo disponibiliza conteúdos para todos os interesses, principalmente em termos de ferramentas que associam: o áudio, o visual e a animação.

Esses recursos são o esteio propulsor de um interesse cada vez maior do público mencionado acima.

O debate a respeito da temática: família, escola, criança e computador, já é tratada há algum tempo. É correto admitir que, o uso da tecnologia na escola e em casa abriu possibilidades e caminhos inimagináveis no mundo da criatividade, da interação, da cognição e do universo lúdico que envolve a imaginação infantil (BENEVENUTO, 2008).

A ausência de orientação diante do acesso extremamente facilitado dificulta a seleção das informações e expõe as crianças à assuntos e imagens inadequadas a faixa etária da mesma, pois a internet não delimita conteúdos de acordo com o usuário que acessa.

Portanto, a criança é mais sujeita aos perigos na internet. Na fase em questão, a criança ainda não desfruta do amadurecimento suficiente para lidar com as muitas possibilidades de riscos que a sociedade em rede oferece, necessitando de um controle especial durante o seu acesso.

Sem dúvida, uma criança sem orientação a respeito da segurança de suas próprias informações poderá refletir em um adulto sem competência para lidar com informações de cunho pessoal e profissional na fase adulta.

Segundo Benevenuto (2008), as ameaças que compreendem a vida infantil exposta na internet podem ser classificadas em diferentes categorias:

- Conteúdos

  - Materiais impróprios, legais ou ilegais, tais como a pornografia, pornografia infantil, violência, ódio, racismo e outros ideais extremistas.

- Contatos

  - Contatos potenciais por parte de pessoas mal-intencionadas, que usam o e-mail, salas de chat, mensageiros instantâneos, fóruns, grupos de discussão, jogos on-line, Orkut, MSN e outros com o intuito de obter informações ou imagens comprometedoras.

- Comércio

  - Práticas comerciais e publicitárias não-éticas.

Benevenuto ainda acrescenta que dentre essas ameaças, podemos destacar:

> [...] os sites de relacionamentos como as ameaças mais atraentes às crianças e aos adolescentes. Apesar de serem disponibilizados para maiores de 18 anos, essas redes de relacionamentos são frequentemente usadas por menores de idade. Isso se deve à falta de restrições quanto ao cadastro das pessoas que se

> registram a essas redes de relacionamentos, já que pedem apenas a data de nascimento do usuário, sendo facilmente alterada de forma leviana.

Dentre os sites de relacionamentos pode-se citar o Facebook, que é uma das redes sociais mais usadas no mundo. As redes sociais serão aprofundadas no item 2.4.2 a seguir.

2.4.2 **Redes Sociais**

As redes sociais abrangem o conceito de mídias sociais, as redes sociais fazem parte do universo das mídias. A definição de mídia seria tudo aquilo que te dá informação como a televisão, jornais e revistas. Porém não te possibilitam uma solução rápida ou uma participação direta na produção, são considerados como uma via de mão única, diferente das redes sociais, já que pode ser considerada uma via de mão dupla, podendo receber e enviar informações e conteúdo de maneira rápida.

O conceito de mídias sociais não envolve somente as redes sociais, mas também blogs, sites de compartilhamento, fóruns e sites como o Wikipédia onde a própria pessoa que está acessando insere informações sobre o que achar interessante e quiser compartir com outros usuários, alterando informações a respeito de um perfil ou assunto específico.

Silveira (2017) afirma que as redes sociais possuem as seguintes vantagens:

- Comunicação instantânea;
- Compartilhar informações, conteúdo e eventos rapidamente;
- Encontrar pessoas e assuntos que interessem o usuário;
- Estabelece ligações profissionais;
- Divulgar seu trabalho e ações;
- Entretenimento através de fotos, vídeos e jogos.

Por outro lado, existem as desvantagens de acessar redes sociais:

- Perda de concentração em outras tarefas;
- Muitas informações falsas, conhecidas como *“Fake News”.*
- Deixar de fazer atividades importantes;
- Possibilidade de esquecer a vida real;
- Vazamento de informações;
- Muitos criminosos buscando dados de usuários.

A seguir vemos que de acordo com a pesquisa da We Are Social com parceria da Hootsuite realizada em janeiro de 2017, um total de 122 milhões de pessoas no Brasil utilizavam redes sociais:

Figura 2 – Pesquisa HootSuite 2017

Fonte: https://wearesocial.com/special-reports/digital-in-2017-global-overview

As redes sociais oferecem facilidade de comunicação e entretenimento, mas é necessário que o usuário esteja atento aos perigos que existem nessa rede, como foi citado acima, além desses problemas citados, é preciso estar de olho nos familiares, principalmente nas crianças, pois um grande perigo que existe nas redes sociais é a pedofilia, que será abordado na seção 2.4.3.

2.4.3 **Pedofilia**

A internet permite às pessoas más intencionadas a facilidade de transmitir, produzir e divulgar materiais impróprios, como o caso dos pedófilos que divulgam conteúdos contendo imagens e vídeos de crianças e adolescentes de forma inapropriada.

Os pedófilos se beneficiam da velocidade e do anonimato disponível na internet para aliciarem crianças e adolescentes sem orientação. Os que utilizam a internet para esse fim são conhecidos como ciberpedófilos. A prática da pedofilia via internet é qualificada como crime de internet a partir da lei 11.829/08 (BENEVENUTO, 2008).

Segundo o portal oficial do Planalto, em 25 de novembro de 2008 o Presidente da República Luiz Inácio Lula da Silva, sancionou a lei 11.829/08 que modifica as considerações anteriormente acordadas pelo Estatuto da Criança e do

Adolescente (ECA) em relação aos crimes realizados com natureza sexual envolvendo crianças ou adolescentes. A lei abrange atos cometidos por pedófilos por meio da internet, já que é qualificado como sendo atos ilícitos as ações referentes à: aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso.

2.5 AMEAÇAS NA REDE MUNDIAL DE COMPUTADORES

2.5.1 **Crimes cibernéticos**

Crime informático, crime eletrônico ou crime digital são alguns termos usados para especificar toda a atividade onde um computador ou uma rede de computadores é usada como uma ferramenta para realizar crime ou atividade ilegal.

Os "crimes cibernéticos" se segmentam em "crimes cibernéticos abertos" e "crimes exclusivamente a prática do crime, que também poderia ser cometido sem o uso dele". Já os crimes "exclusivamente cibernéticos" são diferentes, pois eles somente podem ser realizados com o uso de computadores ou de outros recursos tecnológicos que possibilitam o acesso à internet. Um exemplo é o crime de aliciamento de crianças praticado por intermédio de salas de bate papo na internet, previsto no art. 241-D do Estatuto da Criança e Adolescente (Lei 8.069/90). Também são casos semelhantes os crimes de interceptação telemática ilegal e o recém-aprovado crime de invasão de dispositivos (WENDT; JORGE, 2013).

Antes mesmo do surgimento dos códigos maliciosos, no final da década de 50, foi desenvolvido por um grupo de programadores um jogo chamado Core Wars, que era capaz de se multiplicar a cada vez que era executado, sobrecarregando a memória da máquina do oponente (WENDT; JORGE, 2013).

Em 1982 foi desenvolvido o primeiro vírus com capacidade de infectar um computador, embora o termo "vírus de computador" tivesse sido criado apenas em 1984 por Fred Cohen (WENDT; JORGE, 2013).

Já com a utilização do celular, em 2004 surgiu o seu primeiro vírus, vindo das Filipinas. Denominado de Cabir, ele foi desenvolvido para infectar sistemas operacionais Symbian, com o propósito de descarregar toda a bateria de celulares que eram infectados através do Bluetooth (WENDT; JORGE, 2013).

O Brasil sempre possuiu elevados indicadores de criminalidade digital e, no ano de 2002, chegou a vencer o título de maior "exportador" de criminalidade via internet. Apesar de que houvesse altos índices de crimes, a primeira punição efetiva aconteceu somente em janeiro de 2004, onde um jovem de dezenove anos que aplicava golpes pela

Internet no Brasil e Estados Unidos teve condenação de seis anos e quatro meses (JESUS, 2016).

2.5.2 **Hackers X Crackers**

O termo cracker é usado para definir quem usa seus conhecimentos em informática de forma maléfica, ilegal ou sem ética. Esse nome foi criado em torno de 1985 com o objetivo de se diferenciar do termo já existente hacker. A palavra cracker deriva do verbo em inglês "*to crack*", que significa quebrar (CASSANTI, 2014).

Diferente do cracker, o hacker é um programador com amplo conhecimento sobre sistemas, mas que não tem a intenção de causar transtornos ou danos à população com o intuito de divulgar suas descobertas de forma que mais pessoas sejam beneficiadas e possam consertar seus sistemas antes mesmo que os crackers encontrem maneiras de invadir. Muitas empresas buscam esses programadores para auxiliar no desenvolvimento de softwares de segurança (GUISSO, 2017).

2.5.3 **Engenharia Social**

Em Segurança da informação, denomina-se Engenharia Social as práticas utilizadas para conseguir acesso a informações importantes ou confidenciais em empresas ou sistemas por meio da enganação ou exploração da confiança das pessoas.

A engenharia social mostra que o ser homem é o elemento do sistema mais vulnerável, pois o mesmo possui traços comportamentais e psicológicos que o torna um alvo fácil a ataques de engenharia social.

Para Soares (2001, p.40), o ser humano possui algumas características que o torna suscetível a ataques de engenharia social, pode-se destacar:

- **Vaidade:** O ser humano dispõe ser mais receptivo a comentários positiva e favorável aos seus objetivos.
- **Autoconfiança:** O ser humano busca transmitir em conversas individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando passar segurança.
- **Formação profissional:** O ser humano busca valorizar sua formação e suas habilidades adquiridas.
- **Vontade de ser útil:** O ser humano, geralmente, procura agir com educação, bem como ajudar outros quando preciso.
- **Busca por novas amizades:** O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

- **Propagação de responsabilidade:** Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.
- **Persuasão:** Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas.

2.5.4 **Principais ameaças**

A prática de crimes na internet se dá por meio de vulnerabilidades de segurança nos equipamentos, sistemas ou até mesmo pela ingenuidade humana conforme abordado anteriormente. Antigamente as pessoas tratavam qualquer ameaça como vírus de computador, porém atualmente existe uma grande variedade de tipos de ataques que serão abordados a seguir.

2.5.4.1 Vírus

Vírus são softwares com habilidade de inserir, modificar ou excluir dados, arquivos, informações ou sistemas, ou mesmo executar funções inesperadas em um sistema ou equipamento informatizado (JESUS, 2016).

Existem diversos tipos de vírus, sendo os principais explicados abaixo:

2.5.4.1.1 Vírus de arquivo

São inseridos ao código-fonte de um sistema, geralmente utilizam-se de arquivos executáveis como .EXE, .MSI, e seu efeito começa quando os arquivos são executados (CASSANTI, 2014).

Torres (1997) explica que:

> O arquivo preferido dos vírus é o COMMAND.COM, que é sempre executado. Com o COMMAND.COM infectado, todos os programas que forem executados após o "contágio" serão automaticamente infectados pelo vírus, que tratará de copiar para cada arquivo uma cópia de seu próprio código.

Porém, existem alguns tipos de vírus que substituem trecho do código do arquivo executável, destruindo automaticamente parte do arquivo ao infectá-lo. Com isto, a remoção do vírus torna-se impossível, pois o arquivo original não poderá ser recuperado, já que não é possível recuperar o que o vírus retirou. Contudo, o antivírus é capaz de detectar os arquivos infectados por esse vírus e recomendar que eles sejam apagados (TORRES, 1997).

2.5.4.1.2 Vírus de boot

São considerados os vírus pioneiros, eles se instalam na partição de inicialização de sistemas, impossibilitando de iniciar. Eles se multiplicam através de dispositivos de armazenamento, e sua infecção ocorre quando estão conectados ao computador durante a sua inicialização (WENDT; JORGE, 2013).

Os vírus de boot modificam o setor de boot de todos os discos que encontrarem a partir do momento em que estiverem carregados em memória (RAM). Isto faz com que toda a vez em que for dado um boot com um disco contaminado o vírus seja iniciado de forma automática para a memória antes mesmo do sistema operacional (TORRES, 1997).

A característica desses tipos de vírus é a infecção de códigos executáveis localizados no setor de inicialização das unidades de armazenamento, tanto dispositivos removíveis, quanto discos rígidos.

As unidades de armazenamento possuem um pequeno programa chamado “Bootstrap”, que é responsável por carregar o sistema operacional na memória do computador. Ele é o principal alvo dos vírus de boot, pois modificam o código, que por sua vez modifica a sequência de boot do computador, carregando somente após o BIOS. Exemplos de alguns vírus de boot: Stoned; Ping-Pong; Leandro&Kelly; AntiEXE (SERRANO, 2001).

2.5.4.1.3 Vírus time bomb

Traduzindo para o português, as "bombas-relógio" são vírus programados para executarem em determinados momentos, de acordo com o que foi determinado pelo seu criador. Uma vez infectando um determinado sistema, o vírus somente se tornará ativo e causará algum tipo de dano no dia ou momento previamente definido. Dessa forma, a vítima não percebe nada na hora que o executou, dificultando a descoberta de sua real origem (WENDT; JORGE, 2013).

É frequentemente distribuída como anexo de e-mails e se instalam em computadores pela ação do usuário, ao executar o arquivo. Esses vírus se instalam silenciosamente e agem apenas em datas ou momentos determinados, que são definidos pelo seu criador.

Os mais famosos exemplos de *Time Bombs* foram: Sexta-feira 13, Michelangelo, Eros e 1º de abril (NOVAES,2014).

2.5.4.2 Worm

Segundo Muller (2018) um worm:

> [...] é um programa autorreplicante, ou seja, ele vai se multiplicando dentro da máquina, criando inúmeras cópias dele mesmo, diferente de um vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se alastrar, o worm é um programa completo e não precisa de outro. Um worm pode ser projetado para tomar ações maliciosas após infestar um sistema, sem a necessidade de outro sistema qualquer.

Os Worms consomem muitos recursos do computador, principalmente no armazenamento, devido à quantidade de cópias geradas de si mesmo lotando os discos de armazenamento (WENDT; JORGE, 2013).

2.5.4.3 Cavalo de tróia

O cavalo de troia age silenciosamente, pois é um arquivo aparentemente inocente entregue através de algo conhecido como por exemplo um cartão virtual, um álbum de fotos, protetor de tela ou jogos. O elemento principal do sistema infectado é executado normalmente enquanto o elemento malicioso trabalha de forma oculta ao usuário (CASSANTI, 2014).

Depois de contaminado, o invasor pode se tornar administrador da máquina, ou seja, ele passa a ter permissão de alterar configurações de segurança, deixando o computador ainda mais vulnerável. Também é possível que ele capture informações do usuário e as envie por e-mail para o criminoso (JESUS, 2016).

