UNIVERSIDADE FEDERAL DO MARANHÃO - UFMA
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA- CCET
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO - COCOM

PAULO EDSON CUTRIM SILVA

ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO COMPLEXO DO COMANDO GERAL DA POLÍCIA MILITAR DO MARANHÃO

São Luís
2020

PAULO EDSON CUTRIM SILVA

ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO COMPLEXO DO COMANDO GERAL DA POLÍCIA MILITAR DO MARANHÃO

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Msc Carlos Eduardo Portela Serra de Castro.

São Luís

2020

Silva, Paulo Edson Cutrim.

Análise da Segurança da Informação no Complexo do Comando Geral da Polícia Militar do Maranhão / Paulo Edson Cutrim Silva – São Luís, 2020.

89 f.

Orientador: Prof. Msc. Carlos Eduardo Portela Serra de Castro.

Monografia (Graduação) – Curso de Ciência da Computação, Universidade Federal do Maranhão, Centro de Ciências Exatas e Tecnologia, 2020.

1. Segurança da Informação. 2. Crimes Virtuais. 3. Redes de Computadores. 4. Internet. I. Título.

CDD -- 355.405 (812.1)

PAULO EDSON CUTRIM SILVA

ANÁLISE DA SEGURANÇA DA INFORMAÇÃO NO COMPLEXO DO COMANDO GERAL DA POLÍCIA MILITAR DO MARANHÃO

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Msc. Carlos Eduardo Portela Serra de Castro.

Trabalho aprovado. São Luís – MA, 11 de dezembro de 2020:

BANCA EXAMINADORA

_____

Prof. Msc. Carlos Eduardo Portela Serra de Castro (Orientador)
Universidade Federal do Maranhão – UFMA

_____

Prof. Dr. Tiago Bonini Borchartt (Membro da banca)
Universidade Federal do Maranhão – UFMA

_____

Prof. Esp. Inez Cavalcanti Dantas (Membro da banca)
Universidade Federal do Maranhão – UFMA

AGRADECIMENTOS

Ao Eterno D'us de Israel, pela vida e pelo amor dado à Sua Criação.

À minha mãe Waldilene, pelo exemplo de simplicidade e persistência.

Aos meus irmãos Paulo Roberto, Priscilla e Poliana por compartilharem meus sucessos e reveses.

Aos meus tios Eliene, Reginaldo, Pedro Jorge, e meu padrasto João Pinheiro, pelas orientações.

Ao meu orientador Professor Mestre Carlos Eduardo Portela, por todo conhecimento repassado e por acreditar no meu potencial.

Ao Professor Doutor Marco Antônio Gomes, pelo compartilhamento de irrefragável conhecimento pluridisciplinar e experiência na pesquisa científica.

Aos professores da UFMA, de incomensuráveis qualificações acadêmico-pedagógicas, em especial aos críticos da banca, Inez Dantas e Tiago Bonini, da coordenadora Simara Rocha, e dos inspiradores Anselmo Cardoso, Mário Meirelles, Maria Auxiliadora, Carlos de Salles, Luciano Reis, Geraldo Braz, Mário Meireles, Marcos Rezende, João Dallyson, Francisco Glaubos, Aristófanes Correa, Francisco Silva, Maria Girardi, Alexandre Muniz e Ivo Serra.

À minha amada Gisele, pelo apoio nos bons e maus momentos.

Aos meus colegas de turma da UFMA, em especial, Igor Cavalcanti, Ramon Costa, Rafael Rani, Lucas Alves, Jouberth Borralho, Emanuel Amaral, Afonso Pinheiro, Giovanni Marinheiro, Rafael Pinheiro, Samir Souza e Laudelino Almeida, pelos momentos de descontração, inúmeros trabalhos em equipe e companheirismo.

Aos meus amigos que contribuíram direta ou indiretamente no cumprimento desta etapa. Aos gestores e técnicos administrativos da UFMA.

RESUMO

Na era do desenvolvimento tecnológico, onde as organizações buscam a informatização de processos, o papel da segurança da informação é de fundamental importância, pois ela precisa ser protegida, diante da grande quantidade de ocorrências e crimes no ambiente virtual. É imprescindível aprender sobre os conceitos relacionados às redes de computadores, internet, e segurança da informação, apresentados por especialistas e elencados nas NBR's conhecidas. Este estudo tem como objetivo principal analisar a segurança da informação no Complexo do Comando Geral da Polícia Militar do Maranhão, haja vista esta instituição ser detentora de inúmeras informações sensíveis e sigilosas, onde seus servidores necessitam obter conhecimentos relacionados ao tema, pois podem tornar-se potenciais vítimas de roubos de informações. Na coleta de dados da pesquisa, foi utilizado um questionário para mensurar o nível de conhecimento sobre segurança da informação dos policiais, uma entrevista para saber dos procedimentos e recursos utilizados pelo setor técnico e observações diretas no campo de pesquisa. A partir dessas informações, foi possível elaborar um conjunto de ações positivas a serem implementadas visando incrementar a segurança da informação na PMMA. Concluiu-se que grande parte dos profissionais precisa entender dos riscos que correm ao realizarem procedimentos inseguros na internet, e da necessidade de capacitação em Segurança da Informação. Este estudo é rico em teorias que podem ser exploradas por futuras pesquisas relacionadas ao tema.

Palavras chave: Segurança da informação. Crimes virtuais. Redes de computadores. Internet.

