UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE FORMAÇÃO DE OFICIAIS

DAVID COSTA CARVALHO DOS SANTOS

SEGURANÇA DIGITAL: análise dos procedimentos em segurança da informação atrelada ao uso da internet por militares do Comando Geral na PMMA

São Luís
2018

DAVID COSTA CARVALHO DOS SANTOS

SEGURANÇA DIGITAL: análise dos procedimentos em segurança da informação atrelada ao uso da internet por militares do Comando Geral na PMMA

Monografia apresentada ao Curso de Formação de Oficiais da PMMA integrado com a Universidade Estadual do Maranhão como pré-requisito para a obtenção do título de Bacharel em Segurança Pública.

Orientador: Cap. QOPM Paulo Edson Cutrim Silva

São Luís
2018

Santos, David Costa Carvalho dos.
Segurança digital: análise dos procedimentos em segurança da informação atrelada ao uso da Internet por militares do Comando Geral na PMMA / David Costa Carvalho dos Santos. – São Luís, 2018.

81 fs

Monografia (Graduação) – Curso de Formação de Oficiais, Universidade Estadual do Maranhão, 2018.

Orientador: Prof. Paulo Edson Cutrim Silva.

1.Internet. 2.Polícia militar. 3.Segurança da informação. I.Título

CDU: 355.405(812.1)

Elaborado por Giselle Frazão Tavares – CRB 13/665

DAVID COSTA CARVALHO DOS SANTOS

SEGURANÇA DIGITAL: análise dos procedimentos em segurança da informação atrelada ao uso da internet por militares do Comando Geral na PMMA

Monografia apresentada ao Curso de Formação de Oficiais da PMMA integrado com a Universidade Estadual do Maranhão como pré-requisito para a obtenção do título de Bacharel em Segurança Pública.

Orientador: Cap. QOPM Paulo Edson Cutrim Silva

Aprovada em:____ /____ / 2018

BANCA EXAMINADORA

Capitão QOPM Paulo Edson Cutrim Silva (Orientador)

Polícia Militar do Maranhão

Capitão QOPM Fábio Henrique Magalhães Facundes

Polícia Militar do Maranhão

Prof. Me. Luís Carlos Santos Rodrigues

Universidade Estadual do Maranhão

Dedico esta monografia a Deus. Sem Ele nada seria possível. Aos meus pais Gisberto Carvalho e Jaciara Costa, minha esposa Janiele Carvalho, aos meus irmãos e à toda minha família.

AGRADECIMENTOS

Primeiramente a Deus, por ter me concedido saúde e força necessárias para vencer mais uma etapa. A fé que tenho no Senhor foi o combustível para minha disciplina, persistência e força. Obrigado Senhor, por todas as bênçãos que recaíram sobre mim e a todos aqueles que amo!

Aos meus avós Albino (in memorian) e Maria José (in memorian), Geraldo e Jacira Costa, que sempre buscaram uma vida melhor para nossa família. Sem eles este trabalho e muito dos meus sonhos não se realizariam.

À minha mãe Jaciara Costa, que encheu meu coração de amor e esperança. Sem ela nada teria conquistado, pois ensinou-me que o futuro é feito a partir da constante dedicação no presente. Agradeço a minha vida à senhora.

Ao meu pai Gisberto Carvalho por ser minha motivação e fonte de inspiração, que juntamente com minha mãe dedicaram integralmente suas vidas para me educar. Eles são os responsáveis pelo meu sucesso.

Aos meus irmãos Jaqueline, Rogério, Gláucia e Everton, que nos momentos de minha ausência para dedicar-me aos estudos, sempre me apoiaram e não me deixaram desistir de realizar este sonho.

À minha esposa Janiele Carvalho que me ajudou na confecção desta monografia, me estimulou durante todo esse tempo e compreendeu minha ausência nos momentos ruins. Obrigado por ter dedicado seu tempo a mim, principalmente nos momentos mais difíceis. Obrigado por existir em minha vida!

Às cidades de Olinda/Recife e ao estado de Pernambuco, minha terra natal, local onde a bravura e a coragem pernambucana prevalecem. Pernambuco representa o berço de nossa nação!

Ao colégio da Polícia Militar de Pernambuco.

À universidade Estadual do Maranhão, que contribuiu em minha formação acadêmica.

Aos professores da Universidade Estadual do Maranhão.

Aos professores e instrutores do curso de Formação de Oficiais.

Ao senhor Capitão QOPM Paulo Edson Cutrim, meu orientador, que aceitou esse desafio, e juntamente comigo, me auxiliou a construir e defender essa monografia. Agradeço também pelo suporte durante esse tempo que lhe coube, pelas suas orientações, correções e pelos incentivos nessa jornada.

Aos oficiais da Academia de Polícia Militar “Gonçalves Dias”, que sempre nos motivaram e contribuíram em nossa formação durante esses anos.

À 21ª turma “Bravos Infantes” do Curso de Formação de Oficiais ao qual considero minha segunda família que, diante das dificuldades, me acolheram com muito carinho. Lembrarei para sempre de todos os cadetes, especialmente dos Cadetes João Rocha e Rômulo Ribeiro que ao início do curso me ampararam. Jamais esquecerei! Muito obrigado, sempre serei grato a vocês! Agradeço também aos Cadetes José Neto, Max Bogéa, Jhones Batista, Cleiton Vieira e Claudir Ewerton pela amizade sincera.

Por fim, agradeço a todos que direta ou indiretamente participaram e ajudaram-me a subir mais um degrau.

“Seu trabalho vai preencher uma parte grande de sua vida, e a única maneira de ficar realmente satisfeito é fazer o que você acredita ser um ótimo trabalho. E a única maneira de fazer um excelente trabalho é amar o que você faz.”

Steve Jobs

RESUMO

Na era digital, o papel da segurança da informação é de fundamental importância para as instituições. Com o crescimento e evolução da tecnologia juntamente com a popularidade da internet, surge também um grande problema: os chamados crimes cibernéticos. Os militares que trabalham no Quartel do Comando Geral foram inseridos no meio digital de maneira desnorteada e sem a cultura de ter um acesso seguro às informações, o que poderia torná-los alvos fáceis entre pessoas mal-intencionadas. Desta forma, o presente trabalho buscou analisar os procedimentos em segurança da informação dos militares que trabalham no Comando Geral da Polícia Militar do Maranhão atrelados ao uso da Internet. A partir dessa análise foi possível observar os perigos e vulnerabilidades dos mesmos, evidenciando os erros e ações durante o uso dessa ferramenta e mensurando o nível de conhecimento dos militares sobre segurança digital. Além disso, foi abordada nesta pesquisa o surgimento e história da Internet, boas práticas em segurança, estatísticas sobre os riscos, crescimento dos ataques e vulnerabilidades, assim como alguns conceitos técnicos de autores consagrados no assunto. A pesquisa caracteriza-se metodologicamente como aplicada, não probabilística, quantitativa, levantamento de dados e descritiva. Neste estudo, 35 militares pertencentes ao Comando Geral responderam a um questionário. Os dados refletem a necessidade de criação de uma política de segurança. Em contrapartida, há um déficit de procedimentos em segurança da informação. Ainda que existam ferramentas que ajudem na prevenção dos ataques, estas parecem não ser suficientes diante da problemática enfrentada pelo fator humano.

Palavras-chave: Internet. Polícia Militar do Maranhão. Segurança da Informação.

ABSTRACT

In the digital age, the role of information security is of fundamental importance to institutions. With the growth and evolution of technology along with the popularity of the internet, there is also a big problem: the so-called cyber crimes. The military working at the General Command Headquarters were bogged down in the digital environment and without the culture of having secure access to information, which could make them easy targets among malicious people. In this way, the present work sought to analyze the procedures in information security of the military that work in the General Command of the Military Police of Maranhão linked to the use of the Internet. From this analysis it was possible to observe the dangers and vulnerabilities of the same, showing the errors and actions during the use of this tool and measuring the level of knowledge of the military on digital security. In addition, the Internet's emergence and history, good security practices, risk statistics, attacks growth and vulnerabilities, as well as some technical concepts by authors related to the subject were discussed in this research. The research is characterized methodologically as applied, non-probabilistic, quantitative, data collection and descriptive. In this study, 35 military personnel belonging to the General Command responded to a questionnaire. The data reflect the need to create a security policy. On the other hand, there is a shortage of information security procedures. Although there are tools that help in the prevention of attacks, they do not seem sufficient in the face of the problem faced by the human factor.

Keywords: Internet. Maranhão Military Police. Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

APMGD - Academia de Polícia Militar do Maranhão

CFO - Curso de Formação de Oficiais

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

DHCP - *Dynamic Host Configuration Protocol*

DNS - *Domain name system*

DHCP - *Dynamic Host Configuration Protocol*

FTP - *File Transfer Protocol*

FSF - *Free Software Foundation*

Gnu - *is Not Unix*

HTTP - *Hypertext Transfer Protocol*

HTTPS - *Hyper Text Transfer Protocol Secure*

IMAP - *Internet Message Access Protocol*

ISP - *Internet Service Provider*

IPV4 - *Internet Protocol Version 4*

IP - *Internet Protocol*

ICP - Infra-Estrutura de Chaves Públicas

NBR – Norma brasileira

MIT - Instituto de Tecnologia de Massachusetss

POP3 - *Post Office Protocol version 3*

PMMA - Polícia Militar do Maranhão

QCG – Quartel do Comando Geral

SSH - *Secure Shell*

SMTP - *Simple Mail Transfer Protocol*

TI - Tecnologia da Informação

TKIP - *Temporal Key Integrity Protocol*

TCP – *Transmission Control Protocol*

UEMA – Universidade Estadual do Maranhão

URL - *Uniform Resource Locator*

W3C - *World Wide Web Consortium*

WPA - *Wi-Fi Protected Access*

WEP - *Wired Equivalent Privacy*

SUMÁRIO

1 INTRODUÇÃO

A internet é considerada atualmente o maior canal de circulação de informações que existe. Fundada nos Estados Unidos, seu objetivo inicial era interligar a Universidade da Califórnia ao Instituto de Pesquisa de Stanford a fim de realizar o compartilhamento de informações entre as duas instituições. Cada vez mais vigente no dia-a-dia, esta rede vem fornecendo uma imensa quantidade de conhecimentos perante nossos olhos.

Na era da informação, as tecnologias computacionais mudam rapidamente. Assim, quem possui informação passa a possuir também o poder para decidir e solucionar de maneira rápida os grandes problemas e obstáculos que surgem. A informação é de suma importância para a instituição. Sobre esse conceito, Silva Filho (2010) destaca que:

> Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando ela ser lida, modificada ou até mesmo apagada.

Contudo, com o desenvolvimento das tecnologias computacionais, também cresceu o interesse por essas informações que circulam na rede, permitindo que o número de casos de roubo e destruição de informações se ampliassem nas mesmas proporções. Assim, a necessidade de proteção dos ativos das instituições se tornou um ponto-chave e uma necessidade dentro das empresas.

Algumas instituições estão com as atenções voltadas na administração ferramentas, infraestrutura física, soluções criptográficas, invasões e em outros termos relacionados. Isso é natural, porém esquecem de tomar alguns cuidados com os aspectos humanos de uma organização e deixam esses fatores em segundo plano.

A segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade e confidencialidade. São estes os atributos que constituem os seus pilares (SILVA FILHO, 2004).

Foi constatada durante a pesquisa a existência de alguns hábitos não compatíveis com a segurança da informação (SI), além de não possuírem alguns

conhecimentos e procedimentos em segurança digital, fazendo com que todo esse risco seja capaz de danificar não só os equipamentos computacionais, como também expor de maneira perigosa todas as informações. Diante disso, a necessidade de proteger os ativos da rede se faz presente.

Por vezes os militares do QCG não sabem os perigos que se encontram na web e tornam a navegação vulnerável a ataques, além de concederem acesso a pessoas não autorizadas e mal-intencionadas prontas para roubar as informações.

Algumas tarefas importantes são realizadas através da internet, como transações bancárias, compras, comunicação e armazenamento de arquivos para o envio de documentos. Esses diversos meios de utilizar a rede se expandiram celeremente no mundo inteiro. No entanto, a partir do momento em que tais tecnologias foram inseridas no cotidiano das pessoas, a forma como nos relacionamos com o outro e com o mundo também se transformou, a começar pelos modos de comunicação e de trabalho. Visto isso, “navegar” no presente não é mais uma questão de escolha, e sim uma questão de necessidade.

Nesse exato momento, existem organizações criminosas especializadas em ciberataque planejando o próximo ataque pela internet em diversas partes do mundo, inclusive no Brasil. É comum ver notícias sobre invasões, falhas em segurança da informação em corporações ou até mesmo em órgãos públicos, conhecidos como sequestro de dados. Esses ataques estão atingindo diversas empresas – inclusive algumas instituições governamentais devido a sua vulnerabilidade.

Na região sul do Brasil, uma instituição pública sofreu um ataque em seu banco de dados no dia 12 de janeiro de 2018. Segundo o site G1[1], durante o ataque os invasores adentraram na rede da prefeitura, impedindo o acesso dos funcionários aos sistemas de informações e impossibilitando-os de acessarem a quase todos os programas. Com isso, muitos dos serviços à população ficaram interrompidos.

A realidade institucional da Polícia juntamente com os ataques sofridos pela organização referente à segurança da informação traz à tona a importância desse

---

[1] G1. Portal de Notícias – Globo. **Hackers invadem site da prefeitura de Jóia e cobram pagamento de 4 mil dólares em bitcoin**. Jan/2018 Disponível em: <https://g1.globo.com/rs/rio-grande-do-sul/noticia/hackers-invadem-site-da-prefeitura-de-joia-e-cobram-pagamento-de-4-mil-dolares-em-bitcoin.ghtml> acesso em: 02 maio, 2018.

tema. Desta forma, esta pesquisa busca abordar a segurança da informação a partir de uma esfera pouco explorada: o fator humano. Poucas são as literaturas a respeito disso. No entanto, é importante considerar que a segurança da informação não envolve somente fatores tecnológicos, mas também questões culturais. Um dos principais problemas enfrentados pela segurança digital é a segurança em pessoas. A contribuição dos usuários é de fundamental importância para a sua eficácia.

Assim, esse trabalho analisou os procedimentos dos militares que utilizam esta ferramenta mas que muitas vezes não sabem ou ignoram os riscos no vazamento de informações consideradas sigilosas e importantes para a corporação militar.

O objetivo geral desta pesquisa é realizar uma análise dos procedimentos em segurança da informação aos militares que trabalham nas atividades administrativas do Quartel do Comando Geral (QCG).

Para atingir esse objetivo, será necessário expor os perigos encontrados na internet e, através de um diagnóstico, mensurar o nível de conhecimento dos militares sobre segurança digital, evidenciando erros ou ações realizadas em segurança digital nesta instituição. A problemática fundamental deste trabalho questiona os procedimentos dos militares ao utilizar a tecnologia da informação em consonância com a ferramenta internet.

A coleta dos dados foi realizada através de um questionário estruturado, contendo 11 perguntas do tipo fechada, aplicado entre os meses de setembro e outubro de 2018. Foram realizadas também pesquisas em livros, artigos e trabalhos científicos com o objetivo de reunir informações e dados que servirão de base para a construção da investigação.

A análise dos dados realizou-se no mês de novembro e a partir dela foi feita uma síntese que trouxe explicações aos questionamentos das investigações. Simultaneamente, a interpretação extraiu ao extremo essas informações, analisando profundamente cada resposta, possibilitando o cruzamento destas com outras informações sobre o tema. As análises foram apresentadas em forma de gráficos para um melhor entendimento.

Esse trabalho foi estruturado em títulos para uma melhor organização. O primeiro título é formado pela introdução, na qual constam informações relativas ao tema, o problema que motivou essa pesquisa, os objetivos da pesquisa, metodologia e a justificativa.

No segundo título é apresentado o embasamento teórico do trabalho, abordando os pressupostos das redes de computadores. Essa parte explicará como é o funcionamento de uma rede de computador e seu surgimento, alguns conceitos iniciais a fim de explicar ao leitor a definição das redes de computadores no âmbito da tecnologia da informação, conceitos de protocolo e para que serve, além do surgimento e funcionamento da internet.

O terceiro título consta a segurança na rede de computador, assim como os conceitos de criptografia, assinatura digital, certificado digital e “firewall” de uma rede.

O quarto título relata o contexto da segurança da informação com conceitos sobre a diferença entre *hacker* e *cracker,* o ciclo da informação, os ataques em redes, as principais vulnerabilidades (tanto das máquinas e quanto dos humanos) a tais investidas, e os incidentes envolvendo o uso da internet.

O quinto título é referente à metodologia utilizada no trabalho, ao qual tem seu foco voltado para uma pesquisa responsável por avaliar o nível de conhecimento em segurança digital para o público militar que desenvolve suas funções no QCG.

O sexto título diz respeito a análise dos dados obtidos na pesquisa, assim como a análise dos resultados.

Por fim, no último título serão demonstradas as conclusões alcançadas a partir do referencial teórico, da metodologia e da pesquisa em questão.

2 PRESSUPOSTOS DAS REDES DE COMPUTADORES

Nesse título temos por finalidade abordar o surgimento e evolução das redes, com o objetivo de explicar o seu funcionamento e protocolos, além de exibir as topologias de rede mais utilizada no QCG.

2.1 Funcionamento de uma rede

O surgimento das redes de computadores se deu bem antes da criação da internet, e compreende ser “[...] responsável por prover a conectividade de dados, voz e vídeo à organização tanto na rede local, quanto ao acesso externo por meio da internet” (LAUDON E LAUDON, 2011).

Com a evolução dos microcomputadores, essa tecnologia permitiu a instalação de diversas dessas máquinas com certo grau de processamento, capazes de trocar e compartilhar alguns recursos. Assim com descreve Mazzola (2000, p.1.1):

> A evolução da microeletrônica e da informática tem possibilitado a obteção de processadores e outros componentes cada vez mais potentes e velozes, num tamanho mais reduzido e cada vez mais acessível a um maior número de pessoas.

O surgimento dos microcomputadores foi essencial na necessidade que surgia. Mazzola, (2000, p.1.1) também relata que “nos anos 70, com o surgimento dos minicomputadores, foi possível adaptar as capacidades de processamento às reais necessidades de uma aplicação”. Assim, a popularização dessa tecnologia dava seus primeiros passos.

O IP de uma máquina determina sua identificação necessária para o envio e recebimento de arquivos, ou seja, esta é de suma importância para a troca de informações. Dessa forma, para um dispositivo conectar-se com uma rede e iniciar uma conexão com outros dispositivos, é fundamental que ele receba um número de identificação denominado *Internet Protocol* (IP) – protocolo de internet. Como explicita Arnett (1997, p. 53), “em uma interligação em rede, o endereço de um dispositivo é sua identificação exclusiva. Normalmente, os endereços são numéricos e seguem um formato padrão bem definido [...]”.

Qualquer dispositivo *host* ligado à internet, independentemente de sua natureza, necessitará possuir um endereço IP. Esse acesso é realizado por meio de

um *Internet Service Provider* (ISP), ou como conhecido no Brasil, um Provedor de Serviço de Internet. Os ISP's são organizações comerciais que possuem conexão permanente à Internet e vendem seu acesso a assinantes. Geralmente, os provedores de serviços adquirem ou fazem a locação nas agências reguladoras, faixas de endereços que são concebidos a seus usuários quando conectados à rede. Ao se conectar, um usuário doméstico de internet pode receber um endereço IP distinto.