2.5.4.4 Botnets

Botnets são redes de computadores compostas por diversos bots, que são sistemas instalados por criminosos em estações servidores que respondem a comandos e funções destinados a ele. As máquinas infectadas se tornam “zumbis” e, devido à grande quantidade de computadores infectados, a descoberta da origem se torna quase impossível (JESUS, 2016).

Uma das grandes utilidades das Botnets é para promover ataques conhecidos como Distributed Denial of Service (DDoS), em que vários computadores enviam solicitações para um determinado servidor, sobrecarregando-o e tornando o serviço indisponível.

Para fins de investigação, a polícia primeiro detecta uma máquina utilizada para o ataque e depois aplica a engenharia reversa através da análise dos códigos maliciosos, identificando assim para onde estão sendo enviadas as informações ou de onde elas vêm (WENDT; JORGE, 2013).

2.5.4.5 Deface

A palavra deface, oriunda do inglês defacing, é usada para caracterizar aqueles que desfiguram sites, blogs ou perfis em redes sociais.

Seus ideais podem ser religiosos, filosóficos ou políticos e expressam a sua crítica através de mensagens e imagens. Em alguns casos, informações públicas são roubadas de sites famosos e divulgadas para a população com o objetivo de denegrir a imagem da organização (WENDT; JORGE, 2013).

2.5.4.6 Hijacker

Esse vírus é muito comum atualmente, a palavra inglesa hijack traduzida para o português é sequestrar, e nesse caso os criminosos sequestram os navegadores de internet, ou seja, eles direcionam o navegador para sites que não foram solicitados pelo usuário, alteram sua configuração de página inicial, para assim, quando o usuário abrir o navegador ir direto a página fraudulenta, além disso, abrem pop-ups na tela que são novas janelas com propagandas, conteúdo pornográfico ou de sites fraudulentos. Eles utilizam-se de falhas de segurança em controles ActiveX e modificam registros do Windows para passar a responder da forma como desejam (WENDT; JORGE, 2013).

2.5.4.7 Hoax

Segundo o CERT.BR (2018) hoax é:

> [...] é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Utilizando técnicas de engenharia social e por diferentes meios e discursos, os criminosos buscam enganar e persuadir as vítimas a fornecerem informações pessoais ou a realizarem comandos, como executar códigos maliciosos e acessar páginas fraudulentas. De posse das informações das vítimas, os criminosos costumam efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas (CERT.BR, 2018).

Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato.

Nas próximas seções são apresentados alguns dos principais golpes aplicados na Internet e alguns cuidados que você deve tomar para se proteger deles (CERT.BR, 2018).

2.5.4.8 Spywares

São programas espiões com o objetivo de coletar dados e informações sobre o usuário, seus hábitos de acesso e seus gostos. As informações são enviadas pela Internet para fins de publicidade ou coleta de informações pessoais. São parecidos com os chamados cookies de sites que armazenam preferências dos usuários como idioma utilizado na página, fonte, cor, entre outros, porém os spywares utilizam essas ações de forma maliciosa. Os spywares tem ação de propagação semelhante à dos cavalos de troia, porém se difere por não ter o objetivo de invadir e controlar o sistema (CASSANTI, 2014).

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso: (CERT.BR, 2018).

Legítimo: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

Malicioso: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha) (CERT.BR, 2018).

2.5.4.9 Adwares

Segundo Cassanti (2014), adwares são:

> "[...]programas distribuídos de forma gratuita para download e patrocinados por anúncios de empresas. Quando instalado, além de ter o programa principal, é instalado um componente adicional que é alimentado por propaganda. Esse complemento pode surgir em forma de pop-p, adicionando uma nova barra de ferramentas ao navegador, alterando a página inicial ou redirecionando a vítima para outros sites. Em alguns casos, pode apresentar anomalias no sistema, incompatibilidades ou até mesmo atrapalhar o funcionamento do sistema operacional. "

2.5.4.10 Phishing

A técnica de phishing já é bem famosa e grandes provedores de e-mail como Google e Yahoo buscam obter a conscientização dela. Uma de suas características é que

as mensagens estimulam ser de pessoas ou instituições legítimas como bancos, órgãos governamentais ou empresas. As principais ações envolvendo phishing, são bem comuns de encontrar na internet, são exibidas em inúmeros sites mensagens com links para programas infectados, ofertas fora do padrão, medicamentos inexistentes, fotos e vídeos de celebridades, notícias falsas sobre famosos ou tragédias, reality shows, orçamentos e cotações de preço, informações de cobrança em sites de comércio eletrônico, telefonia e provedores de acesso à internet, informações sobre inclusão do seu nome no SPC e Serasa, avisos de órgãos do governo e instalação de módulos de segurança para a realização de transações bancárias (CASSANTI, 2014).

Um recurso bastante utilizado pelos criminosos para disfarçar suas ações é o uso de encurtadores de URL, onde o link com informações sobre o site é encurtado em poucas letras, dificultando a identificação do site que será redirecionado (WENDT; JORGE, 2013).

2.5.4.11 DoS

O Denial of Service ou traduzindo, “ataque de negação de serviço” se caracteriza por sobrecarregar um serviço informático até que o mesmo fique indisponível. Esses ataques podem ser feitos de diversas formas, como por inundação de pacotes, ou seja, diversos pacotes de rede são enviados causando um congestionamento no site, deixando assim o link inacessível para os usuários. Outra forma que de se praticar o ataque de DDoS muito utilizado atualmente consiste em utilizar diversas máquinas para realização de ataque simultâneo de inundação de pacotes, visto que o tráfego gerado por várias máquinas é muito maior do que se houvesse apenas uma (JESUS, 2016).

2.5.4.12 Quebra de senhas

Existem três tipos conhecidos de ataques pelo método quebra de senhas, um deles é o método de força bruta, ou seja, ela faz um serviço bruto de tentar todas as combinações de dígitos possíveis, porém, sem ser preciso ficar tentando manualmente, os criminosos utilizam ferramentas que fazem isso automaticamente até conseguir êxito no processo. Outro método é o ataque de dicionário, o que faz basicamente é testar palavras de dicionário utilizadas com frequência. O terceiro método mais complexo é chamado rainbow table, destinado à quebra de senhas criptografadas, submetendo os hashs a uma tabela de hashs já calculados para realização de comparações (JESUS, 2016).

2.5.4.13 SQL injection

Essa técnica consiste em modificar parâmetros ou comandos que são executados sobre uma ou mais tabelas de um banco de dados, utilizando da linguagem Structured Query Language (SQL), assim, permitindo o acesso indevido, alteração ou destruição das informações armazenadas no banco de dados (JESUS, 2016).

2.5.4.14 Ransomware

O ransomware é um dos malwares mais temidos pelos usuários, pela forma que atinge suas vítimas. Em suas primeiras ocorrências registradas, esse temido vírus bloqueava a tela do computador deixando exposta uma mensagem exigindo pagamento para que o computador fosse liberado, ou seja, caso não atendesse as exigências, o usuário ficava impossibilitado de realizar qualquer operação na máquina. Com o seu sucesso, surgiram diversas novas variantes e, consequentemente, mais perigosas. As novas versões são capazes de criptografar os arquivos do seu dispositivo exibindo informações de como proceder para receber a chave de desbloqueio. O pagamento geralmente é solicitado através de Bitcoins, uma moeda eletrônica independente de qualquer autoridade central. É bom lembrar que o pagamento não garante que seus arquivos sejam desbloqueados, afinal como é quase impossível identificar o golpista, também não há maneiras de cobrá-lo (TREND MICRO, 2015).

O método mais conhecido de infecção é através de e-mails de phishing, onde o usuário é atraído a clicar em sites que direcionam ao download do ransomware. Atualmente, também é comum o ataque através de sites populares que as pessoas costumam confiar, porém, foram invadidos e tiveram seus códigos fonte e links alterados (GUISSO, 2017).

A seguir será mostrado na figura 3 a forma resumida de como cada vírus é obtido, como ocorre a instalação, como se propaga e suas ações:

Figura 3 – Códigos Maliciosos

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Fonte: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

2.6 CUIDADOS NECESSÁRIOS

Existem diversas ferramentas que auxiliam a prevenção, detecção e tratamento de dados e equipamentos, porém essas ferramentas não garantem uma total segurança. Nesta seção se expõe os tipos de medidas que podem ser adotados para auxiliar na segurança.

2.6.1 **Segurança em geral**

A Internet traz centenas de milhares de equipamentos trocando dados entre si. As próximas seções a demonstra as boas práticas de uso na internet para evitar o acesso dos dados por pessoas não autorizadas.

2.6.1.1 Compartilhamento de informações

É de fundamental importância saber quais dados são rastreados pelas empresas para poder se proteger contra o roubo e uso dos dados e identidade, e assim poder decidir quais desses dados devem ser passados. Por exemplo, quando é solicitado o e-mail para cadastro em sites, nesses casos é possível gerar um e-mail temporário, evitando que seu e-mail real seja entregue a empresas que vendem assinaturas de revistas, produtos ou até mesmo ser inserido em listas de Spam. Em uma busca simples em navegadores, é possível encontrar diversos sites que disponibilizam esse serviço (CHERRY, 2014).

As informações são armazenadas nos chamados cookies que o navegador possui, essas informações coletadas podem ser indevidamente compartilhadas com outros sites e afetar a sua privacidade. Não é incomum, por exemplo, acessar pela primeira vez um site de música e observar que as ofertas de CDs para o seu gênero musical preferido já estão disponíveis, sem que você tenha feito qualquer tipo de escolha (CERT.BR, 2018).

2.6.1.2 Utilização de senhas

Existem quatro grupos de caracteres em um teclado padrão: letras maiúsculas, minúsculas, números e caracteres especiais como: !, @, #, $, %, &, *. Para que uma senha seja considerada segura, é necessário conter ao menos três desses quatro tipos de caracteres. Outro fator importante é a quantidade de caracteres usados na senha, o ideal para uma senha segura é conter no mínimo oito dígitos (CHERRY, 2014).

Atualmente, a maioria dos sites está disponibilizando o recurso de verificação em duas etapas, o método é eficaz, pois somente após uma verificação com algum dispositivo cadastrado o site liberará o acesso a conta (CHERRY, 2014).

A complexidade de uma senha é, normalmente, o que separa uma conta relativamente segura de uma facilmente violável. E segundo a SplashData, empresa que faz programas de gerenciamento de senhas, códigos fáceis foram os mais hackeados do ano.

A SplashData divulgou no final de 2017, via LifeHacker, uma lista com as 25 piores senhas do ano. O levantamento é feito com base em 5 milhões de credenciais vazadas ao longo do ano e mostra quais delas foram as mais utilizadas pelas vítimas, que podemos ver na tabela abaixo:

Tabela 1 – 25 piores senhas de 2017

1	123456
2	password
3	12345678
4	qwerty
5	12345
6	123456789
7	letmein
8	1234567
9	football
10	iloveyou
11	admin
12	welcome
13	monkey
14	login
15	abc123
16	starwars
17	123123
18	dragon
19	passw0rd
20	master
21	hello
22	freedom
23	whatever
24	qazwsx
25	trustno1

Fonte: SPLASHDATA (2017)

Estas senhas reforçam a preocupação citada anteriormente, mostrando que os usuários preferem a criação de senhas fracas, por serem mais fáceis de memorizar, o que os deixam mais vulneráveis a ataques, à criação de senhas mais complexas contendo 3 categorias de caracteres das 4 informadas anteriormente, portanto, se tornam muito mais difíceis de serem decifradas, tornando-se mais seguras. A segurança da informação neste caso esbarra no componente humano.

2.6.1.3 Compras pela internet

Muitos são os atrativos em realizar compras pela Internet. Em apenas alguns minutos é possível buscar produtos, comparar preços facilmente, comprar itens de todas as categorias em um só lugar, tudo isso sete dias por semana, 24 horas por dia e sem enfrentar filas (CASSANTI, 2014).

Este é um mercado que só cresce, tanto para consumidores quanto para golpistas, por isso é necessário ter alguns cuidados ao realizar compras, para então, realizar com segurança. Itens populares ou da moda são um grande atrativo e consequentemente são os mais utilizados pelos golpistas, por isso desconfie sempre de preços muito baixos e procure sempre pesquisar sobre a loja onde está comprando, busque informações com pessoas que já realizaram compras no site em questão (CASSANTI, 2014).

Segundo o site especializado em segurança da informação CERT.BR é necessário seguir algumas orientações ao fazer compras pela internet, como mostrado a seguir:

- Faça uma pesquisa de mercado, comparando o preço do produto exposto no *site* com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;
- Pesquise na Internet sobre o *site*, antes de efetuar a compra, para ver a opinião de outros clientes;
- Acesse sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a esta empresa;
- Fique atento a propagandas recebidas através de spam (mais detalhes no Capítulo Spam);
- Seja cuidadoso ao acessar *links* patrocinados;
- Procure validar os dados de cadastro da empresa no site da Receita Federal;
- Não informe dados de pagamento caso o *site* não ofereça conexão segura ou não apresente um certificado confiável.

Outra dica é sempre verificar todos os detalhes da compra, como os termos de negociação, o prazo de entrega, o endereço físico da loja, as formas de pagamento, garantia e condições de troca. Em caso de devolução ou troca do produto, sempre peça antecipadamente quem deverá arcar com os custos (CASSANTI, 2014).

2.6.1.4 Operações bancárias

Da mesma forma que as compras pela Internet, as operações bancárias também trazem agilidade, praticidade e comodidade, logo os mesmos cuidados devem ser tomados. Além dos cuidados já mencionados, são necessários alguns cuidados extras como, verificar o autor antes de instalar os módulos de proteção das instituições. Nunca pesquise pelo site bancário, procure sempre digitar o endereço do banco de forma

manual na barra de endereços, não aceite sugestões do navegador, há casos de mudar uma letra no endereço, redirecionando para um site fraudulento, evite clicar em links enviados por e-mail, SMS ou redes sociais. Verificar se os links dentro do site do banco não estão direcionando para outros sites, para isso basta posicionar o cursor do mouse sobre o link e ver a informação na parte inferior do navegador antes de clicar. Digite a senha de acesso ao banco errada no primeiro acesso, se o erro for indicado o site está correto, caso contrário então o site é falso, visto que os golpistas não têm como conferir a informação pois querem apenas roubar sua senha. Lembre-se de clicar no botão sair sempre que concluir suas atividades no site, para garantir o encerramento de sua sessão (CASSANTI, 2014).