ABSTRACT

In the era of technological development, where organizations seek the computerization of processes, the role of information security is of fundamental importance, as it needs to be protected, given the large number of occurrences and crimes in the virtual environment. It is essential to learn about the concepts related to computer networks, internet, and information security, presented by specialists and listed in the known NBR's. This study has as main objective to analyze the information security in the Complex of the General Command of the Military Police of Maranhão, considering that this institution has innumerable sensitive and confidential information, where its servants need to obtain knowledge related to the theme, because they can become potential victims of information theft. In the collection of research data, a questionnaire was used to measure the level of knowledge about police information security, an interview to learn about the procedures and resources used by the technical sector and direct observations in the research field. Based on this information, it was possible to develop a set of positive actions to be implemented in order to increase the security of information in the PMMA. It was concluded that most professionals need to understand the risks they take when performing unsafe procedures on the internet, and the need for training in Information Security. This study is rich in theories that can be explored by future research related to the topic.

Key words: Information security. Virtual crimes. Computer networks. Internet.

LISTA DE GRÁFICOS

Gráfico 01 – Conhecimento sobre Segurança da Informação 56
Gráfico 02 – Treinamento em Segurança da Informação 56
Gráfico 03 – Backup de arquivos 57
Gráfico 04 – Segurança nas redes Wi-Fi 58
Gráfico 05 – Uso de antivírus 59
Gráfico 06 – Logon / Login em computador utilizando senha para acesso 60
Gráfico 07 – Utilização de e-mail para atividades administrativas 61
Gráfico 08 – Estado de Switches e Roteadores no ambiente de trabalho 62

LISTA DE FIGURAS

Figura 01 – Camadas e protocolos 17
Figura 02 – Protocolo Humano / TCP 18
Figura 03 – Esquema de funcionamento do protocolo SMTP 24
Figura 04 – Ciclo de Vida da Informação 32
Figura 05 – Gráfico de incidentes reportados ao CERT.br por ano 36
Figura 06 – Infográfico de ataques reportados ao CERT.br no ano de 2019 43
Figura 07 – Visual Geral na Segurança da Informação 46
Figura 08 – Comparativo entre as versões Grátis e Pagas do Antivírus Avast 60
Figura 09 – Vista aérea do Complexo do Comando Geral (CCG). 83
Figura 10 – Fachada do Complexo do Comando Geral A 83
Figura 11 – Fachada do Complexo do Comando Geral B 83
Figura 12 – Fachada do Complexo do Comando Geral C 84
Figura 13 – Fachada do Complexo do Comando Geral D 84
Figura 14 – Curral do Regimento de Polícia Montada 84
Figura 15 – Sede do Regimento de Polícia Montada 84
Figura 16 – Lateral Esquerda do QCG A 85
Figura 17 – Lateral Esquerda do QCG B 85
Figura 18 – Livro para cadastro de visitantes APMGD 85
Figura 19 – Sistema de Videomonitoramento APMGD 85
Figura 20 – Fachada 8º BPM 86
Figura 21 – Sistema de videomonitoramento 8º BPM 86
Figura 22 – Switch de rede com rack no 8º BPM 86
Figura 23 – Switch com função Wi-Fi na Diretoria de Pessoal, sem rack 86
Figura 24 – Roteador armazenado em rack 87
Figura 25 – Roteador Wi-Fi com Switch, exposto 87
Figura 26 – Acesso único para carga e descarga 87
Figura 27 – Acesso restrito credenciado 87

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APMGD	Academia de Polícia Militar Gonçalves Dias
BPM	Batalhão de Polícia Militar
CCG	Complexo do Comando Geral
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CF	Constituição Federal
DGTI	Diretoria de Gestão da Tecnologia da Informação
DNS	*Domain Name System*
IP	Protocolo de internet
ISO	*International Organization for Standardization*
ISP	*Internet Service Provider*
LAN	*Local Area Network*
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Medida Provisória
NBR	Norma Brasileira Regulamentadora
PM	Polícia Militar
PMMA	Polícia Militar do Maranhão
SGSI	Sistema de Gestão da Segurança da Informação
SI	Segurança da Informação
TI	Tecnologia da Informação
URL	*Uniform Resource Locator*
Wi-Fi	*Wireless Fidelity* (Rede sem fio)

SUMÁRIO

LISTA DE GRÁFICOS 06
LISTA DE FIGURAS 07
LISTA DE SIGLAS 08
1 INTRODUÇÃO 11
1.1 Objetivos 12
1.2 Organização do Estudo 13
2 CONCEITOS DE REDES DE COMPUTADORES 14
2.1 Conceitos básicos 14
2.2 Protocolos de comunicação e serviços de Rede 16
2.3 Principais Topologias 19
2.3.1 Ponto a ponto 20
2.3.2 Estrela 20
2.4 Redes locais e Redes de longa distância 21
2.5 A Internet 22
3 SEGURANÇA DE REDES 24
3.1 Segurança de Correio Eletrônico 24
3.2 Segurança em LANs sem fio 26
3.3 *Firewalls* 27
4 O CONTEXTO DA SEGURANÇA DA INFORMAÇÃO 29
4.1 *Hacker x Cracker* 29
4.2 Princípios de Segurança da Informação 30
4.3 A informação e seu ciclo de vida 31
4.4 Mecanismos de Segurança 32
4.4.1 Normas e políticas de Segurança 33
4.4.2 Criptografia 36
4.4.3 Assinaturas digitais e certificado digital 38
4.4.4 Ferramentas *antimalware* 39
4.4.5 Filtro *antispam* 39
4.5 Ataques e incidentes 41
4.5.1 *Adware* 44
4.5.2 *Backdoor* 44
4.5.3 Cavalo de Tróia 44