Segundo Arnett *et al.* (1994, p.60):

> Os endereços TCP/IP apresentam dois componentes: um componente de rede e um componente de host (ou de nó). Os endereços utilizados com o TCP/IP são compostos por quatro bytes (32 bits) e denominados simplesmente endereços IP (e não endereços TCP/IP). Esses endereços são gravados em uma notação de pontos padrão, ou seja, cada byte é gravado como um número decimal separado por pontos (o caractere de ponto final).

No caso do *internet protocol* versão quatro (IPv4), mais utilizado nas redes de comunicação, é formado por quatro partes conhecido como "octetos", variando de 0 a 255, por exemplo: 203.100.100.11. É interessante destacar que o número IP não identifica obrigatoriamente um dispositivo, mas identifica uma conexão. Isso é possível através dos equipamentos conhecidos como *gateways* conectados a várias redes que dispondo em mais um endereço IP.

O (DNS) *Domain Name System*, cuja tradução significa "sistema de nomes de domínios", é um sistema hierárquico utilizado inicialmente em 1984. Sustentado em uma base de dados distribuída hierarquicamente, os dispositivos efetuam consultas para localizar o endereço IP dos computadores (*hosts*) ao qual precisam se conectar (COMER, 2007).

Assim, para acessar os conteúdos da web é necessário conhecer um número IP correspondente. Para uma melhor memorização, foi implementado um sistema de nomes – DNS – possibilitando traduzir um endereço, como exemplo "www2.planalto.gov.br", nos leva até a página desejada – nesse caso, a do Planalto.

A *Uniform Resource Locator ou localizador* (URL) é um padrão de recursos que encaminha a um único local a critério e escolha do usuário, permitindo assim que as informações necessárias estejam disponíveis a qualquer momento.

A utilização da grande rede trouxe novas vulnerabilidades. Além das difíceis tarefas e preocupações com espionagem, fraudes, erros e acidentes, agora os

órgãos têm a necessidade de se preocupar com os ataques, invasões, vírus e outras ameaças.

2.2 Protocolos de comunicação e Serviços de Rede

Embora sejam conceitos distintos, é importante estabelecer uma relação entre os protocolos e serviços de rede. Enquanto o serviço corresponde a um conjunto de operações que uma camada oferece à camada superior, por outro lado, os protocolos definem um conjunto de regras que permitem especificar a realização de um serviço.

Considerado a parte mais importante nas novas concepções de redes de computadores, os protocolos consistem num conjunto de regras que estabelecerão como se dará a comunicação entre dois ou mais dispositivos. Em outras palavras, esta é a “língua” dos computadores, uma espécie de idioma com padrões e normas de comunicação determinados, como descrito por Arnett et all (1994, p.55):

> [...]. esse significado é fornecido pela especificação do protocolo. Um protocolo é um conjunto de regras que define o formato dos pacotes e a semantida de ultilização desses pacotes.

Os protocolos surgiram pela necessidade de conectar equipamentos de fornecedores, máquinas e sistemas distintos do mundo inteiro, sem a necessidade de escrever uma linguagem para cada equipamento diferente. Os protocolos mais utilizados são: IP, DHCP, TCP, HTTP, FTP, TELNET, SSH, POP3, SMTP, IMAP.

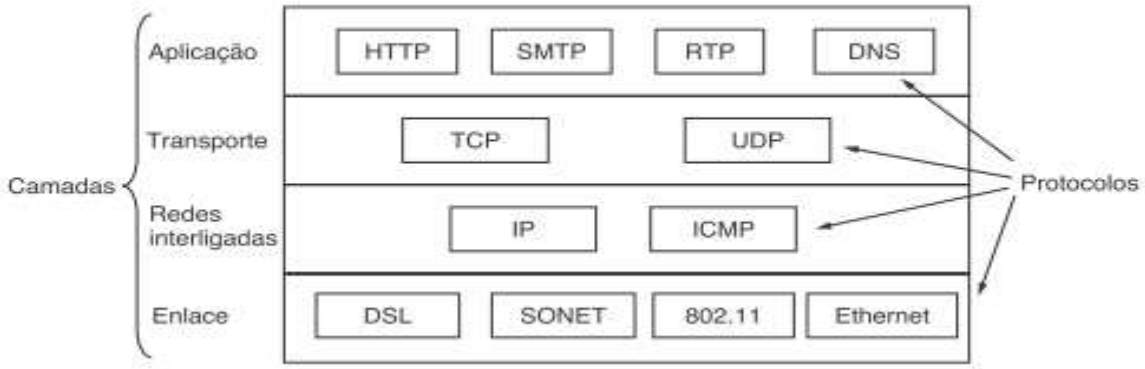
Os protocolos possuem diversas funções, sendo uma delas colher os dados transmitidos pela rede, separá-los em pequenos pedaços chamados de pacotes. É através deles que se estabelecem a fase de criação, controle, circulação e encerramento.

Um serviço de rede pode ser definido como um conjunto de serviços oferecidos pela rede através de uma interface e cedido logo após a camada imediatamente superior, como explica Tanenbaum (2003, p. 29):

> Acima de camada de transporte, encontramos a camada de aplicação. Ela contém todos os protocolos de nível mais alto. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). Muitos outros protocolos foram incluídos no decorrer dos anos (...) incluem o DNS (Domain Name Service), que mapeia os nomes de hosts para seus respectivos endereços da camada de rede (Internet), o HTTP, protocolo usado para buscar páginas na World Wide Web, e o RTP, protocolo para entregar mídia em tempo real, como voz ou vídeo.

Desse modo, nota-se que cada protocolo possui uma função na rede, a fim de que as conexões ocorram de modo efetivo. Eles são essenciais para que a informação contida na internet seja solicitada e recebida. A seguir, temos uma imagem que mostra o conjunto de protocolos na camada de aplicação, transporte e de enlace:

Figura 1 – Conjunto de protocolos



Fonte: Tanenbaum (2003)

Cada serviço de rede é desfrutado por aplicações distintas, permitindo que uma aplicação use vários serviços, como exemplo o Mozilla Firefox, navegador distribuído em várias plataformas ao qual utiliza o *Hypertext Transfer Protocol* (HTTP) e o DNS.

Os serviços se classificam como sendo orientados a conexão e serviço sem conexão. Tanenbaum (2003, p. 22) relatam que:

> O serviço orientado a conexões se baseia no sistema telefônico. Para falar com alguém, você tira o fone do gancho, digita o número, fala e, em seguida, desliga. Da mesma forma, para utilizar um serviço de rede orientado a conexões, primeiro o usuário do serviço estabelece uma conexão, a utiliza, e depois a libera. O aspecto essencial de uma conexão é que ela funciona como um tubo: o transmissor empurra objetos (bits) em uma extremidade, e esses objetos são recebidos pelo receptor na outra extremidade. Na maioria dos casos, a ordem é preservada, de forma que os bits chegam na sequência em que foram enviados.

A família *Transmission Control Protocol* (TCP) é orientada à conexão na medida em que os serviços relacionados ao protocolo são ao contrário, não disponibilizando de orientação à conexão.

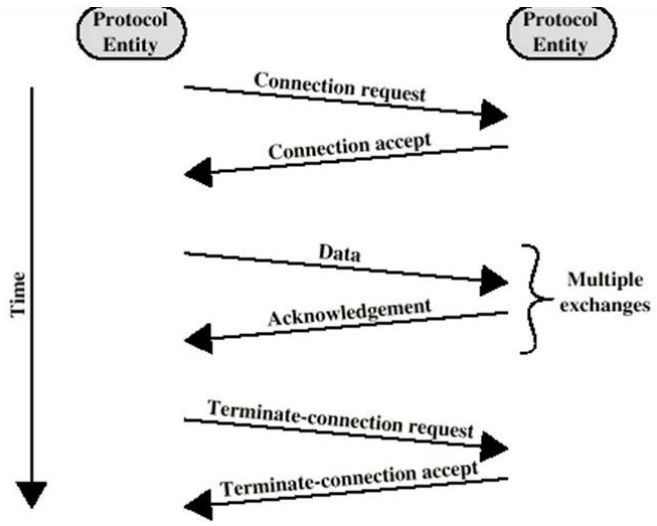
O TCP faz referência ao envio de pacotes mais comum da internet. Numa conexão básica com um site, seu *host* manda informações ao servidor solicitando

que envie os conteúdos da página para máquina do usuário. As informações que foram enviadas são traduzidas pelo navegador para mostrar aquilo que se deseja.

O TCP é considerado um dos principais protocolos de comunicação. Possui a capacidade de gerenciar todas as informações vindas da camada inferior, ou seja, da camada IP. Seu objetivo é permitir que duas máquinas conversem, além de realizar o controle das transmissões.

Esse protocolo funciona também como um organizador dos *datagramas* provenientes do protocolo IP, evitando a saturação da rede. Este divide em segmentos de comprimentos para entregá-los ao protocolo IP, executa a circulação correta das informações e permite o início e o fim de uma comunicação. Graças a esse protocolo o aplicativo pode comunicar-se com segurança. A imagem a seguir relaciona o envio do pacote TCP:

Figura 2 – Conexão TCP



Fonte: Kurose e Ross (2010)

O *User Datagram Protocol* (UDP) é um protocolo não orientado à conexão, como Kurose e Ross (2010, p.22) pontuam:

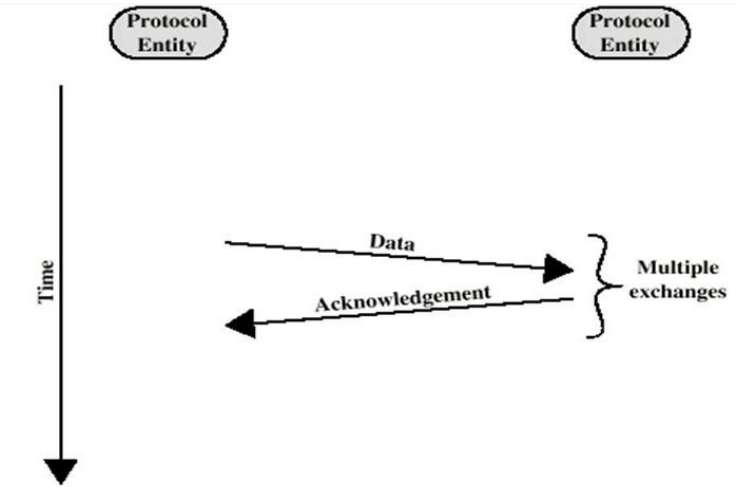
> Ao contrário do serviço orientado a conexões, o serviço não orientado a conexões se baseia no sistema postal. Cada mensagem (carta) carrega o endereço de destino completo e cada uma delas é roteada pelos nós intermediários através do sistema, independentemente de todas as outras. Existem diferentes nomes para mensagens em diferentes contextos; um pacote é uma mensagem na camada de rede. Quando os nós intermediários recebem uma mensagem completa antes de enviá-la para o próximo nó, isso é chamado comutação store-and-forward. A alternativa, em que a transmissão de uma mensagem em um nó começa antes de ser completamente recebida por ele, é chamada comutação cut-through. Normalmente, quando duas mensagens são enviadas ao mesmo destino, a

> primeira a ser enviada é a primeira a chegar. No entanto, é possível que a primeira mensagem a ser enviada esteja atrasada, de modo que a segunda chegue primeiro.

O UDP é baseado no envio de pacotes de informações. Porém, não consta nele a parte de verificação de erros. Seu objetivo é tornar o processo de envio de informações mais rápido, uma vez que as etapas de comunicação e sua verificação de integridade colaboram para tornar mais devagar.

Quando acionado, esse protocolo envia informações ao seu destinatário sem a devida preocupação se a mensagem chegou, ou se foi recebida de maneira íntegra. Caso conste erros, ocorre o envio do próximo pacote. Apesar de que tal método pode potencializar a ocorrência de erros, ele permite uma comunicação mais rápida na rede. A imagem a seguir demonstra a o envio do pacote UDP:

Figura 3 – Conexão UDP



Fonte: Kurose e Ross (2010)

2.3 Principais topologias

Considerado o canal pelo qual os computadores na rede estão conectados, as estruturas topológicas possuem a função de conectar os nós de uma rede. São classificadas de maneira geral como físicas ou lógicas.

A topologia física é basicamente o *layout* da rede, assim como diria Arnett (1994): “Uma topologia física é o modo real como uma fiação é encadeada entre os nós de rede” (ARNETT, , *et al.*, 1994, p. 26). Assim, a parte onde passam os cabos, roteadores, nós, placas de rede e outros equipamentos de uma rede utilizados para a transmissão de dados fazem parte de sua topologia física.

Já a topologia lógica determina o modo de funcionamento de uma placa de rede para um tipo de rede ou a maneira como os dados serão transmitidos de um dispositivo para o outro sem possuir de fato uma ligação física. Podem ainda ser reconfiguradas através de tipos diferentes de equipamentos, como os roteadores e switches.

2.3.1 Ponto a ponto

O *Peer-to-peer* (P2P), ou “ponto-a-ponto”, segundo sua tradução, é uma topologia das redes de computadores responsáveis por ligar dois pontos sem a necessidade de equipamentos de serviço central. Seu funcionamento parte do princípio de permitir o compartilhamento de dados ou serviços. Podem ser usadas para compartilhar músicas, vídeos ou outros formatos digitais. Segundo Mazzola (2000, p. 8):

> Nos canais em ponto-a-ponto, a rede é composta de diversas linhas de comunicação, cada linha sendo associada à conexão de um par de estações.

Esses pontos de ligações possibilitam a troca e distribuição de informações de forma rápida e eficiente, contribuindo para a velocidade da transmissão dos mais diversos formatos de conteúdos que a internet permite compartilhar.

2.3.2 Estrela

Na topologia tipo estrela, as informações passam por um equipamento central inteligente que faz uma conexão com cada estação da rede e consequente distribuição de trafego interno e externo. É nesse aspecto que os diferencia da topologia em barramento.

Arnett (1994, p.28) relata que:

> Em uma topologia de cabeamento de estrela, um sistema central, que pode ser um servidor ou um hub de fiação, estabelece uma conexão com os PCs ou com as estações de trabalho. Cada nó está conectado com o sistema central por um cabo individual. Como cada computador em uma rede necessita de seu próprio fio para se conectar com o hub da rede, geralmente a topologia em estrela.

Esse ponto central gerencia o fluxo de dados da rede. Todas as informações trafegam pela rede de equipamento para equipamento através de um nó, ou seja, quando um *host* tenta enviar um arquivo pela rede, ele primeiro precisa passar pelo equipamento central até chegar a outro dispositivo conectado a ela.

Esse tipo de rede é a mais comum e utiliza um conjunto de par traçado e concentradores como ponto central da rede. Dentre as vantagens dessa topologia, a mais importante é a autonomia entre os nós. A quebra de um cabo afeta somente o equipamento conectado com ela. Porém, sua maior desvantagem é a exigência de uma grande quantidade de cabos e componentes centrais, aumentando o custo total de instalação.

2.4 Redes locais e redes de longa distância

A *Local Area Network* (LAN), conhecida normalmente como rede local é o tipo de rede privada mais utilizada e a mais comum. Seu objetivo é interligar diversos computadores e outros dispositivos como telefones e aparelhos em fax de maneira local. Sua velocidade é normalmente reduzida em comparação às outras redes MAN *Metropolitan Area Network* – Rede de Área Metropolitana, e WAN W*ide Area Network* – Rede de Longa Distância.

De acordo com Tenenbaum (2003, p.18):

> [...] muitas vezes chamadas LANs, são redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais [...].

Diferente da rede LAN, as redes metropolitanas MAN são de grandes dimensões e conectam os dispositivos dentro de uma mesma cidade em algumas dezenas de quilômetros. Os exemplos mais conhecidos são as redes de televisão a cabo, que estão disponíveis na maioria dos locais no mundo. Foi a partir do antigo sistema comunitário de antenas que surgiu esse tipo de rede. Tenenbaum (2003, p.19) ainda relata que:

> Esse sistema cresceu a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca percepção do sinal d televisão pelo ar. Nesses primeiros sistemas, uma grande antena era colocada no alto de colina próxima e o sinal era então conduzido até a casa dos assinantes.

Com a internet atraindo usuários em massa, as operadoras de TV a cabo perceberam que poderiam usar um espectro pelos cabos. A partir de então, estas puderam mandar sinais de internet e vender um serviço que estava em crescente desenvolvimento. Sobre isso, Tenenbaum (2003, p. 20) pontua:

> Nesse momento, o sistema de TV a cabo começou a se transformar, passando de uma forma de distribuição de televisão para uma rede metropolitana.

As WANs conectam redes locais, metropolitanas e regionais em distâncias que podem ser até intercontinentais. Para que a implementação desse tipo de rede seja viável, são usados diversos tipos de tecnologias a fim de viabilizar a troca de dados em alta velocidade mesmo em locais de difícil acesso, como explicado por Mazzola (2000, p.1.2) “a rede utilizada permitiria conectar computadores localizados em diferentes prédios numa mesma cidade ou mesmo em cidades distantes de uma dada região. Esta caracteriza uma Rede de longa distância ou Rede geograficamente distribuida.

2.5 A internet

A internet se constitui como um grande sistema de comunicação que interliga diversas redes de computadores de inúmeras formas, por meio de protocolos e requisitos de segurança. Arnett *et al.* (1994) diz que:

> A internet tem suas raizes em uma iniciativa de interligação em rede e protocolos associados criados pelo Departamento de Defesa dos Estados Unidos.

Corroborando com esta afirmativa, Comer (2007) relata que, assim como outras ferramentas utilizadas pelas forças armadas, a internet também teve forte impulso militar. No transcorrer do período pós-guerra o mundo passava por um grande medo em relação a prováveis ataques nucleares. As pesquisas da época buscavam aperfeiçoar uma corrente de comunicações onde não existisse um ponto principal que, ao ser destruído, colocaria em colapso todo o sistema de comunicações.

Por volta de 1962, os americanos criaram a Cadeia de Comunicação Distribuída (CCD), na qual era composta por inúmeros computadores interligados por diversas linhas telefônicas. A partir de tal estrutura, pretendia-se dividir a quantidade de dados a ser transportado entre os *hosts* em pequenos “pacotes”, enviando-os por meio das diferentes linhas telefônicas até um computador de destino. Neste modelo, as falhas de um dos pacotes no percurso possibilitam que o sistema utilize um caminho equivalente, ou seja, não há um ponto único de falha. Isso implica afirmar que uma possível parada em alguma linha de transmissão não suspende completamente o sistema (COMER, 2007).

A ARPANET foi primeira rede de computadores sendo considerada a ancestral direta da internet. Produzida pela Agência de Projetos e Pesquisas Avançadas – *Advanced Research Projects Agency* (ARPA) do Departamento de Defesa dos EUA, aproximadamente em 1966 ela estava situada em 17 locais diferentes nos quais computadores conectados às linhas telefônicas conseguiam estabelecer e trocar informações. Inicialmente, sua função era exclusivamente militar (KUROSE e ROSS, 2010).