Segundo o CERT.BR (2018) ao acessar sites bancários ou realizar transações bancárias é preciso tomar alguns cuidados:

- Certifique-se de usar computadores e dispositivos móveis seguros;
- Digite o endereço do site bancário diretamente no navegador Web (Evite seguir o clicar links recebidos por e-mail, SMS ou chats).
- Sempre acesse sua conta usando a página ou o aplicativo fornecido pelo próprio banco;
- Antes de instalar um módulo de proteção, certifique-se de que o autor do módulo é realmente a instituição em questão;
- Evite usar dispositivos móveis e computadores de terceiros (como *Lan Houses* e Internet cafés);
- Evite usar redes Wi-Fi públicas;
- Certifique-se de usar conexões seguras. Alguns indícios desse tipo de conexão são:
  - ✓ O endereço do site começa com “https://”;
  - ✓ O desenho de um “cadeado fechado” é mostrado na barra de endereço;

Quando um site possui uma camada extra de segurança, a barra do navegador fica verde ou com um cadeado, como mostra a figura 4 a seguir:

Figura 4 – Visual de um site protegido

Fonte: https://canaltech.com.br/seguranca/Compras-Online-Evite-golpes-e-dores-de-cabeca/

2.6.1.5 Bloqueadores de anúncios

Essas ferramentas são basicamente complementos instalados nos navegadores que tem a finalidade de bloquear a exibição de anúncios e pop-ups nas páginas da web. Elas evitam que o usuário clique em links indesejado, também evita quando clica em um link e o navegador é redirecionado para várias páginas podendo ser páginas fraudulentas, também tornam a exibição da página mais limpa e fluída. Alguns sites verificam a utilização da ferramenta e o impedem de visualizar o conteúdo da página até que o bloqueador seja desativado, isso ocorre pois eles necessitam que suas propagandas apareçam pois geralmente necessitam do valor para manter o site disponível. Por isso, é possível desativar o bloqueador para páginas específicas, adicionando o site na lista de exceções permitidas do bloqueador. O complemento mais utilizado no mundo é o *AdBlock*, que possui versões disponíveis para Chrome, Firefox, *Android* e Opera (GUISSO, 2017).

2.6.1.6 Links encurtados

Os links ou *Uniform Resource Locator* (URL) encurtados surgiram para solucionar o problema de que redes sociais como o Twitter, por exemplo, limitam o número de caracteres por postagem, e muitas vezes o link para um vídeo ou página desejada pode ultrapassar esse limite. Além disso, URLs longas em e-mails e mensagens SMS podem ficar “quebradas”, caso não sejam corretamente inseridas, inviabilizando o acesso ao link. Para essa finalidade, surgiram os sites que encurtam a URL, basicamente esses sites encurtam o link em pequenos caracteres, que ao clicar no link encurtado o navegador é redirecionado ao site real (CRUZ, 2016).

É importante verificar se a URL encurtada realmente direciona para um site seguro, inclusive quando vierem de fontes seguras como amigos, parentes e colegas.

Uma solução útil é descobrir qual o site real que será redirecionado, através do site https://desencurtadordelinks.com.br/, é possível descobrir a URL escondida, lá você

encontra um campo para colar a URL que está encurtada, em seguida clique em *"desencurtar link"*, como pode ser observado na figura 5 mostrada abaixo.

Figura 5 – Desencurtador de links

Fonte: Elaboração própria

Após clicar em "desencurtar link" a verdadeira URL será revelada em segundos, essa é uma forma de evitar ser redirecionado para páginas não desejadas.

2.6.2 Segurança em computadores pessoais

Muito provavelmente é em seu computador pessoal que a maioria das suas informações estão gravadas e, por meio dele, que você acessa e-mails, sites de notícias, redes sociais, sites de compras onde realiza transações bancárias e comerciais. Por isto, mantê-lo seguro é essencial para se proteger dos riscos envolvidos no uso da internet (CERT.BR, 2018).

O site especializado em segurança CERT.BR mostra os cuidados necessários para manter o computador pessoal seguro:

- Mantenha os programas atualizados (Fabricantes costumam lançar novas versões quando há recursos a serem adicionados ou vulnerabilidades a serem corrigidas);
- Use apenas programas originais (Sistemas "piratas" costumam conter vírus);
- Utilize sempre antivírus (Procure manter uma rotina de escaneamento, sempre é bom o antivírus buscar arquivos infectados na máquina).

A seguir, será demonstrado mais alguns cuidados no uso de computadores.

2.6.2.1 Administração de contas de usuário

Uma conta de usuário, também chamada de "nome de usuário", "nome de login" e username, corresponde à identificação única de um usuário em um computador ou serviço. Por meio das contas de usuário é possível que um mesmo computador ou serviço seja, compartilhado por diversas pessoas, pois permite, por exemplo, identificar unicamente cada usuário, separar arquivos, configurações específicas de cada um e controlar as permissões de acesso que o administrador da máquina conceda para cada perfil (CERT.BR, 2018).

A sua conta de usuário é de conhecimento geral e é o que permite a sua identificação. Ela é, muitas vezes, derivada do seu próprio nome, mas pode ser qualquer sequência de caracteres que permita que você seja identificado unicamente, como o seu endereço de e-mail ou CPF. Para garantir que ela seja usada apenas por você, e por mais ninguém, é que existem os mecanismos de autenticação como o caso das senhas que já foi abordado anteriormente neste trabalho (CERT.BR, 2018).

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha ela poderá usá-las para se passar por você na Internet e realizar ações em seu nome, como mostra o (CERT.BR, 2018):

- Acessar a sua conta de correio eletrônico e ler seus e-mails, enviar mensagens, furtar sua lista de contatos e pedir o reenvio de senhas de outras contas;
- Acessar o seu computador e obter informações sensíveis nele armazenadas;
- Desferir ataques contra computadores de terceiros;
- Acessar sites e alterar as configurações feitas por você;
- Acessar a sua rede social e usar a confiança que as pessoas da sua rede de relacionamento depositam em você.

2.6.2.2 O que fazer se o computador for comprometido

Segundo o CERT.BR (2018) existem alguns indícios que, sozinhos ou em conjuntos podem demonstrar que o computador está comprometido. Alguns deles são:

- Computador desligando sozinho;
- Computador lento;
- Acesso à internet demorado;
- Janelas de pop-up aparecendo;

Caso apareça algum desses indícios, o CERT.BR (2018) aconselha tomar algumas medidas para reverter esses problemas. Para isto devem ser executados os seguintes passos:

- Verifique se o computador está atualizado;
- Verifique se o antivírus está ativado e atualizado;
- Limpe todos os arquivos que o antivírus afirme estar infectados;
- Caso não confie, instale outro antivírus.

2.6.2.3 Uso de computadores de terceiros

Ao usar computadores ou outro dispositivo com acesso a informática de terceiros, principalmente cyber cafés, é necessário ter cuidados com segurança redobrados. A seguir o CERT.BR (2018) demonstra alguns cuidados necessários:

- Utilize a opção “Navegar anonimamente” do navegador de internet;
- Utilize um antivírus;;
- Não efetue transações bancárias ou comerciais;
- Não armazene senhas pessoais;
- Limpe todos os dados armazenados durante o seu acesso;
- Assegura de fazer o “Logout” de todas as contas conectadas;
- Ao retornar para seu computador pessoal, altere as senhas utilizadas nos outros computadores.

2.6.3 **Segurança em dispositivos móveis**

Dispositivos móveis, como tablets, smartphones, celulares e etc’s, têm se tornado cada vez mais populares e capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação Web, Internet Banking, acesso a e-mails, redes sociais e jogos. Infelizmente, as semelhanças não se restringem apenas às funcionalidades apresentadas, elas também incluem os riscos de uso que podem representar (CERT.BR, 2018).

Existem riscos como qualquer dispositivo informático, porém há características próprias que os dispositivos móveis possuem que, quando abusadas, os tornam ainda mais atraentes para atacantes e pessoas mal-intencionadas, como o CERT.BR (2018) cita:

- **Grande quantidade de informações pessoais armazenadas:** fotos, vídeos, números de cartão de crédito e senhas;

- **Maior possibilidade de perda e furto:** em virtude do tamanho reduzido, podem ser facilmente esquecidos, perdidos ou roubados.
- **Grande quantidade de aplicações desenvolvidas por terceiros:** há uma infinidade de aplicações sendo desenvolvidas, entre elas podem existir aplicações desenvolvidas para execução de atividades maliciosas.
- Rapidez de substituição dos modelos: em virtude da grande quantidade de novos lançamentos, os dispositivos móveis costumam ser rapidamente substituídos e descartados, sem que nenhum tipo de cuidado seja tomado com os dados nele gravados (CERT.BR, 2018).

Este capítulo teve como propósito fundamentar o tema sobre segurança digital, estabelecendo o panorama no Brasil e no mundo. No próximo capítulo será abordado a pesquisa feita em algumas escolas de ensino fundamental em Rio Branco sobre comportamento em segurança digital.

3 PESQUISA DE ANÁLISE SOBRE COMPORTAMENTOS EM SEGURANÇA DIGITAL

Neste capítulo está descrita a pesquisa elaborada sobre comportamento em segurança digital, na seção 3.1 é apresentada a metodologia utilizada para a elaboração da pesquisa, na seção 3.2 apresenta-se a amostragem da pesquisa, na seção 3.3 apresenta-se o resultado da pesquisa.

3.1 METODOLOGIA

Depois de finalizada as pesquisas para elaboração do referencial teórico, foi desenvolvido um questionário com o uso da ferramenta Google Forms, e impresso fisicamente para distribuição nas escolas de ensino fundamental, especificamente aos alunos do 9º ano, disponível no apêndice A deste trabalho. Este questionário tem por objetivo coletar informações necessárias para responder a questão principal do trabalho, que é indicar qual o nível de conhecimento em segurança digital dos alunos concluintes do ensino fundamental.

O tipo de pesquisa utilizada será a descritiva quantitativa, também conhecida como pesquisa de levantamento ou *survey*. Para Baptista e Campos (2016), as pesquisas de levantamento são feitas principalmente para identificar comportamentos e atitudes e caracteriza-se pela coleta de dados fornecidos pelas próprias pessoas, geralmente através de questionários.

As questões aplicadas são do tipo objetivas fechadas, onde o pesquisador define as alternativas e o respondente, por sua vez, assinala aquela que mais se ajusta às suas características, ideias ou sentimentos. Foram inseridas questões de múltipla escolha, algumas aceitando somente resposta simples e outras com múltipla escolha, além de perguntas em escala.

O método de amostragem será o não probabilístico por conveniência, que segundo Baptista e Campos (2016) caracteriza-se por não ser realizada de forma

aleatória, pois nem toda a população terá a probabilidade de respondê-la, já que apenas alunos do 9º ano estavam aptos a responder o questionário.

Ao término da aplicação do questionário, foi iniciado o processo de análise dos resultados, onde foi utilizado como ferramenta de auxílio para geração de gráficos e estatísticas o próprio Google Forms, onde foi necessário passar todas as respostas obtidas no questionário impresso para a base de dados da ferramenta. A partir dos resultados obtidos, foi desenvolvida uma pequena cartilha, disponível no Apêndice B, com boas práticas de uso da Internet, com destaque para os pontos mais críticos que foram verificados. Essa cartilha foi entregue as turmas que responderam o questionário anteriormente.

3.2 A PESQUISA

A pesquisa teve início na data de 5 de novembro de dois mil e dezoito e foi concluída em 9 de novembro de dois mil e dezoito, totalizando 5 dias de duração. A aplicação do questionário foi agendada anteriormente em duas escolas da rede pública do Estado do Acre, uma central onde estudam alunos de várias localidades da cidade de Rio Branco, desde o centro da cidade até os bairros mais afastados, já a outra escola é localizada em uma área periférica de Rio Branco, onde estudam alunos do próprio bairro onde ela está localizada, com o intuito de buscar uma variedade abrangente de alunos. A pesquisa foi realizada com 120 alunos do 9º ano do ensino fundamental, onde os alunos têm em média 14 anos de idade, com o objetivo de mostrar como os adolescentes estão usando a internet.

As questões foram elaboradas com base na primeira parte do trabalho, buscando identificar o nível de conhecimento dos alunos do 9º ano em relação principalmente relacionada a segurança da informação.

3.3 RESULTADOS DA PESQUISA

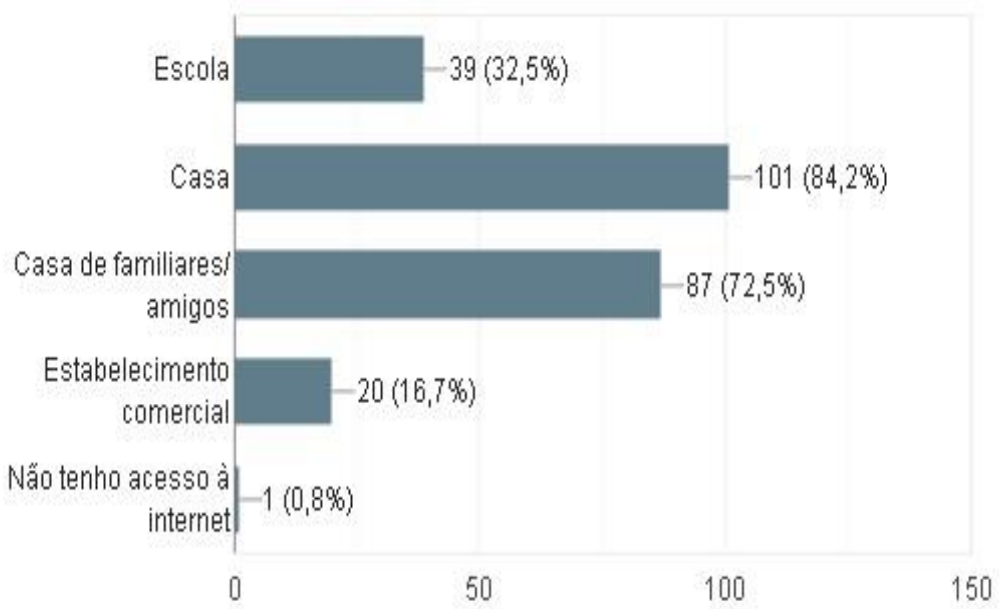
O questionário foi desenvolvido com alguns objetivos: traçar o perfil do respondente; verificar a disponibilidade que ele possui para acessar a internet; o que e como ele acessa; testar o conhecimento do respondente afirmando algumas situações; descobrir o que ele compartilha na internet; como ele utiliza as redes sociais e; quais as medidas de segurança que ele utiliza para se proteger ao acessar.

3.3.1 **Informações do entrevistado**

O primeiro bloco de perguntas tem o objetivo de verificar como o entrevistado tem acesso à internet e qual a frequência do uso. A primeira questão tem o propósito de

verificar aonde o entrevistado se liga à internet, possibilitando a marcação de mais de uma resposta, cujo resultado é apresentado na figura 6.