4.5.4 *Rootkit* 45
4.5.5 *Spyware* 45
4.5.6 *Worm* 45
4.6 Ameaças, vulnerabilidades e riscos 45
4.6.1 *Smartphones* 47
4.6.2 *Phishing* 48
4.7 Sistemas Operacionais Linux 48
4.8 Crimes Virtuais 49
5 METODOLOGIA 52
5.1 Métodos Utilizados 52
5.2 Detalhamento da Pesquisa 53
5.3 Etapas da pesquisa 54
5.4 Pesquisa de Campo 54
6 ANÁLISE DOS RESULTADOS 56
6.1 Questionário 56
6.2 Entrevista 63
6.3 Observação Direta Intensiva 68
6.3.1 Pontos positivos observados 68
6.3.2 Recomendações a serem implementadas 69
7 CONSIDERAÇÕES FINAIS 72
REFERÊNCIAS 73
APÊNDICES 78
ANEXOS 82

1 INTRODUÇÃO

O avanço tecnológico e o grande fluxo de informações repassadas numa velocidade espantosa têm gerado mudanças significativas na dinâmica da sociedade moderna. O novo cenário socioeconômico proporciona ao mundo profundas transformações, propondo um novo modelo de sociedade que, se por um lado, apresenta avanços científicos e tecnológicos, por outro, gera riscos com a exposição de informações e aumento de crimes com a utilização do ambiente virtual.

Para Laudon e Laudon (2014, p. 12), "Por tecnologia da informação (TI), entenda-se todo software e todo hardware de que uma empresa necessita para atingir seus objetivos organizacionais". Desta forma, quando se fala do emprego da TI nas organizações, não se restringe apenas ao hardware utilizado (computadores e mídias), mas também aos softwares (sistemas operacionais e programas computacionais).

Boa parte das rotinas administrativas passou a utilizar ferramentas computacionais para agilidade e automatização de processos, aumentando a quantidade de arquivos produzidos no meio virtual e, consequentemente, a necessidade de proteção desses arquivos, para que estejam disponíveis e seguros dentro do ambiente virtual.

Desta forma, com o aumento da informatização dessas atividades e processos, que antes eram realizadas de forma manual, bem como a maior quantidade de acesso à internet, proporcionalmente, houve também o aumento na quantidade de incidentes relacionados a fraudes e demais crimes praticados no ambiente virtual.

São várias as técnicas empregadas por pessoas mal intencionadas no intuito de obter informações sigilosas de forma ilícita. A análise da segurança da informação se faz necessária dentro de uma instituição e, neste estudo especificamente, dentro do ambiente do CCG da PMMA, pois é responsável pela coleta de diversas informações necessárias para o combate da criminalidade dentro do Estado do Maranhão.

Para Beal (2005), a prática disseminada para a preservação da segurança deve ser orientada através de políticas de segurança da informação, onde os usuários devem ser os principais envolvidos nesse processo de conscientização.

Assim, observa-se a necessidade de adotar medidas que evitem a exposição de informações institucionais que possam ser utilizadas para a prática de crimes ou para beneficiar pessoas mal intencionadas, haja vista que inúmeras tarefas são realizadas através do ambiente virtual, como transações bancárias, compras, armazenamento de arquivos pessoais e envio de documentos sigilosos.

Diante do cenário exposto, esse estudo visa responder ao seguinte problema: de que forma pode-se aumentar a segurança da informação no Complexo do Comando Geral da Polícia Militar do Maranhão, diminuindo os riscos ao qual a instituição e seus membros estão sendo expostos.

A PMMA é uma Instituição de Segurança responsável pela preservação da Ordem Pública, detentora de informações sigilosas que são utilizadas diariamente na tomada de decisões para o combate à criminalidade, sendo necessário adotar medidas para aumento da segurança da informação, visando à salvaguarda de dados e pessoas. Informações como endereço de policiais, quantidade de efetivo das unidades, tipo de armas empregadas, quantidade de viaturas por município, ordem de operações e planejamentos podem ser utilizadas para o cometimento de inúmeros delitos, caso sejam adquiridas por pessoas mal intencionadas.

É importante ressaltar que se trata de uma pesquisa aplicada em uma instituição pública, que se baseia nos princípios do direito administrativo, em especial, ao princípio da transparência, onde a Administração Pública tem a obrigação de dar ampla divulgação dos atos que pratica, salvo nos casos em que possa ameaçar a segurança da sociedade ou do Estado, conforme artigo 5º, XXXIII da Constituição Federal Brasileira. Por outro lado, o princípio da eficiência, reforça a importância desse estudo, uma vez que irá propor medidas mais eficientes para o tratamento das informações e consequente ganho em qualidade nas rotinas administrativas, haja vista que a Administração Pública tem o dever proporcionar melhores resultados possíveis com o menor ônus possível.

1.1 Objetivos

O objetivo geral deste estudo é analisar a segurança da informação no CCG da PMMA.

Como objetivos específicos:

- Apresentar os conceitos de redes, internet e segurança da informação, conforme a literatura;
- Relacionar as principais formas de ataques e como preveni-las no CCG da PMMA;
- Apresentar soluções para neutralizar ou atenuar os riscos identificados no CCG da PMMA.

1.2 Organização do Estudo

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

No segundo capítulo é apresentado o embasamento teórico do estudo, abordando os pressupostos das redes de computadores. Nessa parte será explicado sobre 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, além do surgimento e funcionamento da internet.