De acordo com Stout (1997, p.05)

> Depois de um certo tempo, o governo desistiu da ideia de que sua rede era útil apenas para projetos relacionados à defesa, e ela se tornou conhecida como Arpanet. Nesse tempo, o governo também começou a conectar muitas universidades do país à rede [...].

Passados alguns anos, diversas agências subordinadas ao governo e universidades do Departamento de Defesa dos EUA começaram a restringir o uso da ARPANET apenas para a finalidade de pesquisa. Naquela ocasião, algumas universidades e empresas importantes começaram a criar soluções para interligar suas redes de computadores.

Arnett *et al.* (1994, p.404) explica que:

> Diferente de uma peça de software comercial que é projetada de cima para baixo para realizar coisas específicas de formas específicas, a Internet é adaptada às necessidades dos usuários pelos próprios usuários.

A internet hoje é resultado de constantes aprimoramentos e melhorias tecnológicas inspiradas inicialmente nas ideias e utilização da ARPANET. Nesse contexto, destaca-se o desenvolvimento do protocolo de rede (TCP/IP) aplicada pela ARPANET em 1982 e que, mais tarde, foi pouco a pouco liberado para utilização civil, sendo hoje uma das melhores alternativas para comunicação entre computadores. Com a aplicação de um protocolo único, a conexão com outros dispositivos de diferentes fabricantes aumentou ainda mais. Isso fez com que sua utilização fosse gradativamente fortalecida.

Quando nos referimos a internet, estamos nos reportando à grande rede de dispositivos conectados utilizando um conjunto próprio de protocolos. Assim, para Tenenbaum (2011, p.11):

> A Internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns.

Podemos entender a internet então como uma vasta rede de diversas outras redes de grande infraestrutura. Antes dela se tornar como é conhecida hoje, houve um grande trajeto na evolução dos computadores e das tecnologias de telecomunicações.

Não existe dono, nem existe entidade responsável pela internet, o que possibilita conceituá-la como uma rede de computadores de acesso público e ilimitado que usa a infraestrutura de telecomunicações. Apesar de não existir um dono, alguns consórcios internacionais como o *World Wide Web Consortium* (W3C) pretendem agregar empresas filiadas na tentativa de desenvolver padrões para a internet.

3 SEGURANÇA DE REDES

Nesse capítulo abordaremos a segurança no correio eletrônico, segurança em LANs sem fio e segurança nos *firewalls*.

3.1 Segurança de correio eletrônico

A Internet se baseia em um conjunto de protocolos TCP/IP. Através do protocolo *Simple Mail Transfer Protocol* (SMTP) – protocolo de transferência de correio simples em que ocorre a transferência entre máquinas distintas. Kurose e Ross (2010, p.87) em seu livro relatam que:

> Tal qual como o correio normal, o e-mail é um meio de comunicação assíncrono – as pessoas enviam e recebem mensagens quando for conveniente para elas, sem ter de estar coordenadas com o horário das outras pessoas. Ao do correio normal, que anda a passos lentos, o correio eletronico é rápido, fácil de distribuir e barato. O correio eletrônico moderno tem muitas características poderosas.

Conhecido popularmente como e-mail, o correio eletrônico é uma aplicação de comunicação que permite o envio de mensagens escritas pela Internet independentemente da localização do destinatário.

Para melhor entendimento podemos comparar ao sistema de correios tradicional, onde as correspondências enviadas por um remetente a um destinatário tão somente serão lidas se nos dirigirmos até a agência de correio e retirarmos o material (considerando a inexistência do carteiro).

Através desse serviço, uma aplicação oferece ao cliente alguns campos para preenchimento (destinatários, assunto, texto da mensagem e outros campos) permitindo que, desse modo, uma mensagem seja criada. Após a submissão, o servidor se encarrega de encaminhar os dados às caixas de correio de todos os destinatários. Os elementos enviados são gravados em outros serviços de armazenamento de mensagens.

O usuário que deseja checar se há novas mensagens realiza uma requisição por meio de seu cliente de e-mail, o qual consulta, no respectivo servidor, a existência ou não de mensagens. Se existirem, as mesmas são apresentadas ao destinatário na forma como foram concebidas.

A respeito da importância do e-mail como ferramenta de trabalho, Tanenbaum (2003, p.3) desenvolve:

> Uma rede de computadores pode oferecer um poderoso meio de comunicação entre os funcionários. Praticamente toda empresa com dois ou mais computadores tem o recurso de e-mail (correio eletrônico), que os funcionários utilizam de forma geral para suprir uma grande parte da comunicação diária.

No entanto, por ser uma ferramenta de comunicação e estar ligada diretamente à Internet, o correio eletrônico é suscetível a riscos. Sobre isso, Cert.br (2012, p.9) expõe:

> Você recebe um e-mail, em nome de um site de comércio eletrônico ou de uma instituição financeira, que tenta induzi-lo a clicar em um link. Ao fazer isto, você é direcionado para uma página Web falsa, semelhante ao site que você realmente deseja acessar, onde são solicitados os seus dados pessoais e financeiros.

Uma das formas mais comum que essas tentativas se mostram é pelo alastramento ou propagação de vírus através de mensagens solicitadas de correios denominadas *Sending and Posting Advertisement in Mass* (SPAM), contendo um *malware* em anexo ou links que, caso sejam abertos, originam situações como:

1) Propagação nos correios eletrônicos com a infecção em cadeia;
2) Ataques em massa por *SPAM* por sistemas infectados e, quando comprometidos, são usados como disseminadores para outros computadores em rede interna ou externa.

Alguns e-mails apresentam um remetente que tenta ser credível e convidam o usuário a clicar em links contaminados ou a revelar informações pessoais ou privadas.

3.2 Segurança em LANs sem fio

As redes sem fio são conhecidas como rede *wireless.* Elas surgiram pela necessidade de mobilidade e independência de localização dos seus usuários, no qual traz como possibilidade a computação onipresente, onde o usuário pode fazer acessos de qualquer lugar, a qualquer tempo.

Segundo Laudon e Laudon (2011) essas redes são suscetíveis a ataques. Embora seu alcance seja curto, podem ser invadidas através de dispositivos móveis por pessoas que circundam a área. Redes sem proteção garantem ao invasor uma série de brechas como, por exemplo, o monitoramento de tráfego com interceptação dos dados.

A grande característica dessa tecnologia é a ampla mobilidade que fornecem a seus usuários, além da facilidade de instalação e utilização em locais fechados ou não, sendo a sua simplicidade útil tanto para empresas quanto para uso doméstico. Apesar de ser uma tecnologia que ajuda e facilita a mobilidade dos usuários, há – como em todas as redes de comunicações – alguns problemas em sua segurança que levam à busca das precações no mundo da tecnologia.

Essas redes fazem transmissão através de sinal de rádio e, consequentemente, qualquer pessoa com no mínimo um equipamento pode interceptar as informações que são transmitidas. Diversos roteadores dispõem opções de utilizar a segurança *Wi-Fi Protected Access* (WPA2) com *Temporal Key Integrity Protocol 2* (TKIP) (WPA2-TKIP), *Advanced Encryption Standard* (AES) (WPA2-AES) ou os dois simultaneamente. Escolher a opção errada pode acarretar em problemas. Essa configuração é de suma importância e necessita ser escolhida com cuidado, observando as tecnologias envolvidas e conhecimento na área.

Os principais algoritmos na segurança são: *Wired Equivalent Privacy*, (WEP), WPA e II WPA2. Kurose e Ross (2010, p.532) relatam que “a WEP tem como propósito fornecer um nível de segurança semelhante ao que é encontrado nas redes cabeadas”. Contudo, não é isso que se observa na realidade, pois este é mais antigo e vulnerável, visto que diversas falhas em segurança foram descobertas. A tecnologia seguinte a WAP melhorou esse aspecto, mas já foi considerada vulnerável a intrusos. A WPA2 é considerada atualmente a mais segura.

As criptografias TKIP e o AES (Advanced Encryption Standard) são usados em redes com protocolo WPA2. O TKIP é mais antigo e suscetível a ataques. Atualmente esse padrão não é mais seguro e encontra-se ultrapassado. Porém, o AES é um protocolo mais seguro, tendo como ponto fraco o ataque de força bruta.

Se dentro da instituição existir dispositivos mais antigos, eles não podem se conectar a uma rede WPA2-PSK (AES), e sim poderá se ligar ao WPA2 com a antiga criptografia TKIP. Não é seguro, mas é uma solução para equipamentos defasados.

3.3 *Firewalls*

Para a definição do que é um firewall, trouxemos aqui dois conceitos de autores distintos que conceituam o termo.

Segundo Tanenbaum (2003, p.513):

> O firewall atua como um filtro de pacotes. Ele inspeciona todo e qualquer pacote que entra e que sai. Os pacotes que atenderem a algum critério descrito nas regras formuladas pelo administrador da rede serão remetidos normalmente, mas os que falharem no teste serão descartados sem cerimônia.

Já Kurose e Ross (2010, p.535) estabelecem que:

> um firewall é uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros.

Os dois autores esclarecem que o firewall é uma ferramenta de segurança que controla o tráfego de uma rede. Ela é usada como uma proteção entre a Internet não segura e a rede interna, Intranet e outras redes consideradas de segurança. Através dele é possível implementar uma política que controla o acesso entre as redes. O *firewall* confere as credenciais de cada usuário antes que ele possa acessar a rede. Ele identifica tudo o que o programador deseja na rede, como nomes, endereços IP, aplicativos ou outras características.

Tanenbaum (2003, p.513) afirma que:

> O critério de filtragem normalmente é dado como regras ou em tabelas que listam as origens e os destinos aceitáveis, as origens ou destinos bloqueados e as regras padrão que orientam o que deve ser feito com os pacotes recebidos de outras máquinas ou destinados a elas. No caso comum de uma configuração TCP/IP, uma origem ou destino consiste em uma porta e um endereço IP.

Todo o tráfego que entra e sai na rede passa por um roteador, onde acontece a filtragem de pacotes. É realizado um filtro em cada datagrama e é estabelecido se os dados passam ou ficam bloqueados.

Em seguida, é feita a comparação das informações com as regras de acesso estabelecidas no sistema pelo usuário administrador da rede. Assim, evita-se que conexões não autorizadas trafeguem na rede, possibilitando que a instituição determine as regras de segurança ao tráfego entre sua rede interna e a Internet.

A configuração fica estabelecida de acordo com as regras de organização como explica Kurose e Ross (2010, p.537):

> Um administrador da rede configura o firewall com base na política da organização. A política pode considerar a produtividade do usuário e o uso da largura de banda, bem como as preocupações com a segurança da organização.

Em ambientes que os recursos privados são compartilhados, o administrador precisa garantir que todo o tráfego da rede entre dispositivos seja seguro, evitando perdas tanto feitas por intervenção humana como por ameaças cibernéticas.

4 O CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

O conhecimento em segurança é de suma importância. Porém, é preciso salientar que na área de segurança não existe uma instituição com risco zero, assim como explica Campos (2007, p. 29):

> Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir essa segurança. Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados.

Na utilização da Internet, as estações de trabalho são demasiadamente desprotegidas dos perigos virtuais. Durante suas atividades diárias são armazenadas senhas pessoais, informações dos usuários e da Polícia Militar e, na maioria das vezes, sem a devida proteção ou controle de acesso. Esses locais estão sujeitos a execução de programas desconhecidos, permitindo que fiquem expostos a grampos de teclado ou outras tecnologias que possibilitam ter acesso não autorizado.

4.1 *Hacker x Cracker*

No mundo cibernético, inúmeras expressões podem denominar e classificar os piratas cibernéticos. Tais piratas são apaixonados pela informática, conhecem sobre segurança e ferramentas próprias para suspensão de sistemas e outras características específicas. Contudo, existem algumas semelhanças no nível de conhecimento e objetivos que os impulsionam à pirataria, se diferindo apenas nas suas diversas terminologias.

Principais livros como Anonymous (1998), Gomes (2000), Oliveira (2000) e Vasconcelos (1999) revelam alguns termos:

a) *Lammer:* Busca informações de como se tornar um *hacker*;

b) *Script Kiddie*: Usuário comum com poucos conhecimentos em tecnologia que invade sistemas utilizando ferramentas prontas disponíveis na internet;

c) *Wannabe*: realiza combinações de algumas técnicas de ataques atingindo sistemas frágeis;

d) *Hacker*. Detém demasiado conhecimento em informática, principalmente em programação e sistemas operacionais como *Unix* e *Linux*. Possui ainda vasto conhecimento das falhas de segurança e busca novos desafios;

e) *Cracker*: são usuários avançados com o mesmo conhecimento dos hackers, porém têm intenções criminosas. Suas ações rompem com a segurança de um sistema na busca de informações confidenciais a fim de obter vantagens pessoais;

f) *Guru*: considerado um hacker mais avançado. Trabalha em escala máxima de um "super usuário" com habilidades técnicas em todos os segmentos.

O termo hacker assombra a maioria das pessoas sem informação que julgam como sendo aquele indivíduo que destrói computadores, sistemas, arquivos tomando o controle da máquina. Esse conceito foi criado pela publicidade gerada por filmes como "Jogo de guerra" e "Hacker". A partir desses filmes criou-se uma confusão e inversão de conceitos. Tanto os *crackers* como os hackers possuem conhecimentos em sistemas, redes e outros ramos da tecnologia, mas possuem filosofias antagônicas.

Os *crackers* usam suas habilidades para benefícios pessoais, sem se preocupar com os prejuízos causados por suas ações, sendo considerados como usuários perigosos. Gomes (2000), afirma que seu alvo preferido são as redes de pequeno/médio porte. No entanto, existem *crackers* que realizam ataques e espionagem em empresas de grande porte, inclusive em instituições públicas (FRANCO, 1999). Os *hackers* são os verdadeiramente estudiosos, com conhecimento profundo em *hardware*, linguagens de programação, em sistemas diversos, redes e em protocolos.

Os *hackers* não podem ser apontados como criminosos, uma vez que exercem um papel sem infringir a lei, descobrindo algumas falhas de segurança nos diversos desenvolvimentos de *software,* sugerindo assim algumas técnicas de reparo e sendo responsáveis também pelo desenvolvimento do chamado *software* livre.

Raymond (1999) relata que o termo hacker é datado de 1961 quando o comitê de *Signails and Power do Tech Model Railroad Club* adotou sua primeira máquina PDP-1 produzindo ferramentas de programação juntamente com algumas gírias em torno do assunto. Naquela ocasião, hacker era usado por estudantes para conceituar os que "fuçavam" computadores além dos limites.

Richard Stallman, um dos fundadores da *Free Software Foundation* (FSF), foi um exemplo explícito de hacker ao qual remontam de décadas atrás, desde os primeiros experimentos na ARPANET. Stallman se integrou o Instituto de Tecnologia de Massachusetss (MIT), juntamente com outros colaboradores, criando vários

programas de códigos abertos liderados por ele e que até hoje constituem o projeto *Gnu is Not Unix* (GNU) por desenvolvedores (RAYMOND, 1999).

4.2 Princípios da segurança da informação

Para a discussão conceitual sobre segurança da informação, Beal (2005) SI postula que esta é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. Já para Sêmola (2003), SI compreende ser uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

De acordo com a norma NBR[2] ISO 27002, na parte introdutória é estabelecido que a segurança da informação é “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. A mesma norma discorre ainda que a segurança da informação está diretamente relacionada com a preservação da confidencialidade, da integridade e da disponibilidade da informação. Para Campos (2007, p.17) “um sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade.” Em segurança da informação é necessário transcorrer sobre esses pilares, visto que toda e qualquer ação que afete um destes será considerado um atentado contra a segurança.

Desta forma, SI é a área do conhecimento com o objetivo de proteger a informação das ameaças à integridade, disponibilidade e confidencialidade, garantindo assim a continuidade do negócio. A informação é um bem precioso, devendo ser cuidada mediante regras e procedimentos das políticas de segurança.

A confidencialidade remete a garantia de que uma informação será acessada ou disponibilizada somente por pessoas autorizadas (NBR ISO/IEC 27002, 2005). Ocorre a quebra da confidencialidade ao se conceder que usuários não autorizados tenham acesso ao conteúdo. Deixar de ser confidencial é perder o segredo da informação. No entanto, a garantia de confidencialidade é assegurar que a informação está segura, evitando assim a disseminação indevida.

[2] A Associação Brasileira de Normas Técnicas.

Quebra da disponibilidade é quando a informação não está mais acessível, ou seja, disponível para seus usuários, deixando de ser acessada no momento de necessidade (NBR ISO/IEC 27002, 2005). Assim, garantir a disponibilidade é assegurar o êxito no acesso ao conteúdo da informação, possibilitando a leitura e o armazenamento dela.

Já a integridade é quando a informação não pode ser modificada, viabilizando assim a não alteração ou destruição sem autorização, permitindo que os dados sejam conservados em sua legitimidade e consistência (NBR ISO/IEC 27002, 2005). Ocorre quebra da integridade quando existe a falsificação. Garantir a integridade é permitir que a condição da informação original permanecesse íntegra.

A autenticidade garante que as informações sejam de uma fonte confiável (NBR ISO/IEC 27002, 2005). A confiabilidade garante que as informações são seguras e oriundas de fontes confiáveis. A autenticidade é a idoneidade da fonte, ou seja, quando esta é digna e de confiança. O não repudio garante a não negação da autoria em transações realizadas anteriormente.

4.3 A informação e seu ciclo de vida

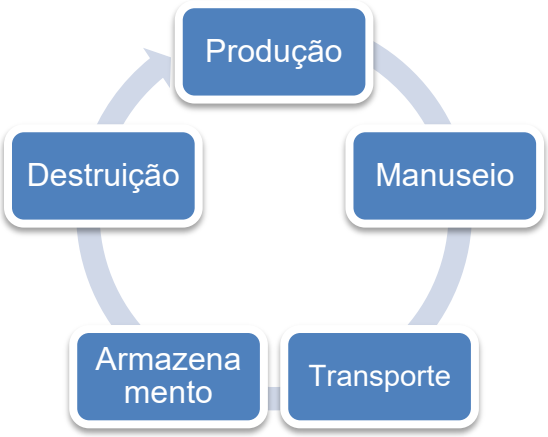
Na sociedade da informação, o principal patrimônio da empresa são seus dados, registros e conhecimentos. Contudo, tais elementos estão sob constante risco (Dias, 2000).

Ramos (2008, p.287) conceitua a informação como:

> [...] todo patrimônio que se refere à cultura da empresa ou ao seu negócio, podendo tais informações ser de caráter comercial, técnico, financeiro, legal, de recursos humanos, ou de qualquer natureza, que tenha valor para a organização e que se encontrem armazenadas em recursos computacionais da empresa, com trafego dentro da sua infra-estrutura tecnológica.

Para um melhor entendimento sobre o objeto da segurança é interessante conhecer os ciclos de vida da informação, que pressupõem uma sequência lógica feita por agentes, porém com funções específicas e de grande importância. A informação compreende um ciclo de vida. A partir da sua produção, tem o seu tempo de vida, na qual é utilizada por diversos agentes, transportada, armazenada, e por fim destruída. É basicamente assim que funciona o ciclo de sua existência. A figura a seguir mostra o ciclo de vida da informação:

Figura 4 - Ciclo de vida da informação



Fonte: próprio autor.