Figura 6 - Locais utilizados para se ligar a internet

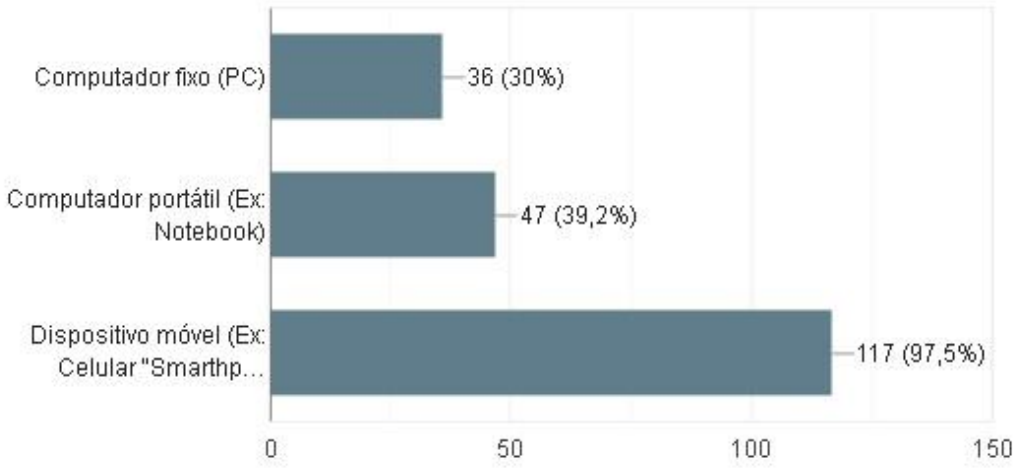


Fonte: Elaboração própria.

A figura 6 chama atenção ao mostrar que apenas 0,8% dos entrevistados não possuem acesso à internet, o que mostra que a quantidade de pessoas conectadas a internet vem crescendo de forma considerável. Outro dado que chama atenção é a quantidade de 84,2% dos respondentes possuírem acesso à internet em sua casa, tendo em vista que a pesquisa foi realizada com um público de escola pública, sendo que boa parte desse grupo resida em área periférica, isso mostra como os adolescentes estão conectados. Os que não possuem acesso disponível em sua residência tem a possibilidade de acessar na casa de familiares ou amigos que é o caso de 72,5% dos entrevistados ou recorrer a escola ou algum estabelecimento comercial, que é o caso de 32,5% e 16,7% respectivamente.

A segunda questão tem o objetivo de revelar com quais tipos de equipamentos os entrevistados utilizam para acessar a internet, a pergunta é de múltipla escolha, cuja resposta é apresentada na figura 7.

Figura 7 - Dispositivos utilizados para se ligar à internet

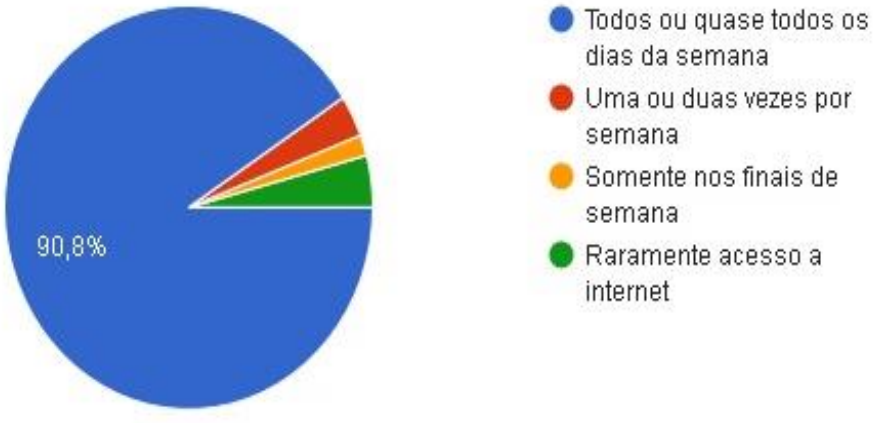


Fonte: Elaboração própria.

Na figura 7 é possível notar o quanto os dispositivos móveis estão em alta no mercado, a questão resultou que 97,5% dos entrevistados utilizam o dispositivo móvel para acessar a internet, confirmando o avanço dos *smartphones* que de acordo com a pesquisa do IBGE realizada em 2014 já possuía mais celulares do que microcomputadores, que é utilizado por apenas 30% dos entrevistados, mostrando uma diferença altamente considerável.

A terceira pergunta tem o objetivo de verificar a frequência que os adolescentes entrevistados destinam a usar a internet. A resposta será mostrada na figura 8.

Figura 8 - Frequência de uso da internet



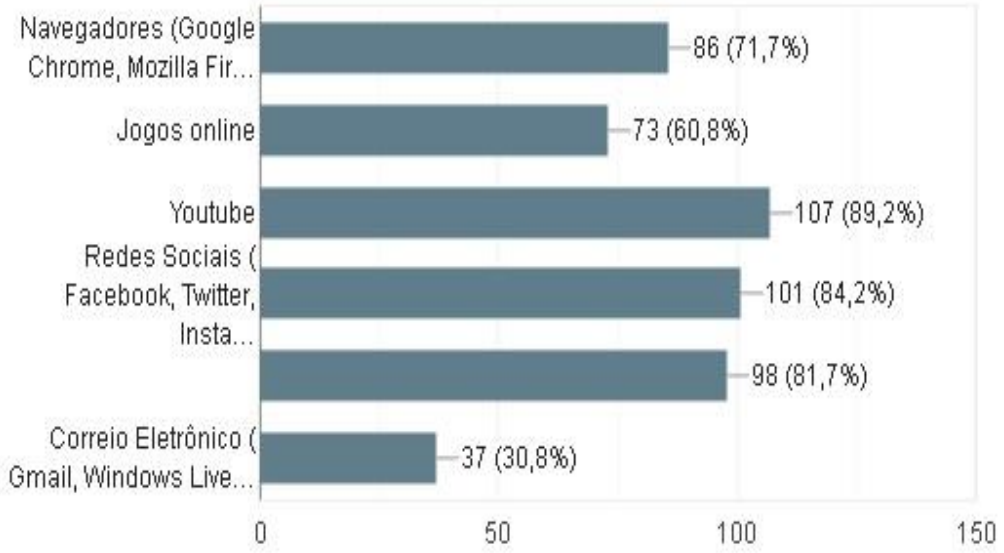
Fonte: Elaboração própria.

A figura 8 mostra o quanto os adolescentes estão utilizando a internet, 90,8% dos entrevistados utilizam a internet todos os dias, mostrando quase uma dependência pelo uso da internet, onde apenas 4,2% raramente acessa a internet. Mas o que os

adolescentes estão fazendo na internet? Será que estão apenas para entretenimento ou estão utilizando-a para adquirir fins didáticos e na busca de novos conhecimentos?

A pergunta seguinte tem o objetivo de verificar quais programas/aplicativos que os entrevistados utilizam de acordo com o que cada um faz na internet, possibilitando a marcação de várias opções, cuja resposta está na figura 9.

Figura 9 – Programas utilizados



Fonte: Elaboração própria.

A figura 9 apresenta informações que chamam a atenção, como 89,2% acessam o site Youtube, seja para ouvir música, assistir vídeos divertidos ou vídeos de estudos, isso mostra que boa parte dos alunos entrevistados estão com acesso esse site podendo ser utilizado como um meio de estudo. Outro dado interessante é que 84,2% dos entrevistados acessam as redes sociais, tendo em vista que boa parte dessas redes tem a restrição de uso para menores de 18 anos, porém facilmente burladas. Outra informação relevante é o uso de chats como por exemplo o WhatsApp, onde 81,7% dos respondentes utilizam esse tipo de ferramenta para se comunicar com outras pessoas, possibilitando conciliar com as redes sociais para conhecer novas pessoas que mais a frente será apresentada no trabalho como os respondentes estão utilizando essas ferramentas. Outros dados apresentados na figura é que 71,7% utilizam navegadores para visitar sites, 60,8% acessam jogos online e apenas 30,8% utilizam correio eletrônico, tendo em vista a pouca necessidade do uso de e-mail para a idade média dos entrevistados.

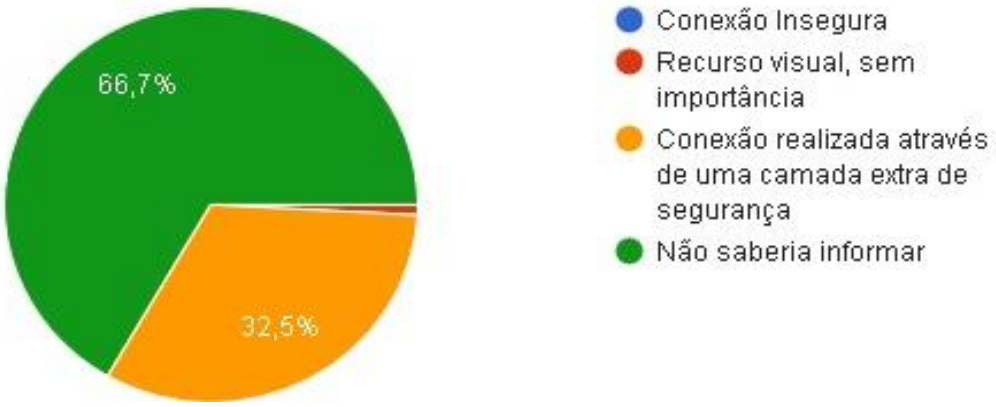
Nesta primeira parte da pesquisa foi possível observar que apenas 1 entrevistado afirma não ter acesso a internet, caracterizando 0,8% dos entrevistados, ou seja, os

outros 99,2% possuem algum meio de acesso à internet, de forma que é possível afirmar que os alunos estão incluídos digitalmente. Também é possível destacar que 97,5% utilizam o dispositivo móvel para acessar a internet, onde mais de 90% afirmar utilizar a internet todos os dias, principalmente para usar redes sociais e assistir vídeos em sites especializados como o Youtube.

3.3.2 **Conhecimento do usuário**

A questão a seguir foi elaborada com o objetivo de avaliar o conhecimento do entrevistado em relação a nomenclatura HTTPS, tendo em vista que 71,7% dos entrevistados afirmaram utilizar navegadores de internet, o resultado da questão está na figura 10.

Figura 10 - Significado da nomenclatura HTTPS

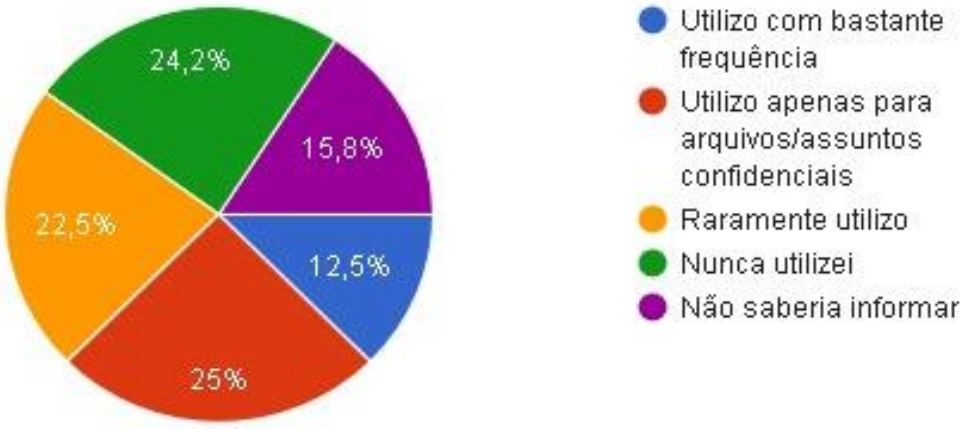


Fonte: Elaboração própria.

A figura 10 revela que 66,7% dos respondentes não sabem o que é a nomenclatura HTTPS, por outro lado apenas 32,5% responderam à pergunta corretamente, o que é bastante preocupante, pois o ideal é sempre buscar acessar a internet em sites que oferecem uma camada extra de segurança, principalmente nos casos que realizam algum tipo de operação, aconselha-se a não realizar operações bancárias ou confidenciais em redes que não possuem essa camada extra na conexão.

Em seguida, foi apresentado o conceito de criptografia de dados, então foi perguntado com que frequência o entrevistado à utiliza, cujo resultado está na figura 11.

Figura 11 - Utilização da criptografia de dados



Fonte: Elaboração própria.

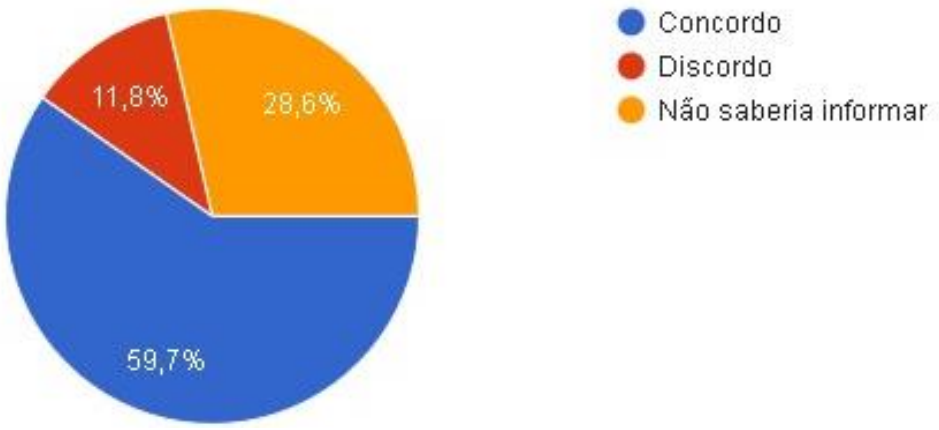
A questão referida na figura 11 causou bastante divergência entre os entrevistados, onde 12,5% afirmaram utilizá-la com bastante frequência, enquanto a maior "fatia" afirmou utilizar apenas para arquivos confidenciais. Por outro lado, a maior parte dos entrevistados relatou utilizar raramente, nunca ter utilizado ou não saber informar, com os dados 22,5%, 24,2% e 15,8% respectivamente, somando um total de 62,5% dos respondentes, o que causa preocupação, pois é bastante significante a quantidade de entrevistados ignorando a criptografia de dados, pois o ideal é criptografar os assuntos ou arquivos confidenciais, pois há muitas pessoas em busca dessas informações.

Nesta segunda parte da pesquisa é possível observar que quando se trata de informações mais aprofundadas como os casos de HTTPS e criptografia de dados, os entrevistados mostraram não entender dos assuntos abordados, onde 66,7% não souberam informar o que seria a representação do site possuir uma camada extra de segurança, já no caso de criptografia de dados, 62,5% afirmam não utilizar ou simplesmente não conhecer sobre o assunto.

3.3.3 **Afirmações de cotidiano**

Seguindo o questionário aplicado aos alunos, foram feitas 5 afirmações, onde o respondente tinha que concordar, discordar ou não saber informar. A primeira afirmação foi "**Durante operações bancárias realizadas na internet, uma prática de segurança comum é digitar a senha incorreta no primeiro acesso, para validar se o site é legítimo**". A resposta é apresentada na figura 12.