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

O quarto capítulo 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 quanto dos humanos) a tais investidas, os incidentes envolvendo o uso da internet e informações sobre o Linux. Neste capítulo também é citado um tópico especial que trata sobre os crimes virtuais ou crimes de internet, conceitos e exemplos.

O quinto capítulo é referente à metodologia utilizada no estudo, 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 Comando Geral da PMMA. Além disso, uma entrevista ao setor técnico será realizada.

O sexto capítulo diz respeito à análise dos resultados obtidos na pesquisa, com a elaboração de gráficos e comentários acerca de cada informação, associando sempre com a literatura e norma técnica vigente.

Por fim, no último capítulo será apresentada uma breve retrospectiva do estudo, e conclusões alcançadas com base nos objetivos propostos, para colaboração em estudos futuros.

2 CONCEITOS DE REDES DE COMPUTADORES

A finalidade deste capítulo é abordar o surgimento e evolução das redes, explicando o seu funcionamento e protocolos.

2.1 Conceitos básicos

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, 2014).

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 obtenção 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 às necessidades emergentes. 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 Tanenbaum e Wetherall (2011, p. 277) "Cada host e roteador na Internet tem um endereço IP que pode ser usado nos campos Endereço de origem e Endereço de destino dos pacotes IP".

Qualquer dispositivo host ligado à internet, independentemente de sua natureza, necessitará possuir um endereço IP. Esse acesso é realizado por meio de uma *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 Tanenbaum e Wetherall (2011, p. 38):

> Para entrar na Internet, o computador é conectado a um provedor de serviço de Internet, ou ISP (*Internet Service Provider*), de quem o usuário compra acesso à Internet ou conectividade. Com isso, o computador pode trocar pacotes com todos os outros hosts acessíveis na Internet. O usuário pode enviar pacotes para navegar pela Web ou para qualquer um dos milhares de outros usos.

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.

Para Alencar (2010), o *Domain Name System* (DNS), cuja tradução significa "sistema de nomes de domínios", tem como principal função associar o IP a um nome, um caminho a uma rede associada na internet. Assim, os dispositivos utilizam o serviço DNS para efetuar consultas e localizar o endereço IP dos computadores (hosts) ao qual precisam se conectar.

Desta forma, como existe a necessidade de acessar aos conteúdos da web através de um número IP, utiliza-se o DNS para uma melhor memorização, possibilitando traduzir um endereço. Como exemplo, vejamos o site da Universidade Estadual do Maranhão, cujo IP do servidor web é 45.71.6.11. Com a utilização do serviço DNS, basta digitar o endereço "www.uema.br" para acessar a página.

Sobre o DNS, cita Kurose e Ross (2013, p. 95):

> [...] assim como os seres humanos podem ser identificados de muitas maneiras, exatamente acontece com os hospedeiros da internet. Um identificador é seu nome de hospedeiro (*hostname*). Nomes de hospedeiro como cnn.com (...) são fáceis de lembrar e, portanto, apreciados pelos seres humanos.

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. Cada página recebe um URL específico, que efetivamente serve como o nome mundial da página. Para Tanenbaum e Wetherall (2011, p. 409) "Os URLs têm três partes: o protocolo (também conhecido como o

esquema), o nome DNS da máquina em que a página está localizada e o caminho que identifica exclusivamente a página específica".

Diante do crescimento gradual da internet e sua utilização pelos mais diversos setores da sociedade, normas para acesso foram estabelecidas, no intuito de regular as condutas nesse ambiente virtual. Assim, segundo Coelho e Araújo (2013, p. 2) "[...] a segurança da informação é determinante para assegurar competitividade, lucratividade, atendimento aos requisitos legais e a imagem da organização junto ao mercado, às organizações, tanto no setor público quanto no setor privado".

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 Kurose e Ross (2013, p.6):

> Um protocolo de rede é semelhante a um protocolo humano; a única diferença é que as entidades que trocam mensagens e realizam ações são componentes de hardware ou software de algum dispositivo (por exemplo, computador, smartphone, tablet, roteador ou outro equipamento habilitado para rede). Todas as atividades na Internet que envolvem duas ou mais entidades remotas comunicantes são governadas por um protocolo.

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.

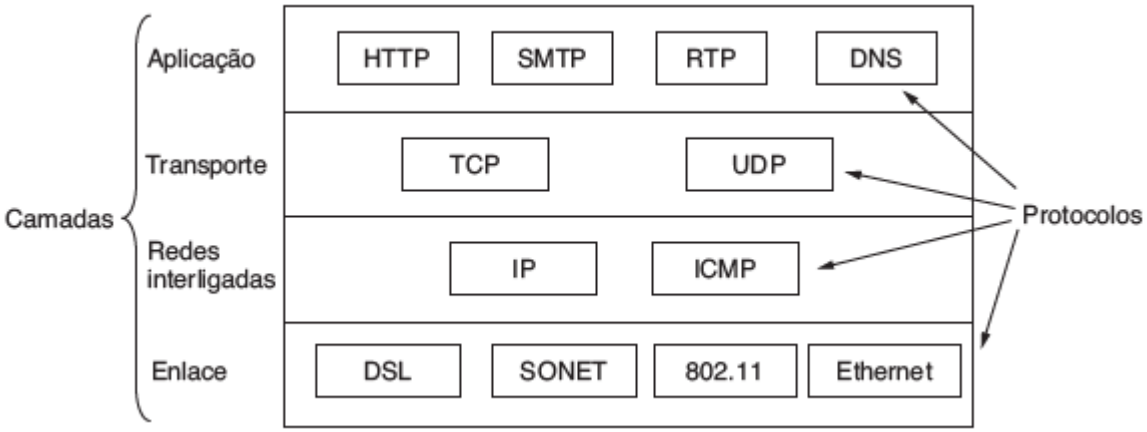
Um serviço de rede pode ser definido como um conjunto de serviços oferecidos pela rede através de uma interface e cedido logo após a camada imediatamente superior, como explica Tanenbaum e Wetherall (2011, p. 29):

> 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 da Figura 01 que mostra o conjunto de protocolos na camada de aplicação, transporte e de enlace.