Inicialmente, há a fase de produção da informação. O manuseio é a parte pela qual a informação é examinada pelos usuários, obtendo a materialização do conhecimento. Já a fase de transporte é responsável pela condução dos dados. O armazenamento é a ação responsável por arquivar os conteúdos. Por fim, o descarte ou a destruição é o ato de tornar a informação inutilizável, jogando fora aquilo que não está mais sendo usado.

4.4 Mecanismos de segurança

Nesta parte do trabalho serão apresentados alguns mecanismos de segurança, tais como: normas e políticas de segurança, criptografia, assinaturas e certificados digitais, ferramentas *antimalware* e os filtros *antispam*.

4.4.1 Normas e políticas de segurança

Com o aumento de ocorrências e seu grande impacto nos investimentos em SI, as instituições buscam uma boa estruturação a fim de garantir que suas atividades estejam protegidas conta diversos tipos de ameaças virtuais.

Em meios a esse problema, nasceram as normas internacionais NBR ISO/IEC 27001[3] e NBR ISO/IEC 27002[4], que estabelecem um padrão para sistemas de gestão e concentra boas práticas à gestão da segurança da informação

[3] ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001 - Tecnologia da informação – Técnicas de Segurança. Sistemas de gestão de segurança da informação**.Rio de Janeiro. 2006.
[4] ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2005.

respectivamente, sendo fundamentais para a consolidação de um Sistema de Gestão de Segurança da Informação (SGSI).

No ano de 1995, as organizações internacionais *The International Organization for Standardization* (ISO) e *International Electrotechnical Commission* (IEC) formaram o embrião que alicerçaram as regras relacionadas ao SI. Em outubro de 2005 a ISO 27001 foi publicada, substituindo a norma BS 7799 e servindo de certificação para o sistema de gestão de segurança da informação.

A ISO/IEC 27002 estabelece melhores práticas para a implementação do SGSI por meio de um guia de implantação. Ao contrário do que diversos especialistas pensam, a ISO pode apoiar a inserção do SGSI em qualquer tipo de organização pública ou privada, grande ou pequena e não somente para empresas caracterizadas em tecnologia.

Seu objetivo é estabelecer instruções e princípios para iniciar, implementar, conservar e proporcionar melhoras na gestão do SI dentro de uma organização, incluindo também a gestão de controles, considerando os riscos encontrados nas organizações.

Tais medidas podem trazer diversos benefícios, proporcionados pela certificação ISO 27002, especialmente pelo fato de possuir um reconhecimento mundial. Além disso, é possível a partir disso proporcionar uma melhora na conscientização em relação à segurança da informação; melhor controle sobre os ativos e informações consideradas sigilosas ou sensíveis para a instituição; identificação e correção de pontos considerados fracos; redução de riscos referentes a não implementação de um SGSI por meio de políticas e procedimentos estabelecidos; e redução de custos com a prevenção em incidentes de segurança.

A norma ISO 27002 é distribuída em seções, e sua parte principal começa a partir da seção 5 da seguinte maneira:

Na Seção 5 a norma inicia com a Política se Segurança da Informação – a criação de um documento no qual deve possuir conceitos de segurança da informação, estabelecer seus objetivos e como serão feitos os controles, o compromisso da gestão com a política e outras normas gerais (NBR ISO/IEC 27002, 2005).

Já na seção 6 se estabelece a “Organização da Segurança da Informação”, que cuida de fazer a implementação do SI em uma organização estabelecendo também uma estrutura para organizar e gerenciar. Assim, suas atividades devem ser

coordenadas por integrantes da organização, além da responsabilidade já definida e a proteção das informações consideradas sigilosas (NBR ISO/IEC 27002, 2005).

A seção 7 refere-se a “Gestão de Ativos”, considerada uma das mais importantes para a organização, já que um ativo, segundo a norma, é qualquer coisa que possua valor e que precisa de proteção. Porém, para que isso ocorra, estes precisam ser identificados e classificados (NBR ISO/IEC 27002, 2005).

A seção 8 preocupa-se com a “Segurança em Recursos Humanos”. Essa seção é encarregada de reduzir os riscos de roubo, fraude e mau uso dos recursos da organização. Quando o usuário estiver em suas atividades, deve adquirir ciência das ameaças referente a SI assim como de suas responsabilidades (NBR ISO/IEC 27002, 2005).

A seção 9 é responsável pela “Segurança Física e do Ambiente”, em que os equipamentos que processam informação devem ser colocados em locais seguros juntamente com os níveis de controles apropriados e proteção contra ameaças (NBR ISO/IEC 27002, 2005).

A seção 10 é encarregada de zelar pela “Segurança das Operações e Comunicações”, em que é importante o estabelecimento de procedimentos e responsabilidades pela operação nos recursos de processamento. Inclui também o planejamento de sistemas que minimizam riscos de falhas e realiza procedimentos referentes a cópias de segurança e recuperação e na gestão segura das redes de comunicação (NBR ISO/IEC 27002, 2005).

Na seção 11 se estabelece o “Controle de Acesso” que assegura a permissão de usuários autorizados a adentrar aos sistemas e evitando a entrada não autorizada de intrusos. Com isso, são evitados danos em documentos ou outros recursos que estejam ao alcance de qualquer usuário (NBR ISO/IEC 27002, 2005).

Já a seção 12 refere-se a “Aquisição, Desenvolvimento e Manutenção de Sistemas” em que os sistemas de informação precisam de identificação. Esse procedimento deve ser combinado antes do desenvolvimento de sua implementação, para que a partir daí consigam ser protegidos, mantendo assim a confidencialidade, autenticidade e a integridade (NBR ISO/IEC 27002, 2005).

A seção 13 compreende ser a “Gestão de Incidentes de Segurança da Informação” que através de procedimentos considerados formais devem ser estabelecidos na organização. Os funcionários devem estar conscientes sobre os

procedimentos de notificação de eventos em segurança, a fim de obter a garantia de possíveis erros no menor espaço de tempo possível (NBR ISO/IEC 27002, 2005).

Além das normas de segurança estabelecidas pelas ISO NBR citadas acima, outro tema bastante importante é a política de segurança, considerada a base da proteção da informação, sendo um papel importante dentro das organizações. Seu objetivo é definir normas, procedimentos, responsabilidades e ferramentas para controle e segurança dos ativos.

Segundo Dias apud Laureano (2010, p. 56), a política de segurança da informação é:

> [...] um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos. Pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais.

Assim, a política de segurança é a formalização dos interesses e anseios em relação à proteção. Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. De modo semelhante, não há como ser diferente em uma empresa: é necessário que os padrões de conduta sejam definidos para garantir o sucesso do negócio (ABREU, 2001).

De acordo com essa definição, a política segue como uma legislação que todos devem seguir e cumprir, atendendo a vários propósitos. Para Wadlow (2000, p.40) a política de segurança:

> 1. Descreve o que está sendo protegido e por quê;
> 2. Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo;
> 3. Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;
> 4. Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário;
> 5. Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”;
> 6. Impede que o departamento de segurança tenha um desempenho fútil.

A implementação é a parte mais difícil, pois envolve conhecimentos gerais em segurança, conhecimento da organização, de sua cultura, das pessoas envolvidas, das tecnologias hostilizadas, sendo considerada uma tarefa complexa e demorada. No entanto, a maior dificuldade é a compreensão de que os procedimentos estabelecidos estão sendo seguindo pelos usuários ou não.

4.4.2 Criptografia

Todas as informações passaram a ser transferidas de maneira muito intensa dentro das redes de computadores, configurando uma vulnerabilidade em qualquer parte do mundo. Assim, dados transcorridos entre dois países, por exemplo, podem ser escutados em um terceiro país. De acordo com o site G1[5], o caso do ex-técnico da CIA, Edward Snowden acusado de espionar informações sigilosas de diversos países (inclusive o Brasil) tratava-se de fraude informacional sigilosa armazenada em meios computacionais. A partir daí surge a necessidade de utilizar ferramentas que protegem as informações armazenadas, transmitidas em computadores ou exploradas dentro das redes de comunicação.

Enviar e receber algum tipo de informação de caráter sigiloso é uma necessidade muita antiga na história da humanidade, remontando desde os tempos de Júlio Cesar, em que o homem desejou guardar inúmeros segredos religiosos, pessoais, familiares, militares e governamentais. Ao mesmo tempo em que surgiu a necessidade de manutenção de sigilo de algumas informações, despertou-se também a vontade de os desvendar. Sendo assim, com o transcorrer dos anos surgiu um enfrentamento entre os que guardam segredos e os que buscam revelar.

Pensando na garantia de conservar em segredo as informações, tem-se hohe a criptografia, oriunda do avanço da tecnologia de comunicação, servindo como uma ferramenta nas redes de computadores em que é utilizada em diversos sistemas fundamentais, a fim de garantir que a informação chegue ao seu destino. Esse processo evita que alguém sem ser o destinatário faça uso da informação. Sobre isso, Kurose & Ross (2010) conceitua.

> Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário é claro, deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados.

A criptografia está sendo usada constantemente em órgão públicos, mantendo a segurança no correio eletrônico. Assim, ela protege a integridade das informações que transitam na Internet, além de assegurar a validade e a autenticidade das mensagens, tanto de quem envia quanto de quem recebe.

---

[5]G1. Portal de Notícias – Globo. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. Jul/2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

Essa ferramenta transforma as informações, impossibilitando sua compreensão enquanto a informação não chegou ao seu local de destino. A partir do momento que os dados estão em seu destino, ela passa para a condição de ser compreendida para seu remetente, sendo assim considerada uma ferramenta segura.

Para uma melhor compreensão é necessário distinguir as expressões cifras e códigos. Para Tanebaum (2003, p.770):

> Uma cifra é uma transformação de caractere por caractere ou de bit por bit, sem levar em contra a estrutura linguística da mensagem. Em contraste, um código substitui uma palavra por outra palavra ou símbolo.

As cifras e os códigos têm seu funcionamento semelhante, porém com o mesmo objetivo: dificultar o acesso às informações. Os códigos não são mais utilizados nos dias atuais, ainda que muito usados por outros países durante a história. A exemplo, temos os Estados Unidos, que utilizou essa ferramenta durante as operações da Segunda Guerra Mundial, assim como conta em seu livro Redes de Computadores, Tanenbaum (2003, p.771):

> Eles simplesmente tinham índios navajo que se comunicavam uns com os outros usando palavras navajo específicas para termos militares como, por exemplo, *chay-dagahi-nail-tsaidi* (literalmente, assassino de cágado) para indicar uma arma antitanque. A linguagem navajo é altamente tonal, extremamente complexa, e não tem nenhuma forma escrita [...]

O funcionamento da criptografia não é tão simples. Por conta disso, é importante que compreendamos o que é a criptografia de chaves simétricas. Os algoritmos criptográficos envolvem a troca de um termo por outro, dificultando o entendimento do texto aberto. O sistema criptográfico é baseado na cifra de césar em que as letras do alfabeto são substituídas por outra, seguindo uma ordem regular, segundo Kurose (2010, p.496):

> A cifra de césar funciona tomando cada letra da mensagem do texto aberto e substituindo-a pela k-ésima letra sucessiva do alfabeto (...). se k=3, então a letra ‘a’ do texto aberto fica sendo ‘d’ no texto cifrado; ‘b’ no texto aberto se transforma em ‘e’ no texto cifrado, e assim por diante.

4.4.3 Assinaturas digitais e certificado digital

Quando se fala em criptografia é importante citar as assinaturas digitais. Essas assinaturas são um método de autenticação que substitui a assinatura física, eliminando a necessidade de possuir a versão de um documento assinado.

O uso dessa assinatura certifica de que a mensagem recebida realmente foi originada pelo emissor. Para constar esse requisito, a assinatura deve possuir as seguintes propriedades já citadas anteriormente (NBR ISO/IEC 27002, 2005):

1. Autenticidade;
2. Integridade;
3. Disponibilidade.

A partir dessas características, a assinatura se difere da manual. O processo de criptografia funciona por meio do *hash* e sua encriptação, que compreende ser um resumo da mensagem através de um algoritmo (MD5, SHA-1, SHA-256). Depois de gerado, este é criptografado através da chave pública, responsável por garantir a autenticidade da mensagem. O autor deve usar a chave privada para assinar a mensagem e armazenar o *hash* que foi criptografado com a mensagem original.

Para ser feita a autenticação do documento, o sistema deve gerar um novo resumo através da mensagem armazenada e comparado com a assinatura, descriptografando e obtendo o *hash* original.

No Brasil, há a Medida Provisória 2.200-2 de 24 de agosto de 2001 que estabelece regras em documentos digitais. De acordo com essa medida, um documento só tem validade se for certificado pelo ICP-Brasil.

> Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Essa medida também prevê a utilização de certificados emitidos por outras chaves públicas, exigindo o reconhecimento de ambas as partes.

Tanenbaum (2003, 506) explica que:

> A principal função de um certificado é vincular uma chave pública ao nome de um protagonista (indivíduo, empresa etc.). Os certificados em si não são secretos ou protegidos.

4.4.4 Ferramentas *antimalware*

São ferramentas que procuram descobrir, suprimir ou remover programas ou códigos de um computador que infectou ou estejam infectando a máquina. Antivírus e *antispwware* são exemplos de ferramentas anti-intrusos.

Apesar de que existam programas específicos para inúmeros tipos de códigos maliciosos, é difícil determinar uma área especifica de atuação para cada um, visto que diversos fabricantes mesclam característica de diversos programas maliciosos em um só programa englobando uma maior quantidade de funcionalidades. Apesar de serem criados para combater os vírus, com o passar do tempo, estes englobaram outras funcionalidades.

Segundo o Cert.br (2012, p.56):

> Para escolher o *antimalware* que melhor se adapta à sua necessidade é importante levar em conta o uso que você faz e as características de cada versão.

Desse modo, para a escolha de um *antimalware*, é importante que se avaliem as necessidades de cada máquina, de acordo com as atividades nela realizadas, bem como o que cada produto no mercado proporciona em termos de segurança.

4.4.5 Filtro *antispam*

Primeiramente, para entendermos a função do antispam é fundamental compreendermos o que é spam. Cert.br (2012, p.33) conceitua-o como:

> *Spam* é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (***U****nsolicited* ***C****ommercial* ***E****-mail*).

Os filtros antispam vêm integrados nos principais *webmails* e *software* leitores de e-mail ao fazerem a separação das mensagens desejadas e indesejadas, denominados de spam. Desde sua primeira aparição, esse tipo de praga virtual só vem evoluindo juntamente com as tecnologias, como comenta o Cert.br (2012, p.33):

> Desde o primeiro *spam* registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias. Atualmente, o envio de *spam* é uma prática que causa preocupação, tanto pelo aumento desenfreado do volume de mensagens na rede, como pela natureza e pelos objetivos destas mensagens.

Os spams estão diretamente associados a ataques pela internet, sendo os principais responsáveis pela propagação e disseminação dos códigos maliciosos. Alguns problemas são causados por eles, e, de acordo com o Cert.br (2012, p.34) são:

> **Perda de mensagens importantes**: devido ao grande volume de spam recebido, você corre o risco de não ler mensagens importantes, lê-las com atraso ou apagá-las por engano;
> **Conteúdo impróprio ou ofensivo**: como grande parte dos spams são enviados para conjuntos aleatórios de endereços de e-mail, é bastante provável que você receba mensagens cujo conteúdo considere impróprio ou ofensivo;
> **Gasto desnecessário de tempo**: para cada spam recebido, é necessário que você gaste um tempo para lê-lo, identificá-lo e removê-lo da sua caixa postal, o que pode resultar em gasto desnecessário de tempo e em perda de produtividade;
> **Não recebimento de e-mails**: caso o número de spams recebidos seja grande e você utilize um serviço de e-mail que limite o tamanho de caixa postal, você corre o risco de lotar a sua área de e-mail e, até que consiga liberar espaço, ficará impedido de receber novas mensagens;
> **Classificação errada de mensagens**: caso utilize sistemas de filtragem com regras antispam ineficientes, você corre o risco de ter mensagens legítimas classificadas como spam e que, de acordo com as suas configurações, podem ser apagadas, movidas para quarentena ou redirecionadas para outras pastas de e-mail.

As técnicas para capturar e-mail são distintas, sendo possível a compra de banco de dados ou na produção de suas listas para ataques. Segundo o Cert.br (2012, p.35) elas podem ser geradas por:

> **Ataques de dicionário:** consistem em formar endereços de *e-mail* a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.
> **Códigos maliciosos:** muitos códigos maliciosos são projetados para varrer o computador infectado em busca de endereços de *e-mail* que, posteriormente, são repassados para os *spammers*.
> ***Harvesting*:** consiste em coletar endereços de *e-mail* por meio de varreduras em páginas *Web* e arquivos de listas de discussão, entre outros. Para tentar combater esta técnica, muitas páginas *Web* e listas de discussão apresentam os endereços de forma ofuscada (por exemplo, substituindo o "@" por "(at)" e os pontos pela palavra "dot"). Infelizmente, tais substituições são previstas por vários dos programas que implementam esta técnica.

4.5 Ataques e incidentes

Uma matéria divulgada no site E-Commerce News[6] em maio de 2018 relata um caso real de um banco no Chile em que os computadores dos funcionários pararam de funcionar. Primeiramente, algumas dúzias foram infectados e logo após milhares de computadores já haviam sido invadidos. A intenção do ataque não era destruir sistemas, mas sim roubar dinheiro. Denominado de *malware MBRKiller*, esse vírus espalha-se dentro da rede, vasculhando sistemas vulneráveis em seu

[6] E-commerce News - Segurança da informação: **Como foi o ataque dos sistemas de um grande banco chileno**. Jul/2018. Disponível em: < https://ecommercenews.com.br/noticias/pesquisas-noticias/seguranca-da-informacao-como-foi-o-ataque-dos-sistemas-de-um-grande-banco-chileno/> acesso em: 27 setembro, 2018.

caminho. Esse vírus torna as estações de trabalho nulas, tendo como resultado a perda dos dados, total ou integralmente. É uma variante de um *malware* mais antigo *KillDisk Wiper*, o que aponta a novas modificações de vírus para o uso adequado em novas ameaças.

Os ataques nada mais são do que a concretização de uma ameaça originada por pessoas que, utilizando recursos computacionais, buscam a penetração dentro de um sistema. João apud Shell (2001) declara que não existe uma ciência capaz de eliminar de maneira definitiva os incidentes de segurança, restando como solução a vigilância e a verificação.

Os ataques mais conhecidos são por meio dos vírus. Veiga (2004, p.65) conceitua vírus:

> Estes são programas informáticos que podem ser introduzidos num computador por vários meios e que têm como objetivo prejudicar o bom funcionamento dos sistemas ao destruir informação, degradando o desempenho do sistema ou capturando informação que depois é enviada para o exterior.

Veiga (2004, p.66) destaca ainda que:

> Um vírus é um programa que uma vez instalado num sistema de informação efetua um conjunto de operações que podem ir desde a destruição de informação, passando pela perturbação do bom funcionamento do sistema ou simplesmente a realização de operações mais ou menos inofensivas. Durante este processo o programa procura replicar-se noutros sistemas da rede em que o sistema inicialmente atacado está integrado.