Figura 12 - Afirmação: Operações bancárias

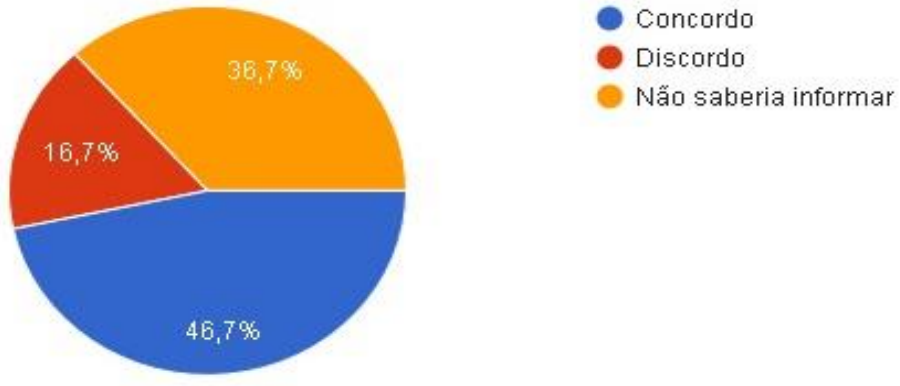


Fonte: Elaboração própria.

O resultado da questão apresentada na figura 12 é bastante satisfatório, pois 59,7% dos entrevistados informariam a senha incorreta no primeiro acesso e realmente é uma ótima prática para verificar se o site é legítimo, pois há muitos sites que copiam todo o *layout* do banco com o objetivo de coletar dados de contas e cartões de crédito de pessoas inocentes. Então o ideal é informar a senha incorreta no primeiro acesso, pois o site falso não verifica se os dados estão corretos, eles irão apenas coletar essas informações e tentaram utilizar para proveito próprio posteriormente.

A segunda afirmação foi "Links de sites encurtados, exemplo: 'goo.gl/Rio8ft', são utilizados para fraudes pois dificultam a identificação do site que estamos sendo direcionados". A resposta segue na figura 13.

Figura 13 – Afirmação: Links encurtados



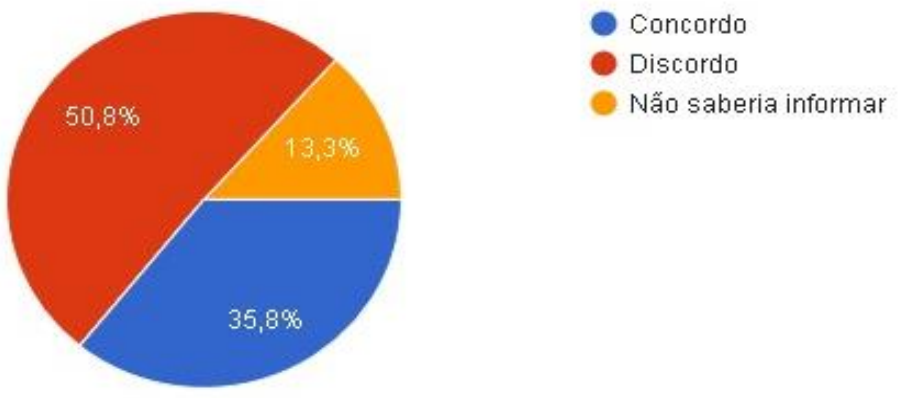
Fonte: Elaboração própria.

O resultado da questão apresentado na figura 13 mostra bastante dúvida dos entrevistados em relação aos links encurtados, 46,7% dos respondentes concordam que esses links podem ser perigosos, eles estão corretos, os links encurtados dificultam a identificação do site, fazendo com que o usuário acesse o determinado link para enfim descobrir de que site realmente se trata, então o ideal é usar ferramentas que exibem o

site real dentro deste link encurtado, como já foi mostrado na seção 2.6.1.6 deste trabalho.

A terceira afirmação foi “Criminosos da internet possuem maior interesse em atacar computadores de grandes empresas, por isso os usuários domésticos estão protegidos”. A resposta segue na figura 14.

Figura 14 – Afirmação: Usuários domésticos

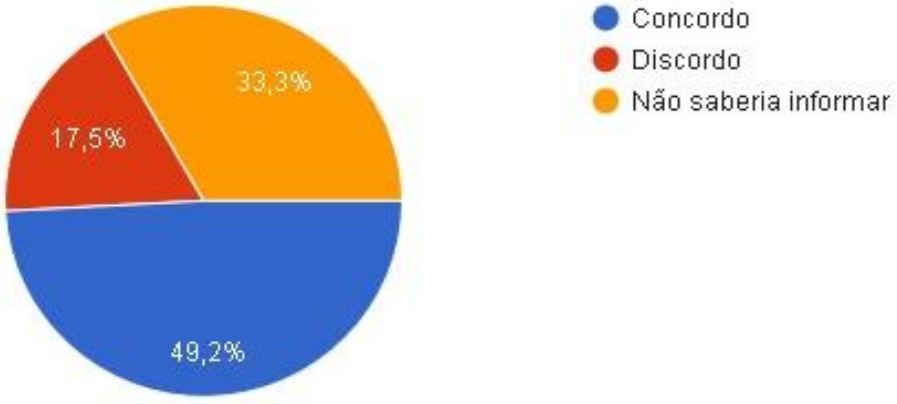


Fonte: Elaboração própria.

A figura 14 traz um dado até certo ponto preocupante, pois 35,8% dos entrevistados acham que por serem usuários domésticos estão protegidos, porém sabe-se que atualmente os criminosos da Internet não escolhem a quem irão atacar, portanto usuários domésticos estão tão expostos às vulnerabilidades quanto os usuários corporativos. Por outro lado, mais da metade dos entrevistados discordam dessa afirmação, 50,8% responderam corretamente a afirmação.

A quarta afirmação foi “Uma empresa legítima não solicitará informações pessoais em uma mensagem de e-mail. Apesar de parecem convincentes, mensagens que solicitam informações pessoais com urgência provavelmente são falsas”. As respostas estão na figura 15.

Figura 15 - Afirmação: Solicitação de informações pessoais

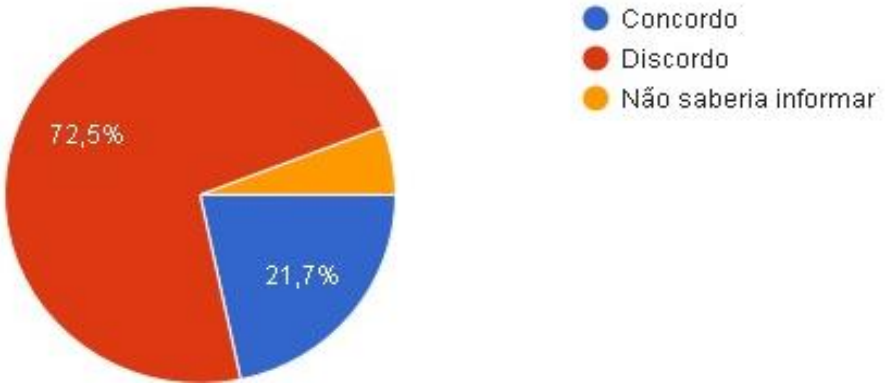


Fonte: Elaboração própria.

A figura 15 apresenta que 49,2% dos entrevistados concordam com a afirmação, enquanto 17,5% discordam, ou seja, muitas pessoas ainda caem em uma das táticas mais comuns da internet. Essa tática é realizada através de e-mail, onde o atacante se passa por uma empresa legítima e lhe solicita dados para confirmar alguma operação ou corrigir um suposto problema. Por mais que estes e-mails despertem curiosidade e pareçam verdadeiros, uma empresa legítima jamais solicitará esse tipo de informação via e-mail, SMS, redes sociais ou por telefone, o comum e correto é elas terem todos esses dados e caso precise de algum outro dado solicitar que o cliente compareça a empresa para informar o que for preciso.

A quinta afirmação foi “Redes Wi-Fi domésticas possuem sinal de curto alcance, logo não é necessário à utilização de senhas difíceis”. As respostas estão na figura.

Figura 16 - Afirmação: Redes Wi-Fi



Fonte: Elaboração própria.

A figura 16 mostra que essa afirmação foi a que obteve mais consenso entre os entrevistados, a grande maioria correspondendo a 72,5% dos respondentes discordam dessa afirmação. Ainda é comum encontrar redes Wi-Fi configuradas sem nenhum tipo de segurança. Isso além de comprometer a qualidade do seu sinal, já que pessoas não autorizadas podem a estar utilizando, possibilita que pessoas mal-intencionadas capturem informações dos demais dispositivos conectados e também distribua conteúdo impróprio na Internet sem poderem ser identificados.

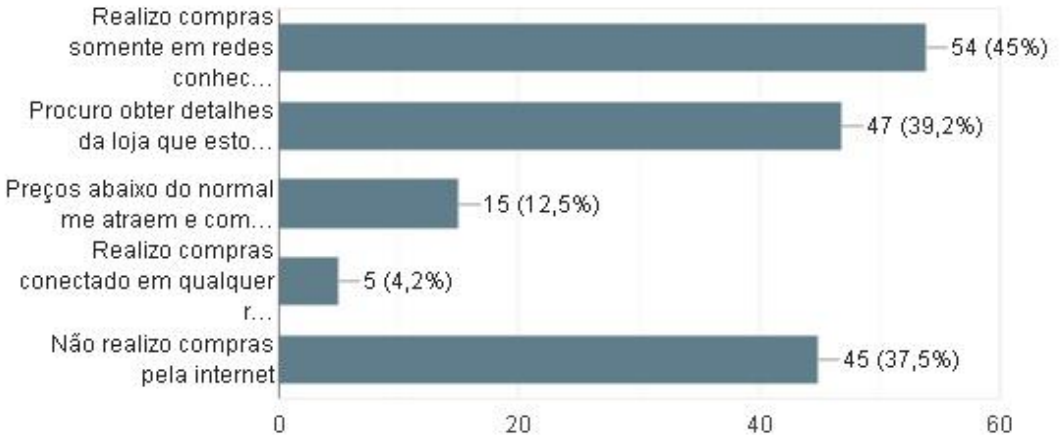
Na parte de afirmações do cotidiano dos entrevistados, pode-se destacar as boas práticas que os mesmos praticam na internet, como os 59,7% que afirmam informar a senha incorreta na primeira vez que acessar um site bancário, com o objetivo de verificar se o site é legítimo. Outro dado importante é que 46,7% acreditam que não é seguro clicar em links encurtados, já que podem direcionar para sites fraudulentos. Outro dado obtido é que mais de 50% acreditam que os usuários domésticos correm o mesmo risco que as empresas. Na quarta afirmação, 49,2% acreditam que sites

legítimos não solicitam dados pessoais via e-mail. Por último 72,5% afirmar que o wi-fi mesmo possuindo um curto alcance, é necessário ter uma senha difícil.

3.3.4 **Comportamento em situações específicas**

O próximo bloco é composto por quatro questões com o objetivo de analisar o comportamento do usuário em algumas situações específicas, podendo marcar mais de uma opção em cada pergunta. A primeira pergunta se refere ao comportamento do usuário ao realizar compras na internet, como os entrevistados são menores de idade, a pergunta foi direcionada a compras na internet com um responsável maior de idade, cujo resultado está na figura 17.

Figura 17 – Compras na internet



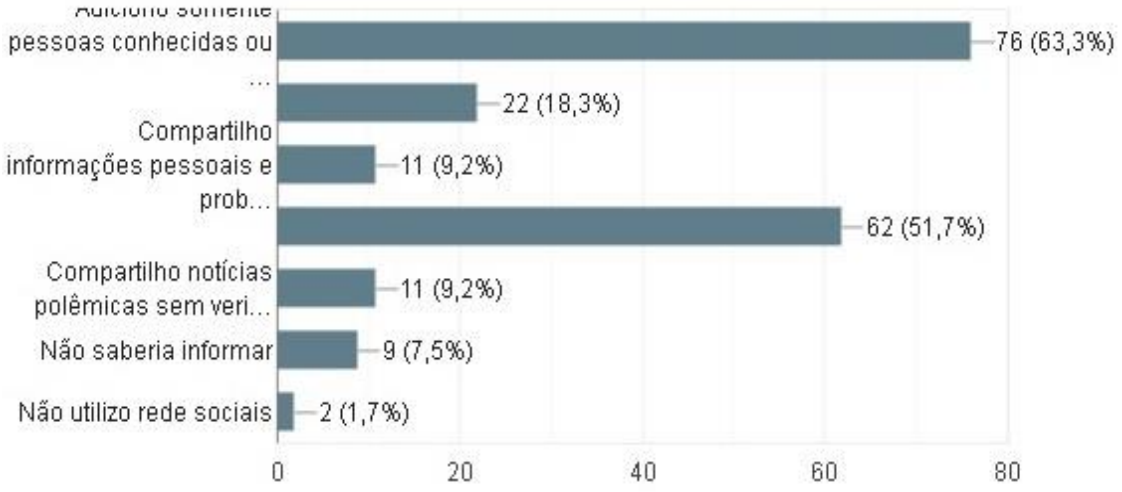
Fonte: Elaboração própria.

A figura 17 mostra que os respondentes se preocupam bastante no momento de realizar compras na internet, pois 45% dos entrevistados afirmam realizar compras somente em redes conhecidas ou privadas, ou seja, não realizam compras usando redes abertas ou que não sabem a procedência, enquanto apenas 4,2% afirmam não ter preocupação com qual rede de conexão estão usando para realizar operações bancárias. Outro dado que chama atenção é que 39,2% dos respondentes procuram buscar a procedência da loja que está fazendo a compra, buscando dados de CNPJ e buscando informações no site reclameaqui, bastante usado para esses fins. Apenas 12,5% se atraem com preços muito abaixo do normal, então é importante alertar, caso o preço esteja muito abaixo, é necessário sempre desconfiar, há muitos sites que copiam o layout das lojas famosas com o intuito de fazer vendas se passando por elas, então todo cuidado é pouco ao realizar compras pela internet.

Grande parte do tempo gasto na internet é destinada na utilização de redes sociais, onde há um grande fluxo de informações dos tipos mais variados, onde muitas

dessas informações são falsas ou adulteradas como o objetivo de causar polêmica ou apenas enganar os usuários. Então, na segunda questão do bloco tem como objetivo extrair informações de uso do usuário nas redes sociais e avaliar o percentual de correspondentes que praticam ações corretas, além de identificar práticas indevidas que necessitam um auxílio na aprendizagem, cujo resultado está na figura 18.

Figura 18 – Uso das redes sociais

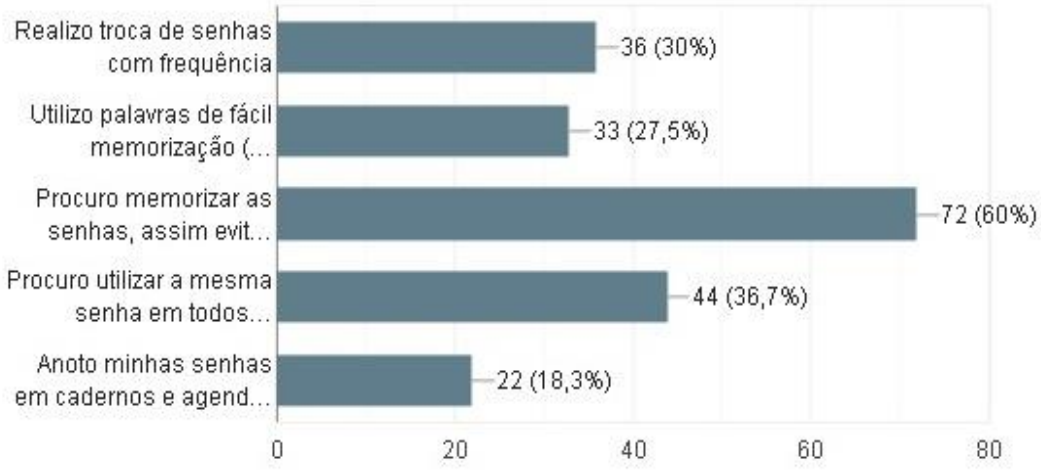


Fonte: Elaboração própria.