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.

Figura 01: Camadas e Protocolos.



Fonte: Tanenbaum e Wetherall (2011, p. 29)

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 e Wetherall (2011, p. 22) relata 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.

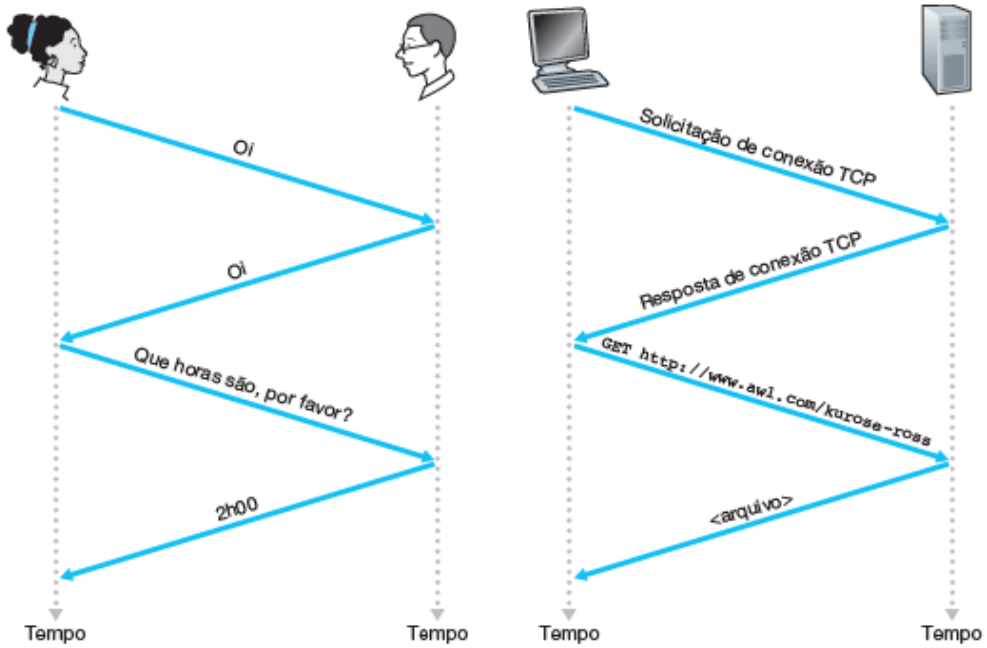
A família *Transmission Control Protocol* (TCP) é orientada à conexão na medida em que os serviços relacionados ao protocolo são ao contrário, não disponibilizando de orientação à conexão.

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.

A Figura 02 relaciona um protocolo da comunicação humana com um protocolo de rede (TCP):

Figura 02: Protocolo humano / TCP.



Fonte: Kurose e Ross (2013, p. 6).

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.

O *User Datagram Protocol* (UDP) é um protocolo não orientado à conexão, como Tanenbaum e Wetherall (2011, p. 29) pontua:

> [...] o protocolo de datagrama do usuário, ou UDP (*User Datagram Protocol*), é um protocolo sem conexões, não confiável, para aplicações que não desejam a sequência ou o controle de fluxo do TCP, e que desejam oferecer seu próprio controle. Ele é muito usado para consultas isoladas, com solicitação e resposta, tipo cliente-servidor, e aplicações em que a entrega imediata é mais importante do que a entrega precisa, como na transmissão de voz ou vídeo.

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 constate 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.

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 Alencar (2010, p. 20): “Podemos dizer que a topologia física de uma rede local compreende os enlaces físicos de ligação dos elementos computacionais da rede [...]”. 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. “[...] a topologia lógica da rede se refere à forma através da qual o sinal é efetivamente transmitido entre um computador e outro” (ALENCAR, 2010, p. 20).

2.3.1 Ponto a ponto

O *Peer-to-peer* (P2P), ou “ponto-a-ponto”, segundo sua tradução, é uma arquitetura das redes de computadores responsável por ligar dois pontos sem a necessidade de equipamentos de serviço central, onde os hosts envolvidos desenvolvem funções ora de clientes ora de servidores. Seu funcionamento parte do princípio de permitir o compartilhamento de dados ou serviços, sendo utilizadas popularmente no compartilhamento de músicas, vídeos ou outros arquivos.

Segundo Mazzola (2000, p. 1.3), “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.

Alencar (2010, p. 21), relata que “A topologia em estrela utiliza um periférico concentrador, normalmente um hub, interligando todas as máquinas da rede”.

Esse ponto central gerencia o fluxo de dados da rede. Todas as informações trafegam pela rede, de equipamento para equipamento, através de nós, 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 Tanenbaum e Wetherall (2011, p.12):

> Uma LAN é uma rede particular que opera dentro e próximo de um único prédio, como uma residência, um escritório ou uma fábrica. As LANs são muito usadas para conectar computadores pessoais e aparelhos eletrônicos, para permitir que compartilhem recursos (como impressoras) e troquem informações.