Os vírus são um tipo de "m*alware".* Cert.br (2012, p.23) conceitua-os como sendo:

> Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

Malware é o termo geral utilizado para se referir a uma variedade de software prejudicial como, por exemplo, um vírus. Esses programas destinam-se a infiltração num sistema de maneira ilícita, com o objetivo de causar algum tipo de dano, alterar ou roubar informações. Podem atacar na sua forma executável, através de scripts ou por outros programas instalados no computador da vítima. Cert.br (2012, p.23):

> Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Os motivos que os fazem lançar ataques na Internet são bastante distintos, que podem variar de uma simples diversão até a realização de ações criminosas. Segundo o site Cert.br (2012, p. 17 e 18) as maiores motivações são:

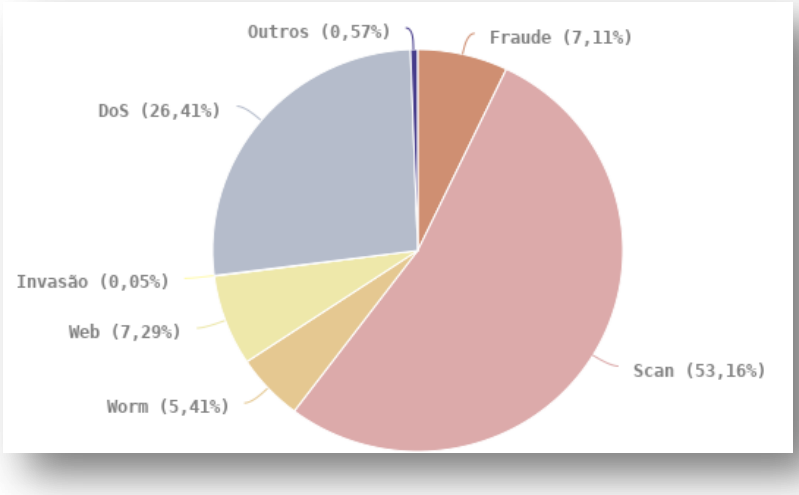
> **Demonstração de poder**: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente;
> **Prestígio**: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo;
> **Motivações financeiras**: coletar e utilizar informações confidenciais de usuários para aplicar golpes (mais detalhes no Capítulo Golpes na Internet).
> **Motivações ideológicas**: tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia;
> **Motivações comerciais**: tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Cert.br (2012, p.24) declara que:

> Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.

O gráfico a seguir demonstra os incidentes mais comuns que foram reportados ao Cert.br (2012):

Gráfico 1 - Incidentes reportados ao CERT.br - janeiro a dezembro



Fonte: CERT.br, 2018.

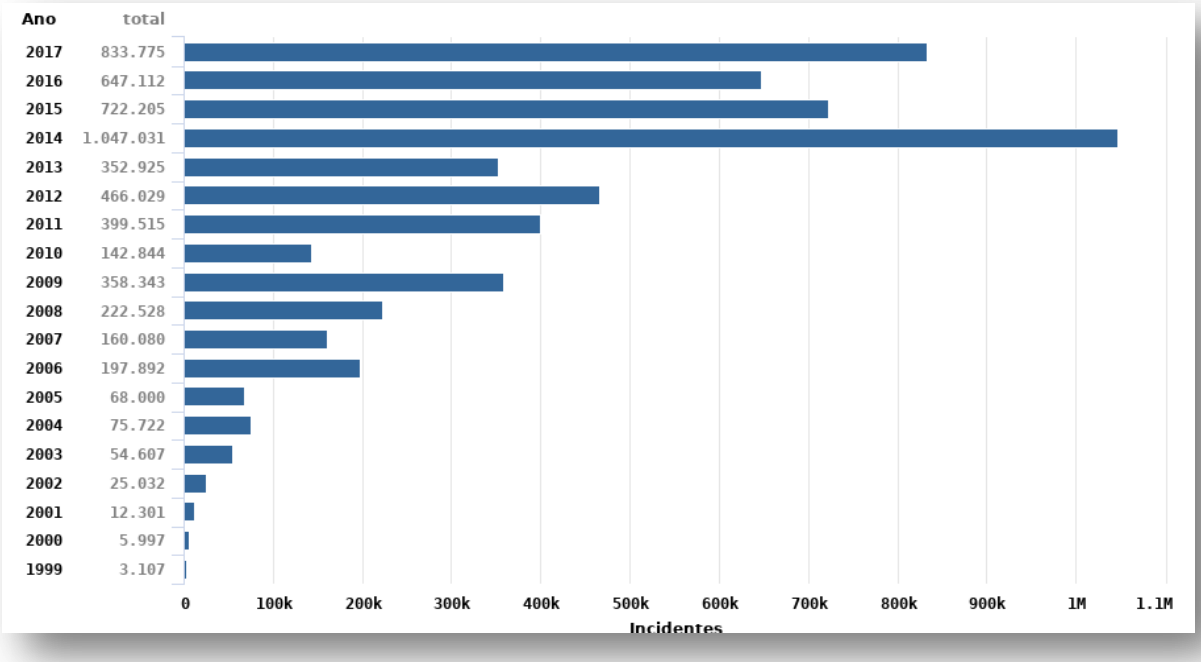
O gráfico relata que cerca de 26,41% correspondem ao ataque *Denial of Service* (DoS), traduzido como “negação de serviço”. 7,29% dizem respeito a um

caso particular de ataque que visa especialmente os servidores Web ou desfigurações de páginas que se encontram na Internet. *Scan* ficou com 53,16% de notificações de varreduras em redes de computadores, objetivando identificar computadores ativos e quais serviços estão sendo disponibilizados.

De acordo com o dicionário online português, um incidente[7] é um "episódio inesperado ou situação que altera a ordem normal das coisas". Na informática, um incidente[8] é qualquer evento relacionado com o sistema informacional com algum tipo de suspeita.

Segundo o site CERT.br, no ano de 2017 o Brasil recebeu um total de 833.775 incidentes de segurança da informação no período de janeiro a dezembro, correspondendo a um aumento de 29% em relação a 2016, como mostra a tabela a seguir:

Gráfico 2 - Total de incidentes reportados ao CERT.br por ano



Fonte: CERT.br, 2018.

[7] INCIDENTES. Dicio dicionário online de português. Disponível em <https://www.dicio.com.br/incidente/>. Acesso em 27 set. 2017.

No ano de 2017 o CERT.br[9] informa que recebeu 220.188 notificações de ataques de negação de serviço conhecidos como o DOS. Esse número representa um aumento de quatro vezes em relação aos datados no ano de 2016.

Ainda no ano de 2017, as notificações correspondentes a varreduras somaram 443.258, equivalendo a um aumento de 15% com relação a 2016. Os ataques de força bruta corresponderam à: *Secure Shell* (SSH) (22/TCP) com 47% das notificações de varreduras, *Telnet* (23/TCP) com 9%, RDP (3389/TCP) com 2% e *File Transfer Protocol* (FTP) (21/TCP) com 1% do total das notificações no ano de 2017 (CERT.br 2017).

Os ataques no protocolo *Telnet* (23/TCP), bem como nas portas 23/TCP e 2323/TCP, que continuam a ter destaque desde o ano de 2015, correspondem a 14% das notificações e parecem visar dispositivos IoT e equipamentos de rede destinados às residências de usuários finais das operadoras, tais como modems (ADSL, cabo e fibra), roteadores Wi-Fi e outros (CERT.br 2017).

As notificações em protocolos de SMTP nas portas (25/TCP), que em 2016 corresponderam a um total de 30% de todas as varreduras, agora correspondem a 21%. As portas *Internet Message Access Protocol* (IMAP) (143/TCP) e *Message Submission* (MAS) (587/TCP) correspondem nesta ordem a 3% e 1% dos ataques notificados. Com relação ao SMTP (25/TCP) existem abusos como: investidas no envio de e-mails com uso de biblioteca de nomes de usuários; exploração nos servidores de e-mail como *open-relays*; e força bruta para envio de mensagens utilizando credenciais de usuários existentes nos sistemas atacados (CERT.br 2017).

As varreduras no protocolo IMAP, porta 143/TCP, e MAS, porta 587/TCP são relacionadas aos ataques de forma bruta com o objetivo de furtar credenciais de usuários do sistema para o envio de e-mail e utilizar tais informações (CERT.br 2017).

As propagações de *worms* e *bots* somam 45.101 no ano de 2017, equivalendo a um aumento de 60% em relação ao ano de 2016 (CERT.br 2017).

---

[9] CERT.BR. **Estatísticas dos incidentes reportados ao Cert.br.** 2018. Disponivel em: < https://www.cert.br/stats/incidentes/>. Acesso em: 27 setembro 2018.

4.5.1 *Adware*

São programas que exibem tanto propagandas como anúncios sem a autorização do usuário, possibilitando que o computador da vítima se torne mais lento. Frequentemente apresentam o formato de *pop-up*, aquelas janelas incômodas que abrem a todo instante enquanto se navega em determinado site. (MARTINS, 2008)

Ou seja, o adware é qualquer software que executa de maneira automática e mostra uma grande quantidade de anúncios sem a autorização do usuário, o que pode ser bastante incômodo. Além disso, a conexão com a internet pode ser prejudicada, uma vez que programas como esses precisam ser atualizados constantemente.

4.5.2 *Backdoor*

Cert.br (2012, p.28) relata que:

> A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como *backdoors*.

É um recurso para garantir acesso remotamente através de *malwares* com o objetivo de explorar falhas críticas nos programas instalados ou até mesmo que não foram atualizados no "*firewall*", abrindo as portas do roteador.

4.5.3 Cavalo de Troia

Cert.br (2012, p.28) descreve como:

> Cavalo de troia, *trojan* ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

O objetivo do cavalo de troia é manter-se oculto e, enquanto o usuário não vê, esse vírus instala as ameaças mais complexas. Sua infecção pode ser através de arquivos de músicas, mensagens de e-mail ou em sites maliciosos. Eles se aproveitam da vulnerabilidade do navegador.

4.5.4 *Rootkit*

Cert.br (2012, p.29) conceitua como:

> *Rootkit* é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Os *Rootkits* usam métodos de programação e são instalados nas camadas mais abaixo que não estão relacionadas nos *logs* do sistema operacional. Sua façanha está na capacidade de recuperação de maneira automática sendo reinstalado após a limpeza do computador.

4.5.5 *Spyware*

Esses são considerados programas espiões, são usados com o objetivo de fazer a captura dos dados sobre costumes que os usuários de internet possuem. Seu principal propósito é a propaganda específica de acordo com o que se acessa. *Spyware* é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros (CERT.BR, 2012).

4.5.6 *Worm*

Cert.br (2012, p.25) relata que:

> Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Esse tipo de ameaça infecta pela rede de computadores e a dispositivos de armazenamento e se replicam sem a necessidade de infectar arquivos legítimos. Sua distribuição também pode contar com as mensagens de e-mail.

4.6 Ameaças, Vulnerabilidades e riscos

De acordo com Dias (200 p. 55) “as ameaças podem ser entendidas como um evento ou atitude indesejável que podem desabilitar, danificar, excluir um recurso” (apud João, 2006, p.47). A mesma autora considera também que um recurso é integrante de um sistema computacional, podendo ser físico ou em formato de informação.

Segundo Silva, Carvalho e Torres (2003) os riscos compreendem identificar medidas que proporcionem a organização certo nível de segurança. É constituído em etapas contendo a identificação e classificação dos riscos, e especificando ainda um conjunto no qual permitirão reduzir ou eliminar os riscos.

Além da confidencialidade, integridade e disponibilidade, existe um fundamento importante que está relacionado diretamente com os riscos: as vulnerabilidades. São as fraquezas com potencialidade de provocar algum tipo de dano, ou seja, são pontos fracos. Segundo a NBR ISO/IEC 27002:2005, a vulnerabilidade é uma fragilidade explorada por uma ou diversas ameaças, ou seja, uma condição a ser explorada por um usuário avançado com ações maliciosas pode ter como resultado um atentado na segurança da informação. Essas ações podem estar relacionadas com os processos, políticas, equipamentos e recurso humanos da empresa. De modo isolado estas não provocam incidentes, mas através de um agente causador torna-se um perigo. Segundo Nakamura (2016):

> Um ataque só acontece porque vulnerabilidades são exploradas pelos atacantes. Temos que eliminar todos os pontos fracos de nosso ambiente. Em todos os níveis. E, em segurança da informação, vulnerabilidades existem em todas as camadas: humano, físico, hardware, protocolo, sistema operacional, aplicação, rede, arquitetura, entre outros. (NAKAMURA, 2016)

Os ataques possuem uma lógica diretamente proporcional: quanto maior a vulnerabilidade, maiores serão as fraquezas e a probabilidade de investidas. Assim, é preciso conhecer todas as fraquezas para que sejam eliminadas as chances de invasões. Para um invasor é necessário somente que esteja disponível no mínimo um ponto fraco e, por conseguinte, explorá-la de acordo com algumas técnicas e ferramentas próprias.

As redes de computadores, os Sistemas de Informação e os bancos de dados são os principais pontos de vulnerabilidade e risco. Elementos básicos como segurança na estação, segurança no meio de transporte, segurança no servidor e na rede interna são necessários para obter maior segurança na aplicação para Internet.

Nota-se que não é mencionado o recurso humano ao qual é considerado um componente de altíssima importância sobre todos os aspectos da segurança. Essa linha acredita que o homem pode gerar prejuízo ao sistema, mas não valida o pressuposto de que ele possa ser capaz de provocar um grande prejuízo informacional para a organização.

Embora muitos administradores e chefes de instituições reconheçam a segurança da informação como sendo algo importante, muitas vezes não lhe é dada a devida importância.

Com o crescimento exponencial das grandes redes, especialmente da internet, surgiu um fenômeno bem complicado para a segurança, “o anonimato”, que permite a não identificação da autoria. Assim, um usuário pode se passar por qualquer outra pessoa. Isso vai exigir que, na maioria dos casos, as corporações adotem medidas ou mecanismo de identificação eletrônica como regras de autenticação ou até mesmo certificado digital.

4.6.1 *Smartphones*

A preocupação em se proteger contra cibercrimes não é um hábito entre os usuários em tecnologia pela maioria das pessoas que acessam a Internet por computadores. No entanto, quando se trata de *smartphones* esse número cai significativamente.

Uma pesquisa feita pela Kaspersky Lab (2016) mostrou que metade de todos os *smartphones* está correndo grande risco a ataques maliciosos por conta da ausência de proteção. A pesquisa foi realizada com 12 mil usuários de 21 países, contando inclusive com a participação do Brasil. Na pesquisa, 57% dos tablets e 53% dos *smartphones* possuem no mínimo uma segurança instalada.

Esses dispositivos possuem diversas informações pessoais. Assim, é um erro os usuários possuírem esse comportamento de risco. Mesmo com tantos acessos, ainda faltam conhecimentos sobre os perigos no acesso à Internet. A pesquisa ainda mostra que os usuários não conhecem a importância de ter a proteção nos dispositivos. De acordo com o relatório, cerca de 21% das pessoas que se conectam à Internet não sabem nada sobre os *malwares* para dispositivos móveis (KASPERSKY LAB, 2016).

Dos entrevistados, 54% concordam que seus computadores precisam de um programa de segurança. Somente 42% destes esclarecem que têm a mesma ideia sobre os dispositivos móveis (KASPERSKY LAB, 2016).

Durante a pesquisa, 82% dos dispositivos possuem senha. Apesar de que as senhas sejam de grande utilidade para dificultar o acesso aos dispositivos, elas não conseguem bloquear os *malwares* ou outros ataques e ameaças. Na realidade

41% dos usuários protegem seus dispositivos móveis com senhas e soluções em segurança (KASPERSKY LAB, 2016).

Os resultados apresentados pela Kaspersky (2016) trazem um cenário alarmante. Dentre as vítimas de ameaças virtuais, 18% apresentaram infecção e 22% tiveram suas informações roubadas.

Outra questão bem preocupante é o ‘recurso humano’. É comum notar que o elo mais fraco na questão da segurança da informação seja o usuário, já que os recursos considerados computacionais já estariam com proteção.

Segurança é uma questão complexa, mesmo para os experientes especialistas em segurança. Não é fácil encontrar o equilíbrio entre as medidas de segurança que são muito restritivas e as ineficazes ou inadequadas.

Os riscos são condições que geram um potencial de danos e perdas. É mensurado pela probabilidade de um acontecimento gerando assim as perdas. Pode-se concluir, portanto, que o risco está relacionado com a probabilidade de um evento e suas consequências. Dessa forma, quando nos referirmos esse termo, devemos sempre atentar para a probabilidade de concretização de um evento e suas consequências. E essas consequências são negativas.

4.6.2 *Phishing*

Esse método é muito utilizado como uma das técnicas de mensagens falsas com links que manipulam os usuários para direcioná-los a sites considerados nocivos.

De acordo com a cartilha digital Cert.br (2012, p.09):

> Phishing , phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Os ataques de *phishing* eram enviados para um grande número para as possíveis vítimas. Atualmente, as técnicas de engenharia social das mensagens estão sendo mais personalizadas. Esses ataques são direcionados através de links maliciosos contendo um programa *malware* com a possibilidade de infectar não somente o computador da vítima como também toda a rede.

Na maioria dos ataques, os funcionários acabam sendo a porta para as falhas de segurança por não possuírem a orientação necessária e por falta de

proteção adequada. Por esse motivo, é importante que haja orientação e treinamentos constantes para educar os profissionais a não abrirem arquivos que possam causar problemas na organização. Para o treinamento dos usuários é importante utilizar casos que se aproximam da realidade, expondo a existência de possíveis pontos vulneráveis a fim de que impossibilitem falhas de segurança (FRITZEN, 2016). Além disso, deve-se orientar a evitar clicar ou abrir sites suspeitos. Assim, é importante uma política completa de uso da Internet na organização com orientações básicas (FRITZEN, 2016).

A conscientização dos funcionários é importante, mas é necessária uma boa estrutura de segurança da Internet, com serviços de antivírus e controle de acesso à mesma, buscando orientações em empresas especializadas na área (FRITZEN, 2016).

5 METODOLOGIA

Levando em consideração a inportância da metodologia para a pesquisa científica, Marconi e Lakatos (2003, p.234) esclarecem que:

> Os trabalhos científicos devem ser elaborados de acordo com as normas preestabelecidas e com os fins a que se destinam. Serem inéditos ou originais e contribuem não só para a ampliação de conhecimentos ou a compreensão de certos ploblemas, mas também servirem de modelo ou oferecer subsídios para outros trabalhos.

O trabalho foi elaborado da seguinte maneira: pesquisa aplicada, probabilística, descritiva, levantamento e quantitativa.

Inicialmente realizou-se uma pesquisa bibliográfica em livros, artigos e trabalhos científicos nas bibliotecas da Universidade Estadual do Maranhão e da Academia de Polícia Militar Gonçalves Dias.

A pesquisa foi realizada no Quartel do Comando Geral da Polícia Militar do Maranhão, localizada na Avenida Jerônimo de Albuquerque, s/nº, bairro Calhau durante os meses de setembro e outubro de 2018. Para a busca dos dados, foram escolhidos usuários que trabalham nas diretorias, especialmente militares que utilizam computadores com acesso direto à Internet. Os policiais escolhidos serviram de amostra para esse trabalho, sendo classificados como usuários comuns, realizando atividades de cunho administrativo. Visando obter informações acerca tema, foi aplicado um questionário contendo 11 perguntas do tipo fechadas para 35 militares.