No quesito “Adiciono somente pessoas conhecidas ou que mantenho algum contato”, 63,3% dos respondentes afirmam não adicionar pessoas desconhecidas, que se trata de um ótimo percentual, se tratando de pessoas desconhecidas, é necessário ter um cuidado maior, pois não é possível saber as reais intenções dessas pessoas, podendo querer obter informações pessoais ou até estudar a rotina do usuário. Outro dado que chama atenção é que 51,7% dos respondentes utilizam configurações de privacidade, ou seja, somente as pessoas que o usuário deseja, pode visualizar as suas publicações. Agora, por outro lado, tem as práticas que devem ser evitadas, como os 18,3% que afirmaram clicar em todos os links que despertam curiosidade, o que deve ser evitado, pois muitos links podem estar contaminados de vírus. Outra prática que deve ser evitada é de compartilhar notícias polêmicas sem verificar a veracidade da informação, é importante pesquisar em sites que possuem boas referências antes de qualquer ação.

A terceira questão do bloco tem o objetivo de estudar o comportamento do usuário se tratando do uso de senhas, cujo resultado está na figura 19.

Figura 19 – Utilização de senhas

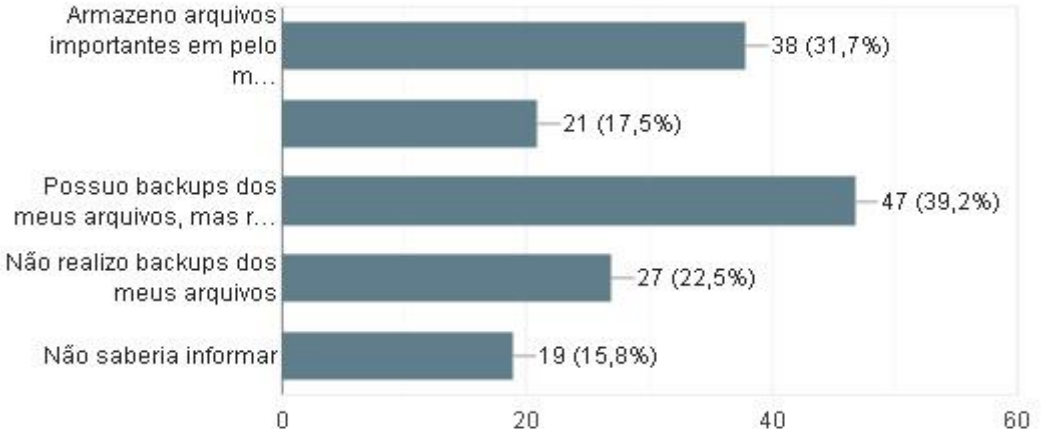


Fonte: Elaboração própria.

Sobre o item “realizo troca de senhas com frequência”, apenas 30% dos usuários praticam essa ação. Enquanto que 36,7% dos respondentes afirmam utilizar a mesma senha para todos os acessos, o que deve ser evitado, pois se alguém por acaso descobrir uma senha de acesso, todos os acessos desse usuário estarão comprometidos. No quesito “utilizo palavras de fácil memorização (como data de nascimento)”, 27,5% dos usuários afirmam adotar essa prática, o que não deve ser adotado, pois são as primeiras tentativas de quebra de senha que terceiros irão utilizar.

Para encerrar esse bloco de perguntas, comenta-se sobre o assunto *backup*, demonstrado na figura. Essa questão auxilia a identificar se o usuário realiza essa prática, caso utilize, identificar se está sendo feito da maneira correta.

Figura 20 - Backup



Fonte: Elaboração própria.

Nota-se, na figura 20, que 39,2% possuem backups dos arquivos, porém raramente atualiza essas informações, ou seja, caso haja algum problema ou perca dos

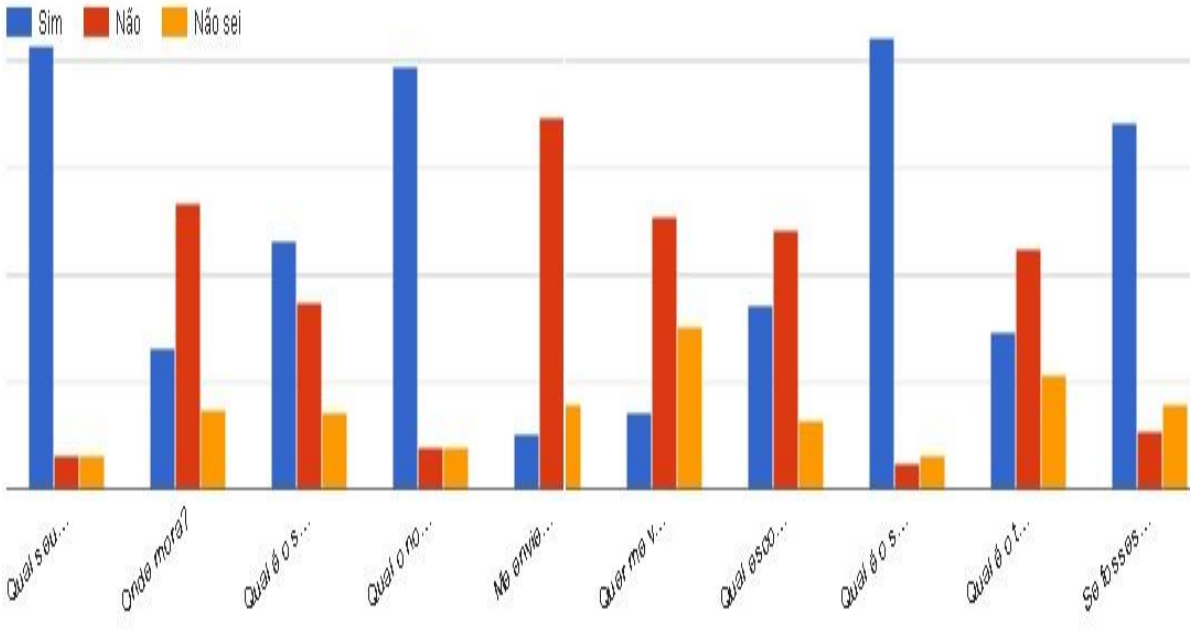
dados, provavelmente estarão desatualizados, impossibilitando a recuperação dos arquivos recentes. No item “Armazeno arquivos importantes em pelo menos dois lugares diferentes”, 31,7% dos respondentes afirma adotar essa prática, que é considerado uma ótima prática, pois há qualquer momento, um dispositivo pode dar falha, então assim, os dados não seriam perdidos. Outro tipo de backup realizado pelos usuários é o famoso “Copiar e Colar”, onde 17,5% dos respondentes afirmam utilizar essa prática. Por outro lado, 38,3% dos usuários não realiza backup ou não saberia informar.

Nesta parte dos comportamentos em situações específicas, podemos destacar os pontos positivos, onde apenas 4,2% dos entrevistados compram em qualquer loja virtual, já relacionado as redes sociais, 9,2% compartilha informações pessoais ou polêmicas sem verificar a veracidade da notícia. Na questão relacionada a utilização de senhas, 60% procura memorizar a senha, assim evita escrever ou armazenar em algum lugar. Para finalizar essa parte, foi questionado o uso de backups, 31,7% afirmam armazenar arquivos importantes em pelo menos dois dispositivos diferentes.

3.3.5 **Compartilhamento de informações**

O próximo bloco de perguntas foi dividido em 3 questionamentos, cada questão possui uma lista de perguntas sobre um tema específico. Na primeira lista foi questionado ao respondente se ele responderia a determinada pergunta de um amigo virtual, ou seja, uma pessoa que ele conhece apenas pela internet. Cada pergunta tem três alternativas, compostas por “sim”, ou seja, ele responderia à pergunta feita pelo amigo, “não”, ou seja, se negaria a responder à pergunta feita, ou “não sei”, cujo resultado está na figura 21.

Figura 21 - Perguntas de um amigo virtual



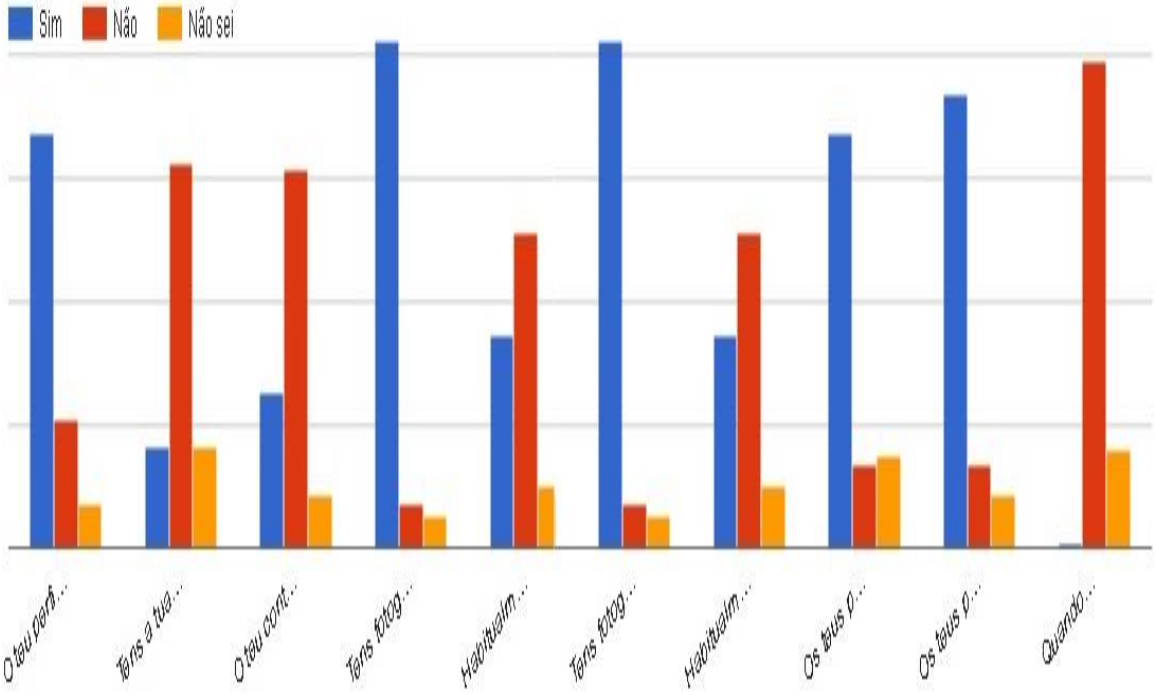
Fonte: Elaboração própria.

Podem-se observar os seguintes resultados em sequência de acordo com a resposta que prevaleceu: 86,6% dos usuários concordam em informar o seu nome; 55,8% afirmam que não informaria o lugar que reside; 48,3% concordam em informar o seu apelido; 82,5% informariam o seu grupo musical preferido; No caso do amigo virtual solicitar uma foto, 72,5% afirma que não enviaria a foto solicitada; 53,3% não concordariam em se encontrar pessoalmente com o suposto amigo; 50,8% informariam em qual escola estuda; 88,3% concordam em informar qual o seu time de futebol preferido; 46,6% não informariam o seu número de telefone; No último questionamento foi perguntado “se fosses convidado a conhecer um amigo virtual cara a cara, levavas um amigo contigo”, 71,6% afirmaram que sim, levaria um amigo para esse encontro.

De maneira geral, é possível analisar que os respondentes se preocupam ao compartilhar informações, porém é preciso evitar o compartilhamento de qualquer informação, até mesmo a informação do seu nome pode ocasionar em uma porta de entrada para pessoas más intencionadas.

O segundo questionamento desse bloco se refere as redes sociais, com o objetivo de analisar o compartilhamento e práticas do usuário dentro das redes sociais, seguindo os moldes do questionamento anterior, cujo resultado está na figura 22.

Figura 22 - Compartilhamento nas redes sociais



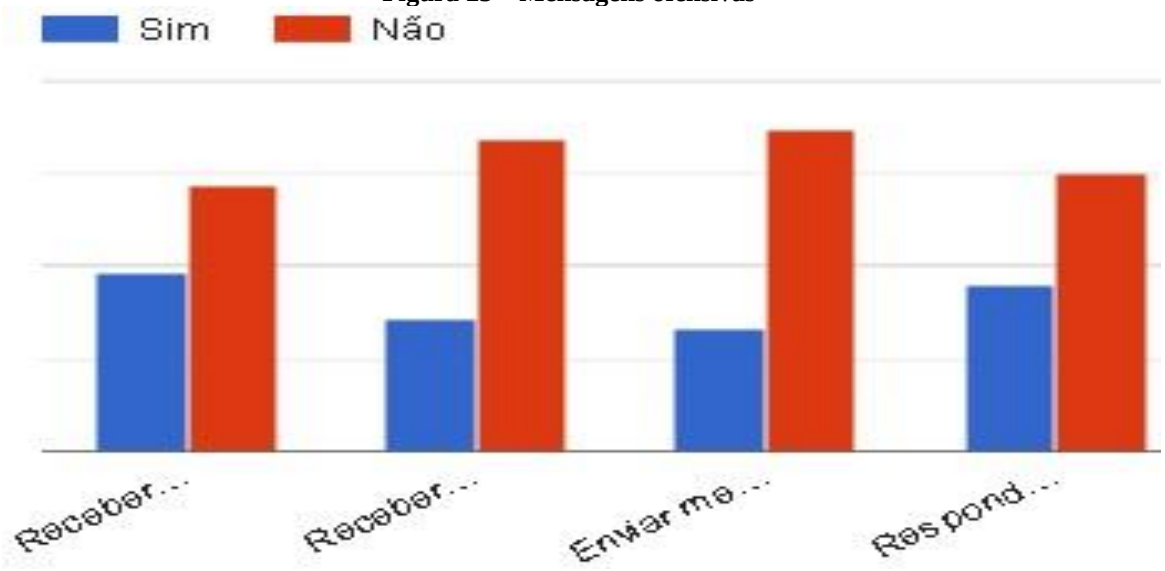
Fonte: Elaboração própria.

Notam-se na figura 22, os seguintes resultados: 70% possuem o perfil público, ou seja, o perfil é aberto para qualquer usuário da rede acessar; 65% não possui o endereço cadastrado nas redes sociais; 64,1% não possui contato telefônico no perfil; 85,8% possuem fotos publicadas; 53,3% não aceitam convites de pessoas desconhecidas; 70% afirmam que os pais possuem conhecimento do seu perfil nas redes sociais; 76,6% afirmam que os pais também possuem cadastro em redes sociais e; 82,5% não dão informação pessoal quando são questionados.