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. Tanenbaum e Wetherall (2011, p.14), sobre as MANs, ainda relata que:

> Esses sistemas cresceram 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, Tanenbaum e Wetherall (2011, p. 14) pontua que "[...] nesse momento, o sistema de TV a cabo começou a se transformar, passando de uma forma de distribuição de televisão para uma rede metropolitana".

Já 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. 1.2-1.3): "[...] 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 distribuída".

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. Foi criada em 1969, nos Estados Unidos com nomenclatura ARPANET, e como função, interligar laboratórios de pesquisa. Essa rede pertencia ao Departamento de Defesa dos Estados Unidos da América, conforme consta na matéria de Silva (2011), da Folha UOL.

Corroborando com esta afirmativa, Boniati e Silva (2013) 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.

Segundo Boniati e Silva (2013, p. 15) "Em meados de 1962, os Estados Unidos criaram a Cadeia de Comunicação Distribuída (CCD), que era composta por vários computadores interligados por várias linhas telefônicas diferentes". A ideia inicial era poder dividir as informações em partes menores entre os computadores a partir de diferentes linhas telefônicas, os computadores conhecidos nas redes como hosts e a divisão das informações como pacotes. Desta forma, se fosse perdida a conexão com uma linha, outras linhas estariam disponíveis para dar continuidade à transmissão.

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, na década de 60 ela estava situada em 17 locais diferentes nos quais computadores conectados às linhas telefônicas conseguiam estabelecer e trocar informações, com uso exclusivamente militar (BONIATI e SILVA, 2013).

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.

> De 1969 a 1972, foi criada a ARPANET, o embrião da Internet que conhecemos hoje. A rede entrou no ar em dezembro de 1969, inicialmente, com apenas quatro nós, que respondiam pelos nomes SRI, UCLA, UCSB e UTAH e eram sediados, respectivamente, no Stanford Research Institute, na Universidade da Califórnia, na Universidade de Santa Barbara e na Universidade de Utah, todas elas nos EUA. Eles eram interligados através de links de 50 kbps, criados usando linhas telefônicas dedicadas, adaptadas para o uso como link de dados (MORIMOTO, 2008b, [não paginado]).

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. Como explica Morimoto (2008b, [não paginado]):

> Em 1974, surgiu o TCP/IP, que se tornou o protocolo definitivo para uso na ARPANET e, mais tarde, na internet. Uma rede interligando diversas universidades permitiu o livre tráfego de informações, levando ao desenvolvimento de recursos que usamos até hoje, como o e-mail, o telnet e o FTP, que permitiam aos usuários conectados trocar informações, acessar outros computadores remotamente e compartilhar arquivos. Na época, mainframes com um bom poder de processamento eram raros e incrivelmente caros, de forma que eles acabavam sendo compartilhados entre diversos pesquisadores e técnicos, que podiam estar situados em qualquer ponto da rede.

Quando nos referimos à internet, estamos nos reportando à grande rede de dispositivos conectados utilizando um conjunto próprio de protocolos. Assim, para Tanenbaum e Wetherall (2011, p.33), "[...] 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 será abordada a segurança no correio eletrônico, segurança em LANs sem fio e funcionalidades dos *firewalls*.

3.1 Segurança de Correio Eletrônico

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 física do remetente e do destinatário.

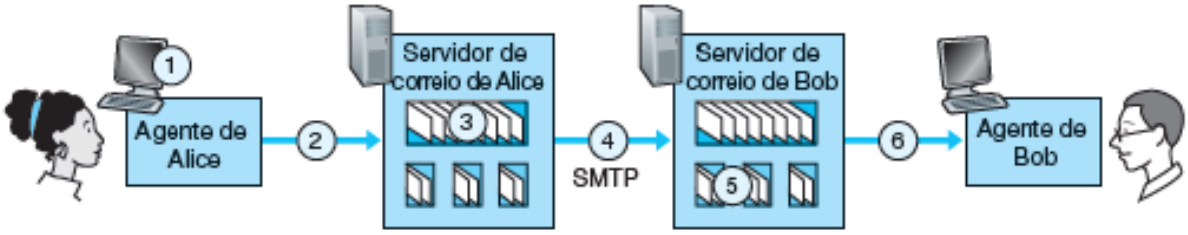
Para melhor entendimento podemos comparar ao sistema de correios tradicional, onde as correspondências enviadas por um remetente a um destinatário tão somente serão lidas se nos dirigirmos até a agência de correio e retirarmos o material (considerando a inexistência do carteiro).

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 consultURAa, no respectivo servidor, a existência ou não de mensagens. Se existirem, as mesmas são apresentadas ao destinatário na forma como foram concebidas.

Para Kurose e Ross (2013), o protocolo mais utilizado para serviços de correio eletrônico na internet é o *Simple Mail Transfer Protocol* (SMTP), e utiliza o protocolo TCP da camada de transporte para uma transmissão de dados confiável entre os servidores de correio do remetente e destinatário.

Figura 03: esquema de funcionamento do protocolo SMTP



Fonte: Kurose e Ross (2013, p. 90).

O correio eletrônico se tornou uma ferramenta computacional para comunicação quase indispensável nas organizações, devido às facilidades proporcionadas pelo meio digital, como rapidez e comodidade para transmissão das informações. A respeito da importância do e-mail como ferramenta de trabalho, Tanenbaum e Wetherall (2011, p.3) desenvolvem:

> 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 comuns 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.