De acordo com Cervo e Bervian (2002, p. 48) o questionário “[...] refere-se a um meio de obter respostas às questões por uma fórmula que o próprio informante preenche”. Contém tanto perguntas abertas como fechadas. De maneira parecida, Marconi e Lakatos (2003, p. 88) conceitua o questionário como uma “[...] série ordenada de perguntas, respondidas por escrito sem a presença do pesquisador”.

Quanto à natureza escolhida, foi escolhida a pesquisa descritiva, pois os fatos serão analisados procurando descobrir a frequência com que ele ocorre e suas possíveis causas. Como estabelece Gil (2002, p.42):

> As pesquisas descritivas tem como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática.

Ao contrário de Gil, Castro (1976, p.66) acredita que a pesquisa descritiva mostra o cenário de uma situação, manifestando seus resultados em números.

> Quando se diz que uma pesquisa é descritiva, se está querendo dizer que se limita a uma descrição pura e simples de cada uma das variáveis, isoladamente, sem que sua associação ou interação com as demais sejam examinadas.

Do ponto de vista da sua natureza, a referida pesquisa é do tipo aplicada, pois objetiva gerar conhecimento na solução de problemas específicos.

Após delinear o universo da pesquisa, foi possível delimitar os elementos que serão estudados, como explica Marconi e Lakatos (2003, p.223):

> [...] não abrange a totalidade dos componentes do universo, surgindo a necessidade de investigar apenas uma parte dessa população. O problema da amostragem é, portanto, escolher uma parte (ou amostra), de tal forma que ela seja a mais representativa possível do todo e, a partir dos resultados obtidos, relativos a essa parte, poder inferir, o mais legitimamente possível, os resultados da população total, se esta fosse verificada.

Assim, de acordo com a técnica de amostragem, essa pesquisa foi probabilística, pois traz amostragens em que há uma escolha deliberada dos elementos da amostra, a depender dos critérios e julgamentos do pesquisador.

Quanto aos procedimentos utilizados, a pesquisa é bibliográfica. Segundo Fonseca (2002, p.32):

> A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referencias teóricas publicadas com o objetivo recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta.

Quanto à abordagem, a pesquisa foi do tipo quantitativa. De maneira a traduzir em forma de gráficos, os números coletados e mensurados, foi feita uma análise estatística. Para Richardson (1999) a pesquisa quantitativa emprega a quantificação tanto pela coleta como pelo tratamento por meios estatísticos. Mattar (2011) busca legitimar hipóteses usando dados estruturados, estatísticos, através de uma grande análise de casos.

Quanto aos procedimentos técnicos utilizados, a pesquisa foi do tipo levantamento, como esclarece Gil (2002, p.50):

> As pesquisas deste tipo caracterizam-se pela interrogação direta das pessoas cujo comportamento se deseja conhecer. Basicamente, procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para, em seguida, mediante análise quantitativa, obterem-se as conclusões correspondentes aos dados coletados.

De modo geral Gil (2002, p. 86) estabelece as fases da pesquisa de levantamento da seguinte maneira: a) Apresentação dos objetivos; b) Definição dos conceitos e variáveis; c) Realização de um estudo piloto; d) Seleção da amostra; e) Elaboração do instrumento e coleta de dados; e f) Análise e apresentação dos resultados.

Durante a pesquisa, algumas limitações ocorreram no decorrer do trabalho, resultando em um grande número de militares que se recusaram a responder ou que deixaram para um segundo momento.

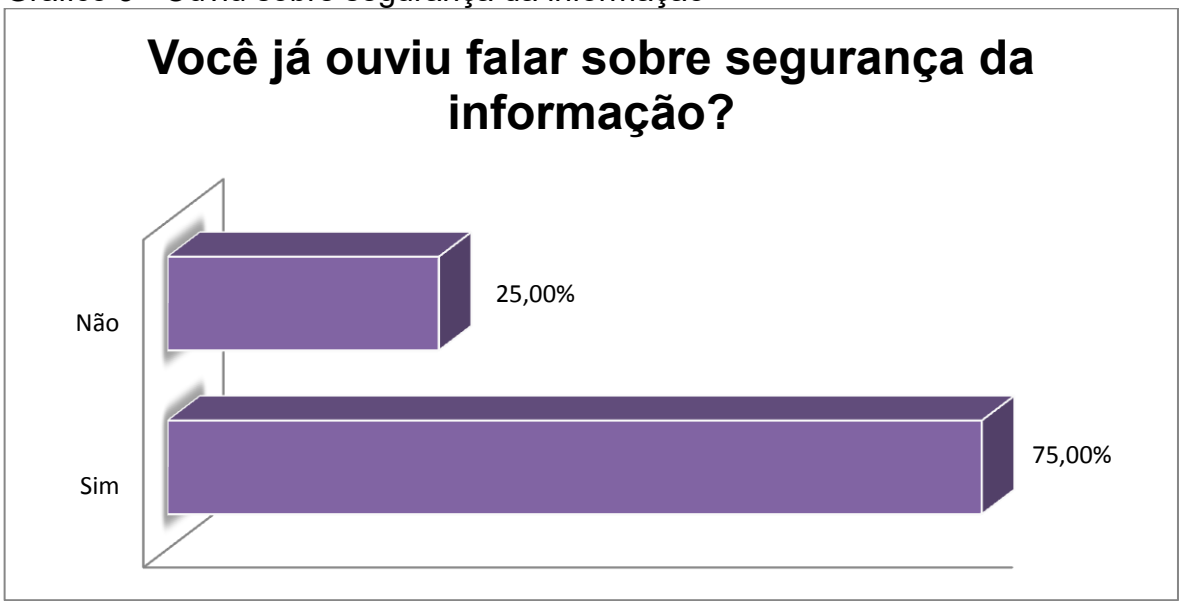
A análise dos dados foi realizada no mês de novembro e a partir dela foi possível organizar e sintetizar as informações de maneira tal que trouxe elucidações às questões das investigações. Simultaneamente, a interpretação extraiu ao extremo as informações. As análises foram apresentadas em forma de gráficos para um melhor entendimento.

6 ANÁLISE E DISCURSÃO DOS RESULTADOS

Foi aplicado um questionário estruturado (APÊNDICE A) com algumas questões importantes, a fim de aferir informações ao policial militar dentro desse universo. O local escolhido foi o Quartel do Comando Geral da PMMA, em que 35 militares participaram da pesquisa.

Nessa unidade militar encontra-se o centro administrativo da instituição, responsável por diversos documentos considerados sigilosos. Esse é o local de onde partem todas as ordens e orientações para a corporação em diversas partes do Estado. Os dados coletados foram analisados e serão apresentados a seguir:

Gráfico 3 - Ouviu sobre segurança da informação



Fonte: Dados da pesquisa, (2018).

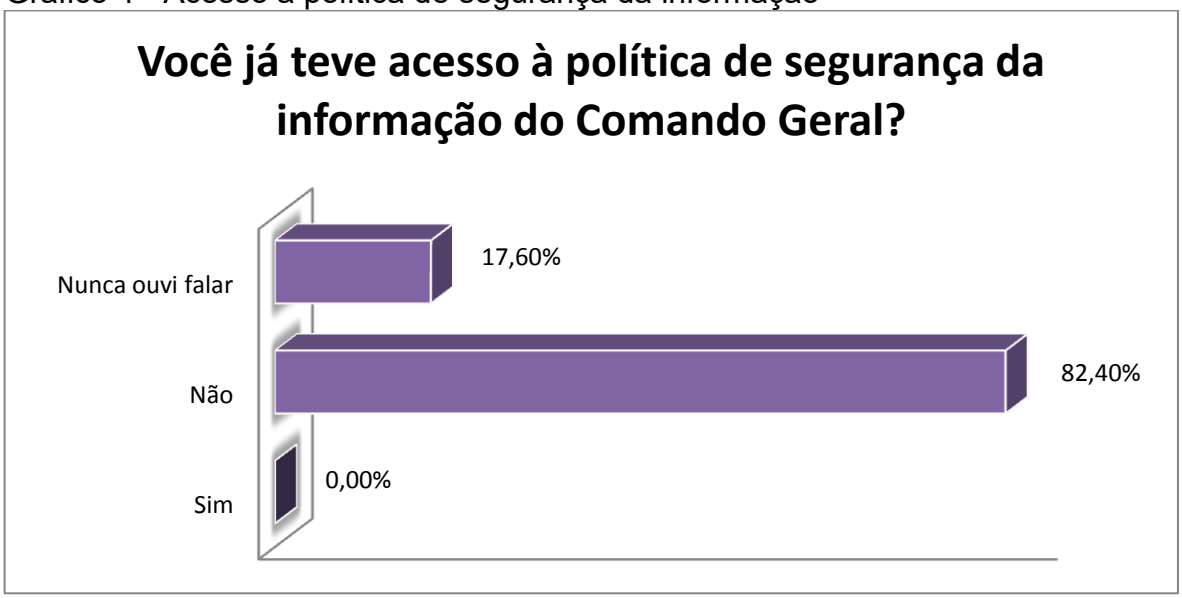
A maioria dos questionados responderam que já ouviram falar sobre segurança da informação, opção esta que representa cerca de 75% do total de respostas. Cerca de 25% dos militares responderam que nunca ouviram sobre segurança da informação.

A segurança da informação é considerada uma temática que necessita integrar a estratégia das organizações, devido ao aumento de incidentes, falhas de segurança e ao desenvolvimento de formas de ataques pela Internet.

Assim, é necessário orientar militares a identificar possíveis riscos, criando programas com instruções e orientações sobre ameaças, vulnerabilidades, riscos em segurança, tipos de ataques e os possíveis prejuízos. É recomendada a existência de uma política de acesso à Internet clara e divulgada, detalhando como os

equipamentos podem ser utilizados ou acessados. Recomenda-se também a utilização de materiais como vídeos e cartilhas com o objetivo de orientar a utilização segura da Internet.

Gráfico 4 - Acesso a política de segurança da informação



Fonte: Dados da pesquisa, (2018).

O gráfico 4 refere-se ao acesso à política de segurança da informação no Comando Geral. Cerca de 82,40% das respostas não teve acesso a política de segurança, e 17,60% nunca ouviram falar.

A política de segurança da informação funciona como um planejamento responsável por cuidar dos ativos da informação guiada pelos três princípios básicos da segurança, que são a confidencialidade, disponibilidade e integridade, já mencionadas no escopo deste trabalho.

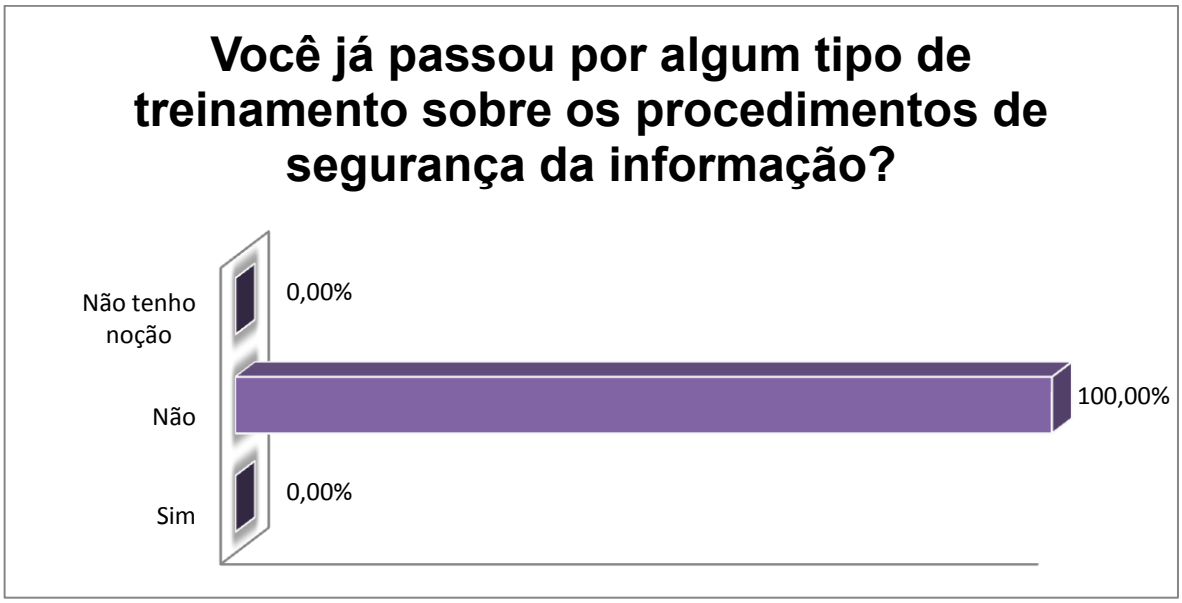
São utilizadas algumas estratégias para garantir esse princípio, além de um conjunto de ferramentas de acordo com o grau de segurança que a instituição precisa. Essas estratégias propiciam um melhor ambiente de confiabilidade e segurança. Como resultado, tem-se a diminuição de vulnerabilidades e detecção da existência de possíveis ameaças.

O centro de Estudos, Respostas e Tratamento de Incidentes no Brasil relatou cerca de 722 mil incidentes de segurança no ano de 2015 no país. Isso indica um fator muito importante e alarmante, apontando que os responsáveis pela gestão dos ativos na rede estão falhando na proteção dos dados.

Isso pode provocar diversos efeitos, como a perda de todos os dados da Polícia Militar do Maranhão, e podendo perder acesso aos seus sistemas e serviços

importantes. Além disso, pode ocorrer o furto de informações consideradas confidenciais.

Gráfico 5 - Treinamento



Fonte: Dados da pesquisa, (2018).

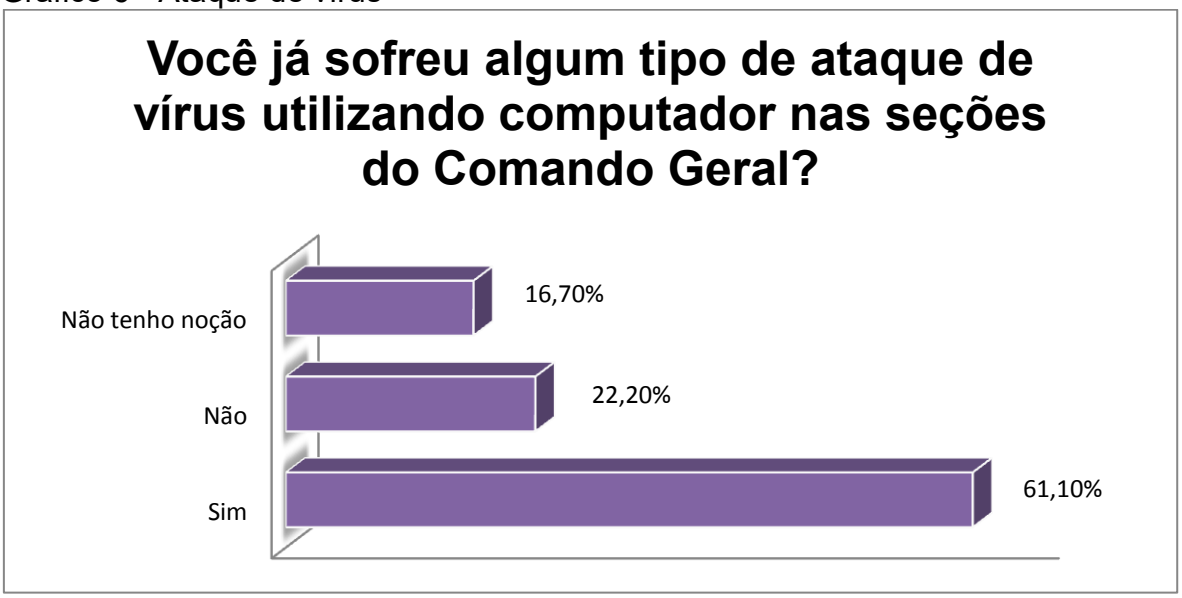
De acordo com o gráfico, 100% dos usuários responderam que nunca passaram por qualquer tipo de treinamento referente à segurança da informação. A conscientização em segurança é capaz de produzir mudanças no comportamento.

Um dos principais problemas na ausência de procedimentos em segurança é a possibilidade de que todos podem acessar qualquer arquivo ou páginas *Web* sem o devido cuidado, possibilitando assim a contaminação de algum *malware*. Isso mostra que os dados da instituição estão correndo um sério risco, proporcionando a propagação dos programas maliciosos pela rede interna.

Todas as boas práticas em segurança indicam para a necessidade de abranger os usuários no processo de segurança. Portanto, assim como o *firewall* e os antivírus, a consciência em segurança é fundamental para boas práticas de segurança da informação. Isso reduz o sucesso dos ataques que geram prejuízos para a instituição.

Assim, os militares ficariam mais atentos a ataques, tornando-se mais dispostos ao envolvimento em treinamentos, à medida em que aumenta a consciência da relevância do papel desempenhado na administração militar, podendo até sugerir novas medidas em segurança. Além de serem apenas usuários conscientes, passariam a ser também usuários participativos.

Gráfico 6 - Ataque de vírus



Fonte: Dados da pesquisa, (2018).

O gráfico 6 mostra se o usuário já sofreu algum tipo de ataque de vírus nos computadores da unidade. A situação é assustadora, pois de acordo as respostas coletadas pelos militares, cerca de 61,10% já sofreram ataques, 16,7% não tem sequer noção e 22,2% nunca sofreram com vírus.

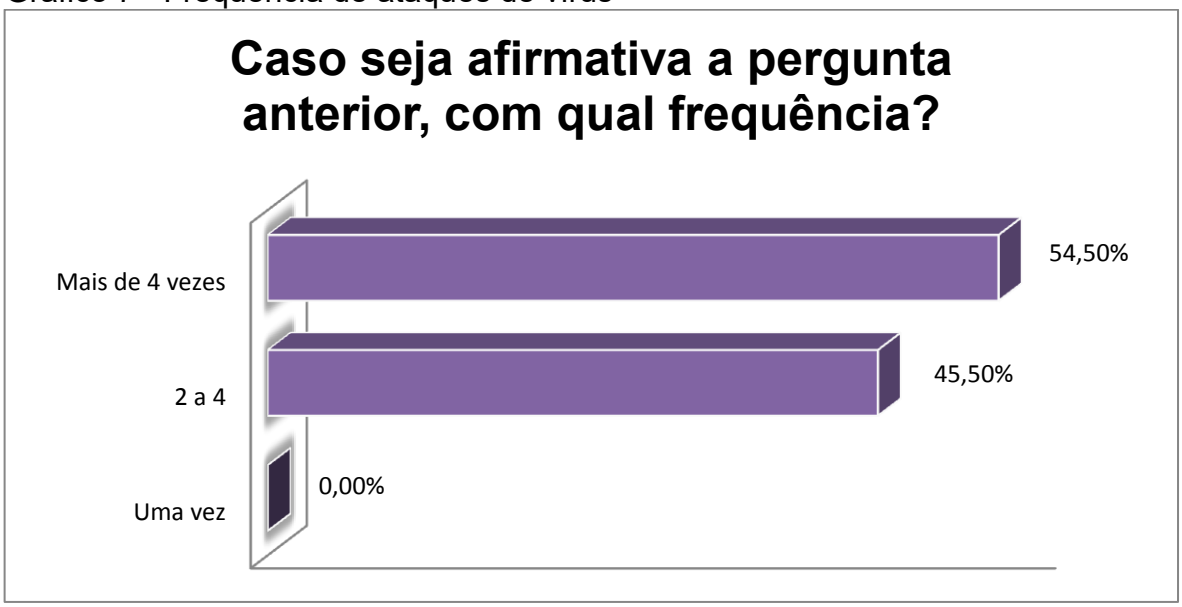
O número correspondente a usuários que já sofreram ataques é alto, configurando um ambiente vulnerável. Isso é um risco e torna o trabalho desempenhado no quartel do Comando Geral perigoso. Arquivos considerados sigilosos podem ser perdidos ou ocorrer vazamento de informações.