Nota-se que a maior parte dos respondentes toma cuidado na utilização das redes sociais ao não compartilhar contato telefônico e endereço. No quesito das fotos publicadas, vale ressaltar que é necessário ter cuidado com fotos íntimas publicadas, um usuário pode manipular e divulgar essas imagens causando outro olhar a essas fotos, por isso a necessidade de adicionar somente pessoas conhecidas.

No último questionamento da pesquisa, trata-se de extrair informações das experiências e situações vividas pelo respondente na internet, devido ao tamanho do questionamento, a apresentação dos resultados foi dividida em 3 partes. Na primeira parte trata-se de mensagens ofensivas enviadas ou recebidas pelo respondente, cujo resultado está na figura 23.

Figura 23 – Mensagens ofensivas

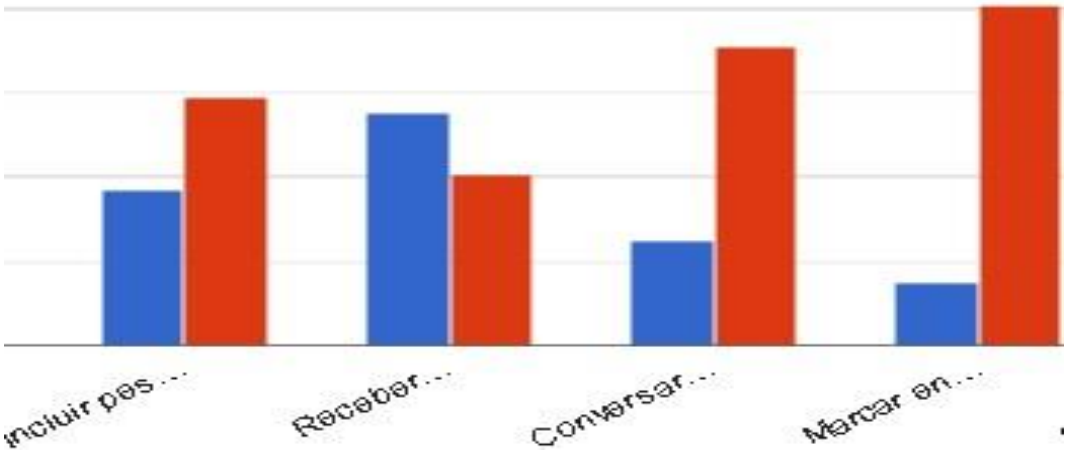


Fonte: Elaboração própria.

Seguindo a ordem, 40% afirmam já terem recebido mensagens ofensivas de pessoas desconhecidas, enquanto 30% afirmam já terem recebido essas mensagens de pessoas conhecidas (amigos/colegas). Seguindo, 72,5% afirmam não enviar mensagens ofensivas a outras pessoas. Para finalizar, 62,5% afirmam não responder mensagens ofensivas recebidas.

Na segunda parte trata-se da relação que o usuário teve com pessoas desconhecidas, cujo resultado está na figura 24.

Figura 24 – Pessoas desconhecidas



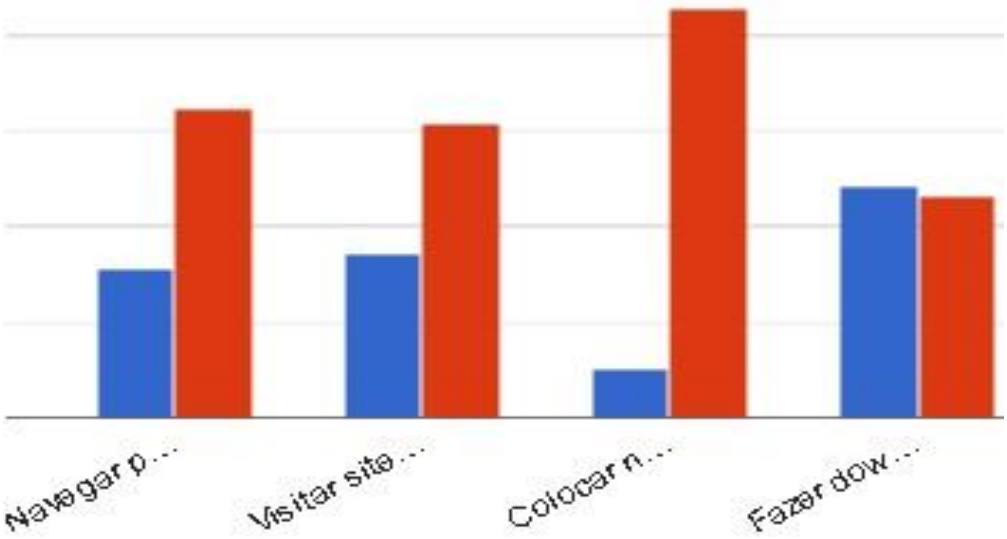
Fonte: Elaboração própria.

Seguindo a ordem, 38,3% afirmam ter incluído pessoas desconhecidas na lista de contato do Skype ou Facebook; 57,5% afirmam já terem recebido mensagens no computador ou no celular de pessoas que conheceu na internet, porém 74,1% afirmam

não conversar sobre assuntos pessoais com essas pessoas; para finalizar, 84,1% afirmam nunca terem marcado encontro com pessoas que conheceu na internet.

Na terceira e última parte trata-se de conteúdos inapropriados que circulam na internet, ou seja, conteúdos contendo violência, pornografia ou discriminação e outros casos como sites de downloads que é uma "mina" de vírus, cujo resultado está na figura.

Figura 25 – Conteúdos inapropriados



Fonte: Elaboração própria.

Seguindo a ordem, nota-se que 67,5% dos respondentes afirmam não acessar sites inapropriados; 64,1% afirmam não acessar sites pornográficos; 89,1% afirmam não colocar imagens ou vídeos contendo conteúdos inapropriados; e por último, 50,8% afirmam acessar sites de downloads não autorizados.

Podemos resumir essa parte da pesquisa com alguns pontos a serem destacados, no quesito pontos positivos podemos destacar que 72,5% não enviaria uma foto sua ao ser solicitado por alguém que conheceu na internet, também vale destacar que em caso de encontro com alguém que conheceu na internet, 71,6% levaria um amigo de confiança para o encontro. Em relação as redes sociais, podemos destacar os 82,5% que não passam informação pessoal para conhecidos da internet. Outro dado que vale destaque é que 72,5% afirma não enviar mensagens ofensivas na internet.

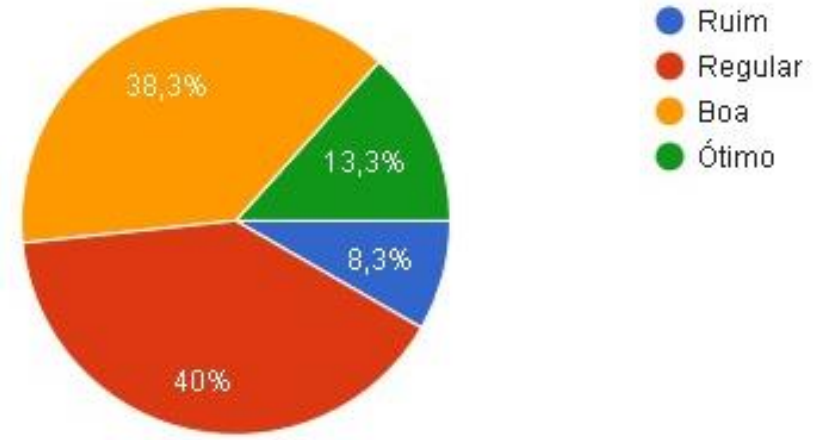
No quesito de pontos negativos podemos destacar os 38,3% afirmam ter adicionado pessoas desconhecidas no Skype e os 50,8% que afirmam acessar sites de downloads não autorizados.

3.3.6 **Perfil dos respondentes**

Como já foi abordado, esta pesquisa ocorreu com alunos entre 13 e 15 anos de idade realizado em algumas escolas públicas na cidade de Rio Branco, Acre.

Nesta última seção, será apresentado o perfil desses usuários na internet que participaram da pesquisa, com o objetivo de traçar um perfil desses usuários para dar um maior embasamento na pesquisa. Foram realizadas algumas questões com esse objetivo, avaliar o conhecimento e o uso da internet dos respondentes. O primeiro item mostra como eles se consideram usando a internet, cujo resultado está na figura.

Figura 266 - Nível de conhecimento em informática



Fonte: Elaboração própria.

E para finalizar, foi questionado o nível de conhecimento do respondente se tratando da informática em geral, e não apenas a internet. Cujo o resultado está na figura 27.

4 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES FUTURAS

Os crimes de Internet evoluíram no mesmo ritmo que as demais tecnologias, e hoje não se pode tratar um ataque como sendo um simples vírus de computador, pois existe uma gama imensa de novos tipos de ataques. Os especialistas que desenvolvem meios de combater esses ataques sempre estão um passo atrás dos criminosos, pois esses desenvolvem novas tecnologias diariamente, onde o objetivo é o mesmo, fraudar o usuário. Atualmente, esses conceitos estão sendo revistos pois foi percebido que é necessário prever e combater fraudes antes mesmo que elas possam trazer prejuízos para a sociedade em geral.

Diante dos resultados obtidos na pesquisa sobre segurança digital, foi possível perceber que os adolescentes de Rio Branco – Acre possuem conhecimento em alguns assuntos, porém foram detectadas algumas falhas ao utilizar a internet que demandam uma atenção maior, devido a pura inocência ou apenas por falta de conhecimento. Essa falta de conhecimento também é percebida pelos criminosos que atuam na internet, e isso influencia no número de ataques que acontecem diariamente. Para evitar isso, é preciso de educação e conhecimento dos usuários.

Acredita-se que a divulgação dos resultados obtidos nesta pesquisa, assim como a pequena cartilha contendo boas práticas na informática, será de grande valia, auxiliando na conscientização dos adolescentes e demais populares que tenham acesso ao material.

Porém, a facilidade com que crianças, adolescentes, adultos e até mesmo idosos interagem com a Internet incentiva cada vez mais aos criminosos desenvolverem técnicas cada dia mais surpreendentes para enganar as pessoas. Os crimes cibernéticos não são algo recente, contudo foi nos últimos anos que o número de ataques e prejuízos digitais aumentou consideravelmente, fazendo com que o assunto fosse visto com maior cuidado por especialistas, governos e educadores, assim, inserindo conhecimentos digitais para as diferentes classes sociais é capaz de quebrar barreiras entre a população

e servir como um incentivo à educação moderna, diminuindo assim a exclusão digital e deixando a população preparada para usar a internet de maneira segura, diminuindo o número de vítimas que sofrem por inocência ou por falta de conhecimento.

Recomenda-se para trabalhos futuros uma pesquisa sobre segurança da informação em âmbito escolar contemplando ensino fundamental e médio, buscando identificar comportamentos e atitudes dos alunos, se possível, comparar o uso da internet entre os alunos do ensino fundamental e do médio. Outra recomendação é para realizar um estudo com professores e alunos sobre o ensino da informática com foco em segurança nas escolas da rede pública, buscar prevê os benefícios que traria aos alunos, buscando maneiras de capacitar os professores onde muitos ainda resistem as ferramentas tecnológicas disponíveis.

REFERÊNCIAS

ALMEIDA, Maria Elizabeth Bianconcini; ALMEIDA, Fernando José de. **Uma zona de conflitos e muitos interesses. In: Salto para o Futuro: TV e Informática na Educação**.

ALVES, Cássio Bastos. **Segurança da Informação VS Engenharia Social: Como se proteger para não ser mais uma vítima.** 2010. 128 f. TCC (Graduação) - Curso de Sistemas de Informação, Universitário do Distrito Federal, Brasília, 2010.

BARBOSA, Jane Rangel Alves. **Administração pública e a escola cidadã. – ANPAE**. Porto Alegre, v. 15, n. 2, p. 217-226, jul/dez, 1999.

BENEVENUTO, Silvana G. D. **Segurança da Informação no âmbito escolar**. Natal-RN: 2008. Monografia em Biblioteconomia na Universidade Federal do Rio Grande do Norte.

CAETANO, H., MIRANDA, G. L. e SOROMENHO, G (2010). **Comportamentos de risco na internet: um estudo realizado numa escola do ensino secundário**, *Revista Latinoamericana de Tecnología Educativa RELATEC*, 9 (2), 167185.

CAMARGO SANTOS, Coriolano Aurélio de Almeida; MONTEIRO, Renato Leite. **Estruturas Críticas: O Próximo Alvo**. 2010.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** Rio de Janeiro: Crimes Virtuais, Vítimas Reais, 2014.

CERT.BR. **Cartilha de segurança para Internet.** Disponível em: <http://cartilha.cert.br/>. Acesso em: 30 out. 2018.

CRUZ, Lucas. **O que é o um encurtador de url**. Disponível em: <http://expertdigital.net/o-que-e-o-um-encurtador-de-url-link-veja-os-mais-populares/>. Acesso em: 01 nov. 2018.

FERREIRA, Fernando Nicolau Freitas. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003.

FRIGERI, Leonara Piran. **Informática na educação: um estudo sobre a utilização das tecnologias digitais na rede de ensino de Engenho Velho - RS.** 2009. 58 f. Monografia (Especialização) - Curso de Gestão Educacional, Universidade Federal de Santa Maria, Constantina, 2009.

GUISSO, Leonardo. **Segurança Digital: avaliação do nível de conhecimento da população sobre os riscos de segurança atrelados ao uso da internet na região de Bento Gonçalves.** 2017. 84 f. TCC (Graduação) - Curso de Sistemas de Informação, Universidade de Caxias do Sul, Bento Gonçalves, 2017.

HONÓRIO, Paulo Henrique Araújo. **Hackers: como se proteger?** 2003. 56 f. TCC (Graduação) - Curso de Ciências da Computação, Centro Universitário do Triângulo, Uberlândia, 2003.

MULLER, Nicolas. **Diferença entre Ransomware, RAT, Backdoor, Worm e Bot**. 2018. Disponível em: <https://www.oficinadanet.com.br/post/18266-diferenca-entre-ransomware-rat-backdoor-worm-e-bot>. Acesso em: 20 set. 2018.

NOVAES, Rafael. **Conheça os malwares do tipo Time Bomb**. 2014. Disponível em: <https://www.psafe.com/blog/time-bomb/>. Acesso em: 30 out. 2018.

Secretaria de Educação a Distância, Brasília: Ministério da Educação e do Desporto, SEED, 1998.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

SERRANO, Paulo. **Cuidados que se deve ter com o seu computador o seu computador o seu computador o seu computador** – Campinas: Campus CCUEC, 2001.

SILVEIRA, Debora Priscila. **Vantagens e desvantagens das redes sociais**. 2017. Disponível em: <https://www.oficinadanet.com.br/post/18285-vantagens-e-desvantagens-das-redes-sociais>. Acesso em: 20 set. 2018.