Sobre essas ameaças Kurose e Ross (2013, p. 41) discorre:

> Conectamos aparelhos à Internet porque queremos receber/enviar dados de/para a rede. Isso inclui todos os tipos de recursos vantajosos, como páginas da Web, mensagens de e-mail, MP3, chamadas telefônicas, vídeo em tempo real, resultados de mecanismo de busca etc. Porém, infelizmente, junto com esses recursos vantajosos aparecem os maliciosos — conhecidos de modo coletivo como malware — que também podem entrar e infectar nossos aparelhos.

Portanto, apesar das vantagens apresentadas pelo serviço de correio eletrônico, é necessário o mínimo de conhecimento sobre os riscos oferecidos pelo ambiente virtual.

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.

Kurose e Ross (2013, p. 389), discorrem sobre as LANs sem fio:

> Presentes no local de trabalho, em casa, em instituições educacionais, em cafés, aeroportos e esquinas, as LANs sem fio agora são uma das mais importantes tecnologias de rede de acesso na Internet de hoje. Embora muitas tecnologias e padrões para LANs sem fio tenham sido desenvolvidos na década de 1990, uma classe particular de padrões surgiu claramente como a vencedora: a LAN sem fio IEEE 802.11, também conhecida como Wi-Fi.

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, pessoas com bons conhecimentos em redes podem interceptar as informações que são transmitidas por este meio. Assim, no intuito de aumentar a proteção na transmissão dos dados, o padrão 802.11 (*Wi-Fi*), traz alguns dos principais protocolos de criptografia: o *Wired Equivalent Privacy* (WEP), o *Wi-fi Protected Access* (WPA) e o WPA2.

Diversos roteadores dispõem de opções para utilização de proteção através de senha, tais como *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 comprometer a segurança na transmissão dos dados.

Sobre os conceitos acima, Tanenbaum e Wetherall (2011, p. 45), mostra que:

> Como as transmissões sem fio são feitas por radiodifusão, é fácil que computadores vizinhos recebam pacotes de informações que não foram solicitados por eles. Para evitar isso, o padrão 802.11 incluiu um esquema de encriptação conhecido como WEP (Wired Equivalent Privacy). A ideia foi tornar a segurança da rede sem fios semelhante à segurança da rede cabeada. Essa é uma boa ideia, mas infelizmente o esquema tinha falhas e logo foi quebrado. Desde então, ele foi substituído por esquemas mais recentes, que possuem diferentes detalhes criptográficos no padrão 802.11i, também chamado WiFi Protected Access, inicialmente WPA e depois substituído pelo WPA2.

Desta forma, com o passar do tempo e avanço nas técnicas para interceptação de dados (invasão), foi necessário incrementar mudanças nos algoritmos de criptografia, a fim de dar mais segurança nos protocolos de segurança do padrão 802.11. 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 tão seguro e encontra-se ultrapassado. Porém, o AES é um protocolo mais seguro, tendo como ponto fraco o ataque de força bruta, segundo matéria de Brito (2017), da página Techtudo.

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. É menos seguro, mas é uma solução de conexão opcional.

Segundo Paim (2011), a criptografia 802.1X, com modo EAP (protocolo de autenticação estendível), utiliza o controle de acesso à rede através de portas, possibilitando ao administrador da rede adicionar o acesso à rede através de um usuário e senha, e assim, proporcionar um incremento na segurança da rede.

3.3 *Firewalls*

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

Segundo Tanenbaum e Wetherall (2011, 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 (2013, p.538) 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 e Wetherall (2011, 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 (2013, p.539), “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

A aplicação de conceitos de segurança da informação dentro do ambiente de trabalho é de suma importância, pois na de tecnologia, não existem instituições com risco zero, mas sim, procedimentos e técnicas que visam diminuir esses riscos. Assim como explica Coelho e Araújo (2013, p. 2):

> Segundo a norma ABNT NBR ISO/IEC 27002:2005, a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

Na utilização da Internet, as estações de trabalho são demasiadamente expostas aos perigos virtuais. Durante as atividades diárias são armazenadas senhas pessoais, informações dos usuários e das organizações, na maioria das vezes, sem a devida proteção ou filtros. Usuários mal orientados com relação à segurança da informação se tornam potenciais vítimas em ações delituosas, através do ambiente virtual. Esses locais estão sujeitos à execução de programas desconhecidos, permitindo que fiquem expostos a vírus e outras tecnologias de invasão que possibilitam ter acesso não autorizado a arquivos e sistemas.

4.1 *Hacker x Cracker*

Dentro da Tecnologia da Informação, inúmeras expressões podem denominar os usuários de computador, conhecidos como *peopleware,* tais como engenheiros da computação, analista de sistemas, analista de banco de dados, programadores, técnicos de manutenção, etc. Mais especificamente, dentro dos conceitos de segurança da informação, dois personagens se destacam pela habilidade em detecção de falhas e infiltrações: os *hackers* e os *crackers*. Existe uma diferença nestes termos, conforme cita Tanenbaum e Wetherall (2011, p. 530), "A imprensa popular chama as pessoas que invadem computadores de 'hackers', mas muitos programadores reservam esse termo para os ótimos programadores. Preferimos chamar esses invasores de 'crackers'".

Barreto e Brasil (2016, p. 29) destacam essa diferença:

> No ambiente virtual devem ser bem distinguidas duas figuras: as dos hackers, que possuem grande conhecimento de informática e segurança de redes, utilizando-o para proteção e em defesa dos menos favorecidos, também conhecidos como *white hats* (chapéus brancos), e a dos crackers ou *black hats* (chapéus pretos), os quais utilizam seus conhecimentos para práticas criminosas ou antiéticas.