Os vírus se infiltram dentro de um sistema, causando algum tipo de prejuízo. Podem atacar na sua forma executável, através de scripts ou por outros programas instalados no computador da vítima, roubando ou editando informações consideradas importantes.

Tais dados são preocupantes, visto que na área da informação existem diversos tipos de vírus – dos mais simples aos mais complexos – que infectam todos ou alguns arquivos e programas utilizados pelos usuários.

Um dos principais responsáveis pelas invasões são os próprios usuários. Normalmente é ele quem faz a execução dessas “pragas virtuais” através de e-mails desconhecidos. Existe também a autoexecução, porém é mais rara de acontecer, havendo a possibilidade de autopropagação.

Gráfico 7 - Frequência de ataques de vírus



Fonte: Dados da pesquisa, (2018).

O gráfico 7 revela a frequência de ocorrências com vírus em computadores utilizados no QCG. De acordo com os resultados mostrados acima, cerca de 45,5% dos usuários relataram que tiveram de 2 a 4 vezes problemas com vírus. 54,5% já sofreram com essa dificuldade por mais de 4 vezes.

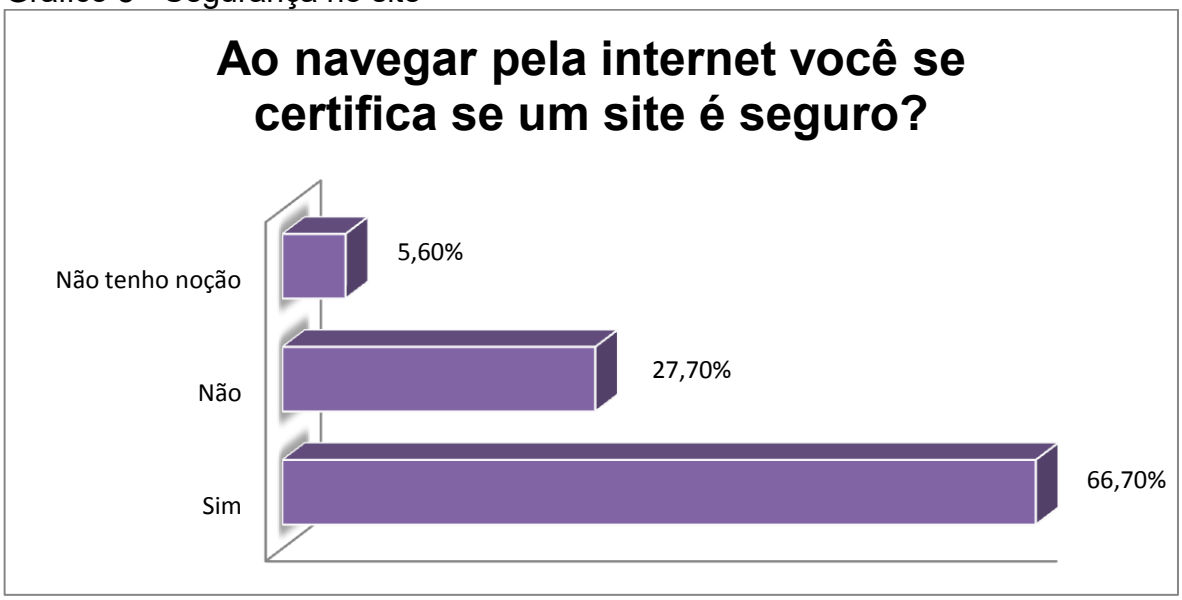
Isso indica que não há segurança nos computadores do Comando Geral, permitindo que ataques sejam feitos mais de uma vez. Isso ocasiona um risco para a Polícia Militar, considerada uma instituição pública que trabalha com documentos públicos com grau de sigilo.

É preciso cuidado na hora de usar a internet. A falta de uma política de segurança, de conhecimento e de mentalidade sobre o assunto corroboram conjuntamente para um ambiente de alto risco.

Existem computadores em que os indicativos de vírus são diferentes um dos outros. Os exemplos mais rotineiros são: barras de ferramentas, quedas no desempenho dos computadores e abertura de sites de maneira involuntária.

É necessário que os computadores infectados sejam iniciados em modo de segurança, e que seja executada a varredura de todo o sistema. Caso o procedimento não seja suficiente, as máquinas precisam ser examinadas por profissionais especialistas. Para João (2001), não existe uma total segurança, restando como solução a vigilância e a verificação nos sistemas.

Gráfico 8 - Segurança no site



Fonte: Dados da pesquisa, (2018).

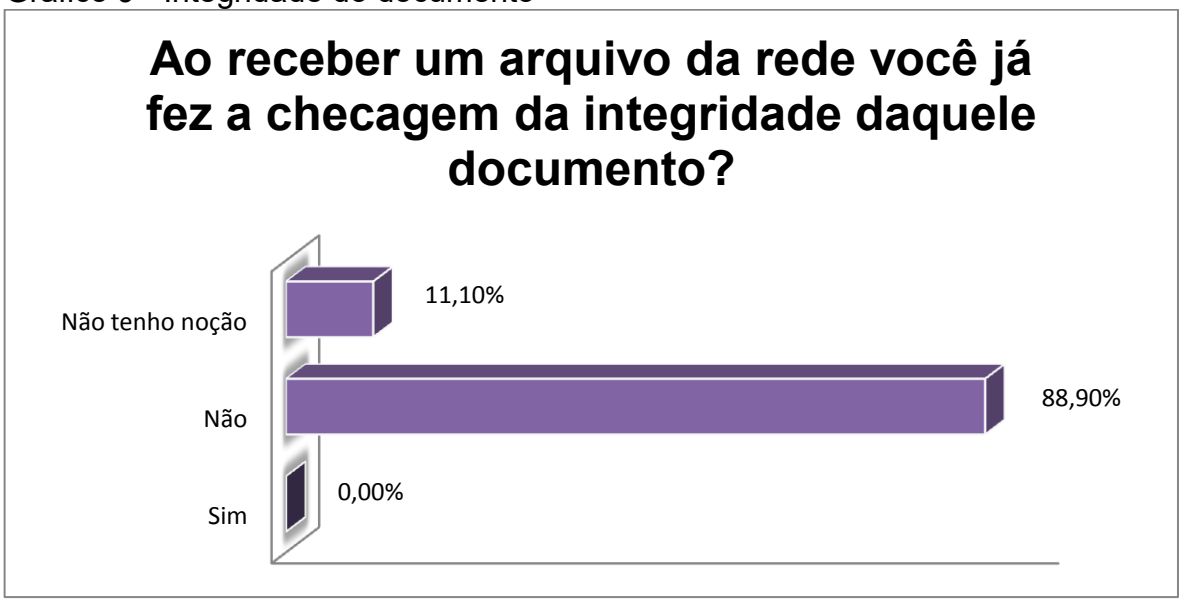
O gráfico 8 tenta questionar se durante a navegação o militar certifica se um site possui segurança. Apesar da maioria dos entrevistados responder que “sim”, cerca de 27,7% dos militares não realizam a checagem e 5,60% não possuem noção sobre segurança em sites, tornando o sistema vulnerável a ataques de usuários maliciosos.

Os navegadores mais usados incluem algumas ferramentas de segurança para ajudar o usuário a manter sua navegação protegida. Essas ferramentas podem desativar conteúdo Flash sem segurança, bloquear downloads malignos e controlar sites que podem acessar recursos audiovisuais. Além disso, é utilizado o protocolo que torna a navegação segura, denominado HTTPS, uma versão do HTTP, porém é inserido uma linha de segurança. O cadeado na barra de navegação indica se o site utiliza o certifica digital SSL confiável, ou seja, se a conexão está protegida.

Embora haja uma parcela considerável de militares que sabem identificar a aplicação desse recurso de segurança, a quantidade de “desorientados” é significativa. Estes usuários realizam diariamente acessos a sites bancários, envio de e-mails e compras pela Internet sem saber que seus dados podem estar sendo interceptados ou violados.

Além de realizar a checagem da segurança em sites, é necessário também averiguar se a página é verdadeira, ou seja, se a página corresponde a um site genuíno. Apesar da segurança em certificado digital, sites maliciosos podem usar de segurança para roubar informações.

Gráfico 9 - Integridade do documento



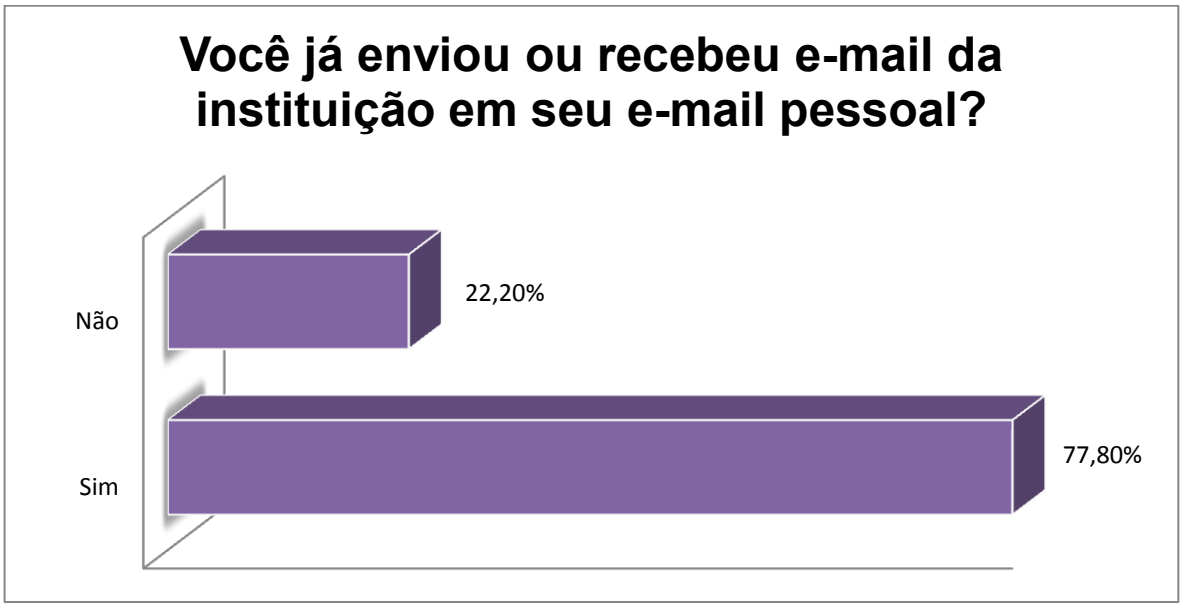
Fonte: Dados da pesquisa, (2018).

O gráfico 9 estabelece a checagem da integridade dos documentos recebidos pela rede do Comando Geral. Durante a análise verificou-se que 88,90% não fazer a checagem da integridade do documento, 11,10% não tem noção e nenhum dos questionados responderam “sim” ao questionário.

Essas ações visam certificar-se de que um documento não teve seu conteúdo modificado após a assinatura. Para tanto, o sistema é capacitado a identificar alterações em seu conteúdo. Qualquer alteração realizada em um documento com certificado digital o torna inválido e por esse motivo é impossível falsificá-lo.

O Brasil possui uma entidade pública certificadora composta por autoridades certificadoras que, através de técnicas e procedimentos, consegue assegurar a identidade de um usuário na mídia eletrônica. Esse método de segurança garante também que um usuário de e-mail seja realmente o emissor da mensagem e que o receptor seja realmente uma pessoa autêntica.

Gráfico 10 - Envio e recebimento de e-mail



Fonte: Dados da pesquisa, (2018).

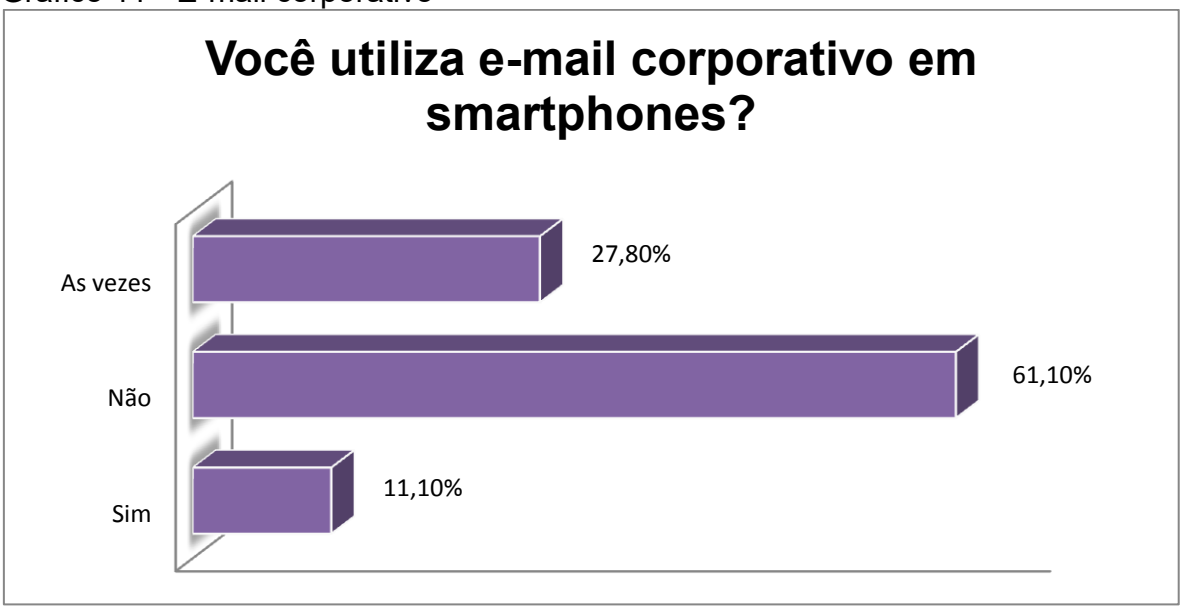
O gráfico 10 indaga sobre o recebimento ou envio de e-mails da instituição em e-mails pessoais do militar. Os resultados mostram que 77,8% dos usuários interagem com a corporação através do envio ou recebimento de mensagens de texto ou de arquivos. Isso é um perigo imenso, já que as informações referentes à corporação não podem ser interagidas com as informações pessoais.

Desta maneira, a utilização de e-mails institucionais garantiria um arquivamento e um registro de arquivos mais eficientes com acessos aos documentos de forma ágil e completamente integrada, contemplando também o histórico de conversas e a localização de informações relevantes para a corporação. O administrador da rede tem controle de todas as mensagens, como senhas, monitoramento de ações, bloqueios de acessos indesejados, contemplando sempre a privacidade e a segurança dos ativos da Polícia Militar.

O e-mail institucional evita alguns riscos e problemas inesperados que atingem servidores externos gratuitos, como mencionado anteriormente no escopo deste trabalho. O site Cert.br (2012) reportou informações de notificações com investidas no envio de *e-mails* com uso de biblioteca de nomes de usuários; exploração nos servidores de *e-mail* como open-relays; e força bruta para envio de mensagens utilizando credenciais de usuários existentes nos sistemas atacados. As varreduras no protocolo IMAP, porta 143/TCP, e MAS, porta 587/TCP são relacionadas aos ataques de forma bruta com o objetivo de furtar credenciais de

usuários do sistema para o envio de e-mail usando as credenciais descobertas pelo atacante.

Gráfico 11 - E-mail corporativo



Fonte: Dados da pesquisa, (2018).

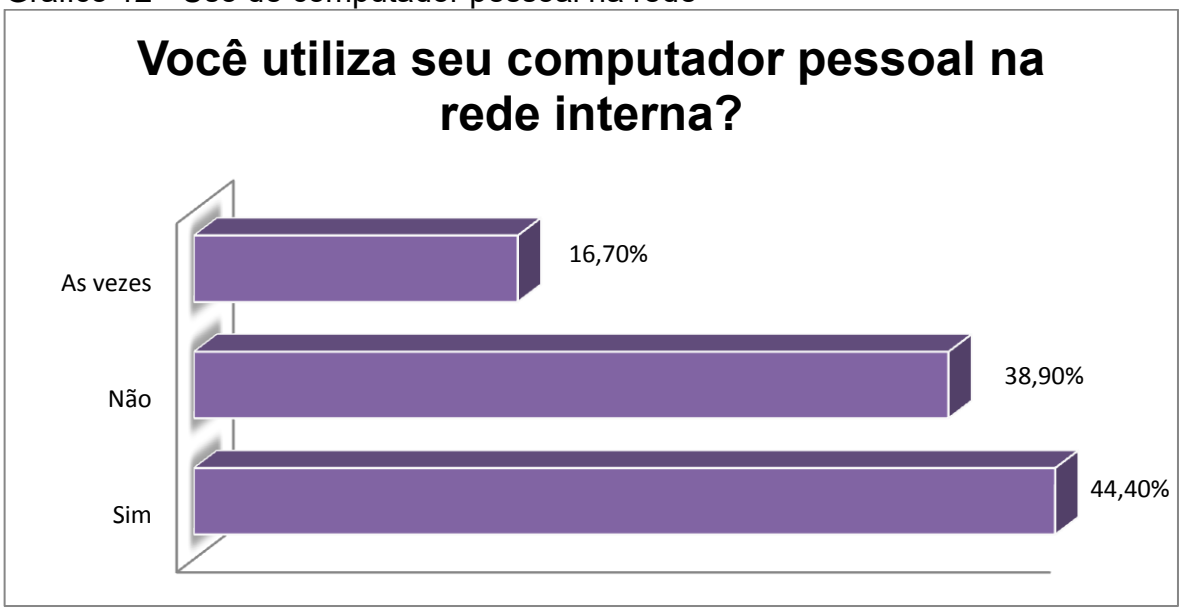
A pesquisa mostrou que cerca de 11,10% responderam que sim e 27,8% responderam que às vezes utilizam o e-mail corporativo em *smartphones*. Uma pesquisa feita já citada no corpo deste trabalho mostrou que metades desses aparelhos estão correndo grande risco a ataques maliciosos por conta da ausência de proteção.

Existem alguns riscos na utilização do e-mail corporativo como, por exemplo, o roubo de credenciais. É através dos dispositivos móveis que o militar pode acessar diversas informações e até arquivos que pertencem à unidade. Na ocasião de roubo de credenciais de acesso, as informações da empresa estarão disponíveis.

Por acidente alguém pode enviar um e-mail corporativo com informações corporativas através da conta pessoal. Devemos garantir que as informações sejam segregadas e que estas estejam em locais diferentes e não se comuniquem.