TORRES, Gabriel. **Vírus.** 1997. Disponível em: <https://www.clubedohardware.com.br/artigos/programas/v%C3%ADrus-r33867/>. Acesso em: 30 out. 2018.

TREND MICRO. **Ransomware: o que é e como se proteger?** 2015. Disponível em: <http://blog.trendmicro.com.br/ransomware-o-que-e-e-como-voce-pode-seproteger>. Acesso em: 30 out. 2018.

WENDT, E. JORGE, Higor Vinicius Nogueria (2013). "**Crimes Cibernéticos" Ameaças e Procedimentos de Investigação**. Rio de Janeiro, Brasport, 2ªedição.

VALENTIM, M. L. P. **Inteligência competitiva em organizações: dado, informação e conhecimento**. DataGramaZero, Rio de Janeiro, v.3, n.4, ago. 2002.

SOCIAL, We Are. **DIGITAL IN 2017: GLOBAL OVERVIEW.** Disponível em: <https://wearesocial.com/special-reports/digital-in-2017-global-overview>. Acesso em: 20 set. 2018.

SOCIAL, We Are. **GLOBAL DIGITAL REPORT 2018.** Disponível em: <https://digitalreport.wearesocial.com/>. Acesso em: 15 jan. 2019.

WENDT, Emerson. **Inteligência cibernética: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil [recurso eletrônico]** / Emerson Wendt. – livro digital. – São Paulo: Editora Delfos, 2011.

APÊNDICE A - PESQUISA DE ANÁLISE SOBRE COMPORTAMENTOS EM SEGURANÇA DIGITAL

1. **Marque a opção que melhor define você como usuário de internet**
Mark only one oval.

- ◯ Principiante / Pouco conhecedor
- ◯ Curioso / Impulsivo
- ◯ Reflexivo / Cauteloso
- ◯ Conhecedor avançado

2. **A partir de onde é que habitualmente se liga à Internet?**
Check all that apply.

- ☐ Estabelecimento comercial
- ☐ Não tenho acesso à internet
- ☐ Escola
- ☐ Casa
- ☐ Casa de familiares/amigos

3. **Como você avalia seu conhecimento em informática?**
Mark only one oval.

- ◯ Ruim
- ◯ Regular
- ◯ Boa
- ◯ Ótimo

4. **Que tipo de equipamentos/dispositivos utiliza para se conectar à internet?**
Check all that apply.

- ☐ Computador fixo (PC)
- ☐ Computador portátil (Ex: Notebook)
- ☐ Dispositivo móvel (Ex: Celular "Smarthpone", Tablet)
- ☐ Other: _____

5. **Com que frequência utiliza a internet?**
Mark only one oval.

- ◯ Todos ou quase todos os dias da semana
- ◯ Uma ou duas vezes por semana
- ◯ Somente nos finais de semana
- ◯ Raramente acesso a internet

6. **Que tipo de programas/aplicações costuma utilizar na internet?**
Check all that apply.

- [ ] Navegadores (Google Chrome, Mozilla Firefox, Opera)
- [ ] Jogos online
- [ ] Youtube
- [ ] Redes Sociais (Facebook, Twitter, Instagram, Google+)
- [ ] Chats (Whatsapp, Telegram, Skype, Google Chat)
- [ ] Correio Eletrônico (Gmail, Windows Live, Yahoo, Apple Mail)

7. **Considera que a navegação que faz na internet é segura?**
Mark only one oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei

8. **Qual o significado da nomenclatura HTTPS, inserida no início do endereço de alguns sites?**
Mark only one oval.

- ◯ Conexão Insegura
- ◯ Recurso visual, sem importância
- ◯ Conexão realizada através de uma camada extra de segurança
- ◯ Não saberia informar

9. **O principal objetivo da criptografia de dados é que só o destinatário certo e com a chave específica possa ter acesso a determinada informação. Você já utilizou a criptografia de dados?**
Mark only one oval.

- ◯ Utilizo com bastante frequência
- ◯ Utilizo apenas para arquivos/assuntos confidenciais
- ◯ Raramente utilizo
- ◯ Nunca utilizei
- ◯ Não saberia informar

Nas questões de 10 a 14, avalie as afirmações:

10. **"Durante operações bancárias realizadas na internet, uma prática de segurança comum é digitar a senha incorreta no primeiro acesso, para validar se o site é legítimo".**
Mark only one oval.

- ◯ Concordo
- ◯ Discordo
- ◯ Não saberia informar

11. **"Links de sites encurtados, exemplo: 'goo.gl/Rio8ff', são utilizados para fraudes pois dificultam a identificação do site que estamos sendo direcionados".**
Mark only one oval.

- ◯ Concordo
- ◯ Discordo
- ◯ Não saberia informar

12. **"Criminosos da internet possuem maior interesse em atacar computadores de grandes empresas, por isso os usuários domésticos estão protegidos"**
Mark only one oval.

- ◯ Concordo
- ◯ Discordo
- ◯ Não saberia informar

13. **"Uma empresa legítima não solicitará informações pessoais em uma mensagem de e-mail. Apesar de parecerem convincentes, mensagens que solicitam informações pessoais com urgência provavelmente são falsas"**
Mark only one oval.

- ◯ Concordo
- ◯ Discordo
- ◯ Não saberia informar

14. **"Redes Wi-Fi domésticas possuem sinal de curto alcance, logo não é necessário a utilização de senhas difíceis".**
Mark only one oval.

- ◯ Concordo
- ◯ Discordo
- ◯ Não saberia informar

15. **"Todos possuem informações pessoais compartilhadas online, que são obtidas principalmente através de cadastros" Dentre os itens abaixo, avalie se você concorda ou não em compartilhá-los:**
Check all that apply.

	Concordo em compartilhar	Discordo em compartilhar	Não saberia informar
Telefones para contato	☐	☐	☐
Informações bancárias	☐	☐	☐
CPF/RG	☐	☐	☐
Endereço	☐	☐	☐
Perfil do Facebook/G+,Twitter	☐	☐	☐

16. **Sobre o assunto compras pela internet (Lojas Online/Google Play Store/Apple Store), marque as opções que caracterizam sua utilização com o seu responsável (pai/mãe/outro):**
Check all that apply.

- [ ] Realizo compras somente em redes conhecidas ou privadas
- [ ] Procuro obter detalhes da loja que estou comprando (Procedência, CNPJ, sites como o reclameaqui)
- [ ] Preços abaixo do normal me atraem e com rapidez realizo compra antes que a promoção acabe
- [ ] Realizo compras conectado em qualquer rede
- [ ] Não realizo compras pela internet

17. **Sobre o uso de "Redes Sociais", qual(is) dos comportamentos abaixo você utiliza no seu dia dia?**
Check all that apply.

- [ ] Adiciono somente pessoas conhecidas ou que mantenho algum contato
- [ ] Clico em todos os links que vejo e que me despertam curiosidade
- [ ] Compartilho informações pessoais e problemas particulares
- [ ] Utilizo configurações de privacidade, onde somente pessoas que desejo podem ver as informações que compartilho
- [ ] Compartilho notícias polêmicas sem verificar a veracidade da informação
- [ ] Não saberia informar
- [ ] Não utilizo rede sociais

18. **Marque a (as) opções que caracterizam o seu comportamento com o uso de senhas:**
Check all that apply.

- [ ] Realizo troca de senhas com frequência
- [ ] Utilizo palavras de fácil memorização (nome dos pais, namorado(a), data de nascimento, times de futebol, etc.)
- [ ] Procuro memorizar as senhas, assim evito de escrever em qualquer lugar
- [ ] Procuro utilizar a mesma senha em todos os acessos
- [ ] Anoto minhas senhas em cadernos e agendas para não esquecer

19. **"Backups ou cópias de segurança podem ser utilizados para restaurar dados que foram perdidos, apagados, roubados ou corrompidos". Marque a (as) opções que definem seu comportamento sobre backups:**
Check all that apply.

- [ ] Armazeno arquivos importantes em pelo menos dois locais diferentes
- [ ] Faço backup dos arquivos duplicando (Copiando e colando) eles no mesmo local
- [ ] Possuo backups dos meus arquivos, mas raramente atualizo essas informações
- [ ] Não realizo backups dos meus arquivos
- [ ] Não saberia informar

20. **Se um amigo virtual te perguntasse as seguintes questões, num Chat ou outra ferramenta, você respondia:**

Mark only one oval per row

	Sim	Não	Não sei
Qual seu nome?	◯	◯	◯
Onde mora?	◯	◯	◯
Qual é o seu apelido?	◯	◯	◯
Qual o nome do teu grupo musical favorito?	◯	◯	◯
Me envie uma foto sua?	◯	◯	◯
Quer me ver pessoalmente?	◯	◯	◯
Qual escola você estuda?	◯	◯	◯
Qual é o seu time de futebol preferido?	◯	◯	◯
Qual é o teu número de telefone?	◯	◯	◯
Se fosses convidado a conhecer um amigo virtual cara a cara, levavas um amigo contigo?	◯	◯	◯

21. **Em relação as Redes Sociais(Facebook, Twitter, Instagram, etc):**

Mark only one oval per row

	Sim	Não	Não sei
O teu perfil é público?	◯	◯	◯
Tens a tua morada nessa rede?	◯	◯	◯
O teu contato telefônico está no teu perfil?	◯	◯	◯
Tens fotografias publicadas?	◯	◯	◯
Habitualmente aceitas convites de pessoas desconhecidas?	◯	◯	◯
Os teus pais têm conhecimento da tua página na rede social a que pertences?	◯	◯	◯
Os teus pais pertencem a alguma rede social?	◯	◯	◯
Quando me pedem informação pessoal, habitualmente dás?	◯	◯	◯

22. **Das experiências/situações que teve na Internet já aconteceu alguma(s) da(s) que apresentamos?**
Check all that apply.

	Sim	Não
Receber mensagens com ameaças ou comentários desagradáveis de pessoas desconhecidas	☐	☐
Receber mensagens com ameaças ou comentários desagradáveis de pessoas conhecidas (amigos/colegas)	☐	☐
Enviar mensagens ofensivas a outras pessoas	☐	☐
Responder a mensagens ofensivas	☐	☐
Receber mensagens com conteúdos inapropriados (fotos, vídeos, animações, etc.)	☐	☐
Incluir pessoas desconhecidas nas listas de contacto do Skype, Facebook, etc.	☐	☐
Receber mensagens no computador/telemóvel de pessoas que conheceu na Internet	☐	☐
Conversar sobre assuntos pessoais com alguém que apenas conheceu na Internet	☐	☐
Marcar encontros com pessoas que conheceu na Internet	☐	☐
Navegar por sites com conteúdos impróprios (conteúdo sexual, violência, discriminação, etc.)	☐	☐
Visitar sites para adultos	☐	☐
Colocar na Internet imagens ou vídeos com conteúdos inapropriados	☐	☐
Fazer downloads ilegais de músicas, filmes, jogos, software, etc.	☐	☐
Entrar, sem autorização, nos espaços de Internet de outros utilizadores	☐	☐
Fazer de conta que é outra pessoa a enviar mensagens a outros utilizadores	☐	☐
Ligar uma Webcam para que todos os utilizadores o possam ver na Internet	☐	☐
Criar uma personagem virtual ou um perfil falso	☐	☐
Ter mais do que um perfil nas redes sociais	☐	☐

Para acessar o Livro da Cartilha de Segurança para Internet, contendo boas práticas de uso na internet, acesse: https://cartilha.cert.br/livro/

APÊNDICE B - CARTILHA DE SEGURANÇA

Acesso à Internet

- ✓ Verifique a privacidade nas redes sociais, não deixe dados pessoais acessíveis;
- ✓ Utilize sites seguros sempre que possível, de preferência aqueles que possuem HTTPS;
- ✓ Não revele dados pessoais à estranhos ou pessoas conhecidas na internet;
- ✓ Caso precise falar algo sigiloso, procure falar por telefone ou pessoalmente;
- ✓ De acordo com sua publicação, defina se todos podem visualizar ou apenas amigos;
- ✓ Evite usar a webcam com estranhos, sua imagem pode ser manipulada e divulgada;
- ✓ Não envie fotos comprometedoras, elas tendem a se propagar na internet;
- ✓ Caso se sinta ameaçado, grave as conversas e bloqueie o contato do agressor;
- ✓ Faça operações apenas nos seus dispositivos pessoais;
- ✓ Cuidado ao clicar em links, independente de quem os enviou.

Computadores Pessoais/Notebooks

- ✓ Mantenha os programas atualizados;
- ✓ Use apenas programas originais;
- ✓ Instale um antivírus confiável;
- ✓ Utilize senhas longas, compostas de diferentes tipos de caracteres;
- ✓ Faça backups regularmente;
- ✓ Mantenha a data e hora atualizada;
- ✓ Ao usar computadores de terceiros:
    - Utilize a opção de navegar anonimamente;
    - Não efetue transações bancárias;
    - Não armazene senhas ou logins.
- ✓ Ao enviar o seu computador para assistência técnica:
    - Selecione empresas de boas referências;
    - Não permita a instalação de programas piratas;

Dispositivos Móveis

- ✓ Instale um programa antivírus, antes de instalar qualquer outro aplicativo;
- ✓ Não siga links recebidos nos aplicativos de mensagens como WhatsApp;
- ✓ Não acredite em promoções e prêmios através de links recebidos por mensagem;

- ✓ Mantenha o controle físico do seu dispositivo, não o deixe em cima de mesas;
- ✓ Cadastre senhas bem elaboradas, evite usar dados fáceis como data de nascimento;
- ✓ Se possível, utilize a opção “biometria” para desbloquear o seu dispositivo;
- ✓ Seja cuidadoso ao dar permissões à aplicativos, utilize apenas aplicativos confiáveis;
- ✓ Faça backups dos seus dados regularmente;
- ✓ Use uma conexão segura ao realizar comunicação que envolva dados confidenciais;
- ✓ Cuidado ao usar um Wi-Fi público, pois muitas pessoas têm acesso a ela.
- ✓ Mantenha Bluetooth e Wi-Fi desabilitado, ative somente quando for necessário;
- ✓ Configure a conexão Bluetooth para não ser descoberta por outros aparelhos;
- ✓ Ao instalar aplicativos:
    - Procure obter aplicativos de fontes confiáveis, como o Google Play;
    - Escolha aplicativos bem avaliados e com grande quantidade de usuários;
    - Verifique o aplicativo à ser instalado através de um antivírus;
    - Observe as permissões solicitadas pelo aplicativo, verifique a coerência.
- ✓ Ao se desfazer do dispositivo:
    - Apague todas as informações nele contidos;
    - Restaure as configurações de fábrica.
- ✓ Em caso de perca ou roubo:
    - Configure-o previamente para ser localizado e bloqueado remotamente;
    - Informe sua operadora e solicite o bloqueio do chip;
    - Bloqueie cartões de créditos que estejam armazenados no dispositivo;

Conteúdo produzido com auxílio do site:

https://cartilha.cert.br/