Através do dispositivo móvel é possível enviar e receber documentos, planilhas, apresentações e outros arquivos importantes. É viável evitar que elas sejam roubadas, então é necessário ter um controle de acesso. Não se pode permitir que qualquer pessoa possua acesso a essas informações. Assim, os perigos resumem-se em: roubo de credenciais, a maneira como compartilhamos informações e contatos e a misturas de informações pessoais e corporativas.

Gráfico 12 - Uso de computador pessoal na rede



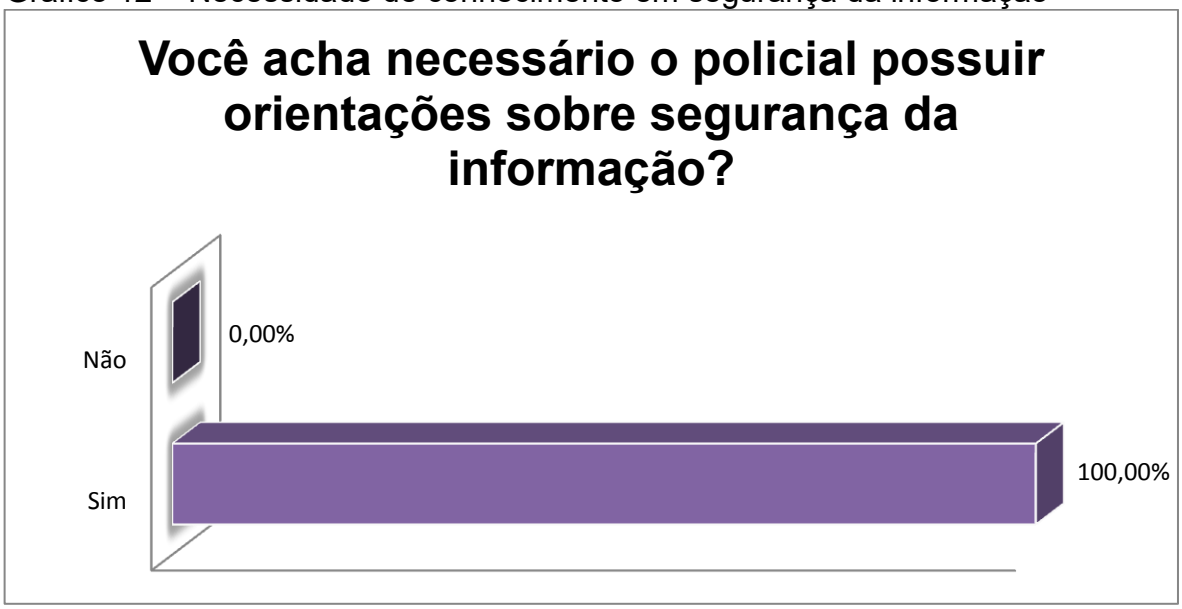
Fonte: Dados da pesquisa, (2018).

O gráfico 12 destaca um número significativo de militares que usam seus computadores pessoais na rede interna. Cerca de 44,4% responderam que “sim”, utilizam seu computador pessoal na rede interna. Isso aumenta as chances de contaminação, já que, além da possibilidade de infecção e roubo de dados e informações, os computadores pessoais podem estar com programas maliciosos com o mesmo propósito.

Há ainda a possibilidade de ataque por vírus que podem se autorreplicar em computadores através da rede. Essas infecções podem se espalhar muito rapidamente e causar altos níveis de danos na rede.

Desse modo, as recomendações detalhadas na (ISO NBR 27002, 2005) denotam a necessidade de segregar ou separar a rede em pedaços menores, denominados sub-redes. Os benefícios são diversos, tais como: melhoria de desempenho, já que, com menos *hosts* por sub-rede, haverá menos trafego e mais largura de banda usada na comunicação; melhor segurança, pois, com menos tráfego, todos os segmentos de rede dificultam a vida do atacante em mapear a infraestrutura, pois um problema em uma das segregações não se espalha para as demais partes; e por último, é possível ter um melhor controle de acesso, ou seja, podem ser estabelecidos acessos de visitantes e de computadores locais. Isso permitiria que as redes não conversassem e os dados internos da corporação seriam protegidos.

Gráfico 12 – Necessidade de conhecimento em segurança da informação



Fonte: Dados da pesquisa, (2018).

O gráfico 13 representa a necessidade de conhecimento em segurança da informação. Os dados se referem a seguinte pergunta: você acha necessário o policial possuir orientações sobre segurança da informação? A resposta foi unânime: todos os entrevistados responderam “sim” no questionário. Isso mostra que os usuários se preocupam em manter o ambiente organizacional seguro e protegido de “pragas virtuais” ou outro tipo de ameaça.

Na maioria dos ataques realizados nas organizações, os funcionários acabam sendo os responsáveis pelas falhas de segurança. Por esse motivo, é importante existir orientações e treinamentos constantes para educar os profissionais a não abrirem arquivos que possam causar problemas na organização.

As orientações podem ser estabelecidas diante das normas de uma política de segurança e através de cartilhas divulgadas nos meios digitais da corporação. Fritzen (2016) esclarece que o treinamento dos usuários é de suma importância, visto que esse tipo de ação evita a execução de códigos maliciosos, principalmente quando o usuário clica em sites suspeitos. Desta forma, fica nítida a sua importância.

Apesar disso, deve-se considerar que é necessária uma boa estrutura de segurança da Internet, com serviços de antivírus e controle de acesso, buscando orientações em empresas especializadas na área (FRITZEN, 2016).

CONSIDERAÇÕES FINAIS

Atualmente não se pode atribuir um ataque como sendo um simples vírus, uma vez que existe uma imensa quantidade de novos modos de invasões e maneiras distintas para adentrar num sistema ou roubar informações. Especialistas no assunto estão constantemente desenvolvendo formas e tecnologias para combater qualquer tipo de abuso. No entanto, devemos estar sempre atentos as ações dos criminosos, pois esses desenvolvem constantemente outras formas de ocupar os sistemas, onde seus objetivos são simplesmente os mesmos: roubar, destruir ou alterar informações. É preciso prever e combater antes de trazer problemas para a sociedade e principalmente para as instituições públicas.

A facilidade com que os usuários interagem com a Internet estimula cada vez mais os invasores no desenvolvimento de maneiras distintas e surpreendentes para confundir as pessoas. Esses crimes não são novidade. Entretanto, nas últimas décadas houve um aumento de ataques, bem como um aumento nos prejuízos.

Além dos conceitos de boas práticas no uso da Internet e avaliação do nível de conhecimentos dos militares que trabalham no QCG, o trabalho abordou também outras questões mais técnicas que norteiam o funcionamento de uma rede de computador, discorrendo sobre os crimes virtuais e as práticas mais apropriadas para assegura-se de algumas situações de risco. Mais adiante na análise, foi realizada uma pesquisa expondo pontos mais críticos e vulneráveis em que necessitam ser corrigidos o mais brevemente.

Constatou-se durante a pesquisa que as ferramentas utilizadas para proteção de equipamento são capazes de defender os ataques em que o militar não tem conhecimento. Porém, isso não é o bastante. O uso de práticas cotidianas juntamente com o cuidado diante o uso da internet são um grande apoio nesse combate.

Diante dos resultados na pesquisa, percebeu-se que os militares que trabalham no QCG possuem conhecimentos em alguns assuntos referente à segurança. Contudo, foram constatados diversos pontos de fragilidade que exigem uma atenção maior. Na maioria dos ataques realizados nas organizações, os funcionários acabam sendo os responsáveis por algumas falhas de segurança. Sendo assim, é importante existir orientações e treinamentos de maneira continuada.

A política de segurança é necessária dentro da instituição. Ela é responsável pelo planejamento e pela proteção dos ativos da informação guiada pelos três princípios básicos da segurança. Por esse motivo, são necessárias algumas estratégias que garantam os princípios somados ao conjunto de ferramentas com grau de segurança que a instituição precisa. Essas estratégias possibilitam um melhor ambiente de confiabilidade e segurança, diminuindo vulnerabilidades e possíveis ameaças. Em função disto, a segurança da informação necessita integrar a estratégia da Polícia Militar.

É necessário orientar os militares a identificar as possíveis ameaças e os riscos, criando programa e orientações sobre as vulnerabilidades e os tipos de ataques. De forma geral, todas as boas práticas em segurança indicam a necessidade de incluir os usuários no processo de segurança. Logo, assim como os sistemas físicos ou lógicos que impedem os intrusos de invadirem a rede, a conscientização é fundamental para que haja um progresso nesse aspecto. Isso reduz o sucesso dos ataques para a instituição. Assim, os militares ficaram mais atentos aos perigos, possibilitando que sejam envolvidos em treinamentos à medida que aumenta a consciência de seu papel na administração militar.

Há uma necessidade de mais segurança nas instalações de maneira geral, visto que a pesquisa mostrou a frequência das ocorrências com vírus nos computadores. Na área da informação existem diversos tipos de vírus, que infectam todos ou alguns arquivos e programas utilizados pelos usuários. Essa situação entra em desacordo com o que preconiza a instituição, já que a Polícia Militar do Maranhão é considerada uma instituição pública que trabalha com documentos públicos sigilosos.

É preciso também assegurar que as informações estejam separadas e em locais diferentes sem comunicação, de modo a não colocar em risco os dados da Polícia Militar do Maranhão por uso de informações corporativas em e-mails pessoais. Além disso, permanece a possibilidade de ataque por vírus que podem se autorreplicar através da rede. Essas infecções podem se espalhar muito rapidamente e causar danos em todo o sistema. Caso isso ocorra, é importante que os computadores sejam iniciados em modo de segurança, realizando uma varredura do sistema ou mesmo sendo averiguados por um profissional habilitado para resolver o problema.

Apesar de que exista uma parcela considerável de militares que checam a segurança de um site, a quantidade de usuários sem procedimentos em segurança é significativa. Os militares realizam diversos acessos durante o dia, enviando e-mails e registrando dados sem o devido conhecimento de que suas informações podem estar sendo interceptadas ou violadas.

As recomendações da ISO 27002 declaram diversas necessidades de separar a rede em pedaços menores, dificultando de certa maneira a vida do atacante em mapear a infraestrutura interna. É possível também ter um melhor controle de acesso estabelecido aos visitantes em uma rede diferenciada, não permitindo, assim, que as redes conversem, protegendo os dados internos da corporação.

Dessa forma, foi possível verificar a ausência de uma política de segurança consistente que estabeleça os procedimentos e o controle de acesso a sites e a sistemas. Constatou-se também a presença de riscos e vírus em sistemas operacionais nos computadores das seções administrativas da instituição, permitindo a presença de vulnerabilidade humana. O desconhecimento e a não conscientização em segurança na rede contribuem para um ambiente vulnerável. O uso de sistemas operacionais baseados em sistemas UNIX reduz de maneira expressiva diversos incidentes em segurança, tornando então a instituição mais segura e eficiente em seus trabalhos diários nas seções da corporação.

Espera-se que o presente estudo desperte o cuidado no uso da Internet, oferecendo material de apoio para elaboração e o ampliamento de estratégias para a prevenção e combate aos riscos nos erros de procedimentos por militares que trabalham no Quartel do Comando Geral da Polícia Militar do Maranhão. Este trabalho facilita também que outros estudos semelhantes sejam confeccionados a fim de evitar erros em procedimentos referentes a segurança da informação por policiais militares.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001 - Tecnologia da informação – Técnicas de Segurança. Sistemas de gestão de segurança da informação**.Rio de Janeiro. 2006.

_____Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. Rio de Janeiro. 2005.

ANONYMOUS. **Maximum Security - Hacker's Guide to Protecting Your Intemet Site and Network**. 2ª. ed. Indianapolis : SAMS Publishing, 1998.

ABREU, D. **Melhores Práticas para Classificar as Informações**. **Modulo**, 2001. Disponivel em: <http://www.modulo.com.br>. Acesso em: 21 outubro 2018.

ARNETT, M. F. et al. **Desvendando o TCP/IP**. Rio de Janeiro: Campus, 1994.

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CASTRO, C. M. **Estrutura e apresentação de publicações científicas**. São Paulo: McGraw-Hill, 1976.

CERT.BR. **Cartilha de segurança para internet**. Cartilha.cert, 2012. Disponivel em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 27 setembro 2018.

CERVO, A. L.; BERVIAN, P. A. **Metodologia científica**. 5ª. ed. São Paulo: Prentice, 2002.

COMER, D. E. **Redes de Computadores e Internet**. Porto Alegre: Bookman, 2007.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. AxcelBooks. Rio de Janeiro, 2000.

FONSECA, J. J. S. **Metodologia da Pesquisa Científica**. Fortaleza: UEC, 2002.

FRITZEN, C. E. **Importância de orientar os colaboradores para evitar problemas de segurança nas empresas**. lumiun, 2016. Disponivel em: <https://www.lumiun.com/blog/importancia-de-orientar-os-colaboradores-para-evitar-problemas-de-seguranca-nas-empresas/>. Acesso em: 15 novembro 2018.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4ª. ed. São Paulo: Atlas S.A, 2002.

_____**Métodos e Tecnicas de Pesquisa Social**. 6ª. ed. São Paulo: Atlas S.A, 2008.

GOMES, Olavo José A. **Segurança Total - Protegendo-se contra os hackers São Paulo** : Makron Books, 2000.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**. São Paulo: Pearson, 2010.

LAUDON, K.; , J. L. **Sistemas de informação gerenciais**. 9. ed. São Paulo: Pearson Prentice Hall, 2011.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. Disponível em: <http://www.scribd.com/doc/20723105/apostila-versao-20> Acesso em: 27 set. 2018.

MARCONI, M. D. A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. 5ª. ed. São Paulo: Atlas S.A, 2003.

MARTINS, E. **o que é Adware?** tecmundo, 24 set. 2008. Disponivel em: <https://www.tecmundo.com.br/spyware/271-o-que-e-adware-.htm>. Acesso em: 10 setembro 2018.

MATTAR, F. N. **Pesquisa de Marketing**. 3. ed. São Paulo: Atlas, 2011.

MAZZOLA, V. B. **Arquitetura de redes de computadores**. Santa catarina: [s.n.], 2000.

NAKAMURA, E. T. **Segurança da Informação e de Redes**. Londrina: Educaciona S.A, 2016.

OLIVEIRA, Wilson José. **Hacker Invasão e Proteção**. Florianópolis ; Visual Books, 1999.

RICHARDSON, R. J. **Pesquisa social:** Métodos e tecnicas. 3. ed. São Paulo: Atlas, 1999.

RAMOS, A. (Org.) **Security Officer 1**: guia oficial para formação de gestores em Segurança da Informação. 2 ed. Porto Alegre: Zouk, 2008.

SEGURANÇA da informação: Como foi o ataque dos sistemas de um grande banco chileno. E-commerce News, 2018. Disponivel em: <https://ecommercenews.com.br/noticias/pesquisas-noticias/seguranca-da-informacao-como-foi-o-ataque-dos-sistemas-de-um-grande-banco-chileno/>. Acesso em: 27 setembro 2018.

SÊMOLA, M. **Gestão da Segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

STOUT, R. **Dominando a world wide web**. São Paulo: Makron Books, 1997.

SILVA FILHO, Antonio Mendes Da. **Segurança da Informação**: Sobre a Necessidade de Proteção de Sistemas de Informações. Revista Espaço Acadêmico

Nº42/2004. Disponível em: < https://pt.scribd.com/document/67898900/Artigo-Seguranca-Da-Informacao> Acesso em: 27 set. 2018.

TANENBAUM, A. S. **Redes de Computadores**. Rio de Janeiro: Elsevier, 2003.

VEIGA, P. **Sociedade Portuguesa de Inovação**, 2004. Disponivel em: <http://www.spi.pt/documents/books/inovacao_autarquia/docs/Manual_III.pdf>. Acesso em: 1 outubro 2018.

VASCONCELLOS, Márcio José Acciolli de. **A Internet e os Hackers - Ataques e Defesas**. 4. ed. São Paulo; Chantal, 1999.

WADLOW, T. A. **Segurança de Redes:** Projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.

YABLOKOV, V. **Apenas metade dos dispositivos móveis em todo o mundo estão protegidos contra crimes virtuais, aponta estudo da Kaspersky Lab**. kaspersky, 2016. Disponivel em: <https://www.kaspersky.com.br/about/press-releases/2016_apenas-metade-dos-dispositivos-moveis-em-todo-o-mundo-estao-protegidos-contra-crimes-virtuais-aponta-estudo-da-kaspersky-lab>. Acesso em: 27 setembro 2018.

APÊNDICE

APÊNDICE A – QUESTIONÁRIO DESTINADO AOS POLICIAIS MILITARES DO QCG

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
DIRETORIA DE ENSINO
ACADEMIA DE POLÍCIA MILITAR "GONÇALVES DIAS"
"Escola de Comandantes, Celeiro de Líderes".
Criada pela Lei Estadual (MA) nº 5.657 de 26/04/93
Conveniada a Universidade Estadual do Maranhão – UEMA desde abril/1993
Unidade de Ensino Superior através da Lei (MA) nº 9658 de 17 de Julho 2012.

Questionário

Caros policiais militares,
Este questionário faz parte de uma pesquisa monográfica para a conclusão do Curso de Formação de Oficiais da PMMA. A referida pesquisa aborda a seguinte temática "**SEGURANÇA DIGITAL:** análise dos procedimentos em segurança da informação atrelada ao uso da internet por militares do Comando Geral na PMMA".

Favor marcar com X somente em uma única resposta que melhor se apresente para você.

Pergunta 01: Você já ouviu falar sobre segurança da informação?

SIM ( ) NÃO ( )

Pergunta 02: Você já teve acesso à política de segurança da informação do Comando Geral?

SIM ( ) NÃO ( ) Nunca ouvir falar ( )

Pergunta 03: Você já passou por algum tipo de treinamento sobre os procedimentos de segurança da informação?

SIM ( ) SIM, mas foi só uma vez ( )

NÃO ( ) SIM, mais de uma vez ( )

Pergunta 04: Você já sofreu algum tipo de ataque de vírus utilizando computador nas seções do Comando Geral?

SIM ( ) NÃO ( ) Não tenho noção ( )

Pergunta 05: Caso seja afirmativa a pergunta anterior, com qual frequência?

Uma vez ( ) 2 a 4 ( ) Mais de 4 vezes ( )

Pergunta 06: Ao navegar pela internet você se certifica se um site é seguro?
SIM ( ) NÃO ( ) Não tenho noção ( )
Pergunta 07: Ao receber um arquivo da rede você já fez a checagem da integridade daquele documento?
SIM ( ) NÃO ( ) Não tenho noção ( )
Pergunta 08: Você já enviou ou recebeu e-mail da instituição em seu e-mail pessoal?
SIM ( ) NÃO ( )
Pergunta 09: Você utiliza e-mail corporativo em *smartphones*?
SIM ( ) NÃO ( ) As vezes ( )
Pergunta 10: Você utiliza seu computador pessoal na rede interna?
SIM ( ) NÃO ( ) As vezes ( )
Pergunta 11: Você acha necessário o policial possuir orientações sobre segurança da informação?
SIM ( ) NÃO ( )