O termo hacker é mal interpretado por muitas pessoas sem informação que julgam como sendo aquele indivíduo que destrói computadores, sistemas, arquivos tomando o controle do computador. Esse conceito foi criado, em parte, pelo marketing gerado pela indústria cinematográfica. 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. Barreto e Brasil (2016) afirmam que o maior objetivo dos criminosos virtuais é de ordem financeira, e utilizam-se do suposto anonimato proporcionado pelo ambiente virtual para a prática dos crimes.

4.2 Princípios da Segurança da Informação

O conceito de segurança da informação surge da necessidade de proteção dos dados das pessoas e organizações, que possam resultar em prejuízos das diversas formas (econômico, moral, psicológico, cultural, etc.). Desta forma, inúmeras técnicas foram criadas para diminuir os riscos de invasão a sistemas e para evitar esses prejuízos.

Para Coelho e Araújo (2013, p. 2):

> Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

A Associação Brasileira de Normas Técnicas (ABNT), através da Norma Brasileira (NBR) ISO (*International Organization for Standardization*) 27002:2013 adiciona que a segurança da informação visa proteger a informação de ameaças diversas, para garantir a continuidade do negócio, maximizando o retorno sobre os investimentos e diminuindo riscos. 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.

Já Campos (2007, p.17) complementa que "um sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade." Assim, é necessário esclarecer esses conceitos com maior riqueza de detalhes.

A confidencialidade remete a garantia de que uma informação será acessada ou disponibilizada somente por pessoas autorizadas (NBR ISO/IEC 27002:2013). 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.

Também sobre a confidencialidade citam Coelho e Araújo (2013, p. 6) que "compreende a proteção de dados transmitidos contra ataques passivos, isto é, contra acessos não autorizados, envolvendo medidas como controle de acesso e criptografia.".

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, 2013). Ocorre quebra da integridade quando existe a falsificação. Garantir a integridade é permitir que a condição da informação original permanecesse íntegra.

Por fim, sobre a disponibilidade, Coelho e Araújo (2013, p. 7) dizem que ela "determina que recursos estejam disponíveis para acesso por entidades autorizadas, sempre que solicitados, representando a proteção contra perdas ou degradações". Assim, garantir a disponibilidade é assegurar o êxito no acesso ao conteúdo da informação, possibilitando a leitura e o armazenamento dela sempre que necessário.

Outra quarta característica também citada na literatura, diz respeito à autenticidade, que serve para mensurar o nível de confiabilidade de uma fonte. Para Campos (2007) a autenticidade garante a idoneidade da fonte, ou seja, quando esta é digna e de confiança.

4.3 A informação e seu ciclo de vida

Na sociedade da informação, o principal patrimônio da empresa são seus dados, registros e conhecimentos. Os dados reunidos se transformam em conhecimento útil para uma organização, influenciando na tomada de decisões e negócios, essenciais dentro de um planejamento estratégico. Os Sistemas de Informação são essenciais para sobrevivência das empresas nos dias atuais, como cita Laudon e Laudon (2014, p. 75):

> Os sistemas de informação apoiam o setor estratégico, ao produzir dados que permitem técnicas de venda e de marketing perfeitamente afinadas. Esses sistemas tratam a informação como uma mina de recursos que a organização pode explorar para aumentar a lucratividade e a penetração no mercado.

Segundo Sêmola (2003), a informação compreende um ciclo de vida. O início do ciclo começa a partir da sua produção, depois sendo manuseada por diversos agentes, transportada, armazenada, e por fim destruída. É basicamente assim que funciona o ciclo de sua existência. A Figura 04 a seguir mostra o ciclo de vida da informação:

Figura 04 – Ciclo de Vida da Informação

Fonte: Sêmola (2003, p. 11), adaptado.

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 estudo 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 segurança da informação (SI), as instituições buscaram uma boa estruturação a fim de garantir que suas atividades estejam protegidas contra diversos tipos de ameaças virtuais.

Em meios a esse problema, foram criadas as normas internacionais NBR ISO/IEC 27001 e NBR ISO/IEC 27002, que estabelecem padrões para sistemas de gestão e concentram boas práticas à gestão da segurança da informação respectivamente, sendo fundamentais para a consolidação de um Sistema de Gestão de Segurança da Informação (SGSI).

Pandini (2015) relata que 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. Essas normas podem 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 da 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 tratando sobre a Política de Segurança da Informação, ou seja, a criação de um documento que deve prover diretrizes para implantação de uma política de segurança da informação num ambiente, levando em conta os requisitos do negócio e outras normais gerais em vigência (NBR ISO/IEC 27002, 2013).

Já na seção 6 se estabelece a Organização da Segurança da Informação, que cuida de fazer a implementação da 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, 2013).

A seção 7 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, além de regras de recrutamento e seleção de candidatos (NBR ISO/IEC 27002, 2013).

A seção 8 refere-se à 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, 2013).

Na seção 9 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, 2013).

A seção 10 trata sobre a Criptografia, cujo objetivo é assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e a integridade da informação. (NBR ISO/IEC 27002, 2013).

A seção 11 é responsável pela Segurança Física e do Ambiente, prevendo medidas que visam restringir o acesso físico de pessoas não autorizadas a locais específicos e assegurar a instalação de equipamentos que processam informações sensíveis em locais seguros, e definição de níveis de controles apropriados contra ameaças (NBR ISO/IEC 27002, 2013).

A seção 12 é encarregada de zelar pela Segurança nas operações, cujo objetivo é garantir a correta aplicação dos recursos para processamento das informações, tais como documentação de procedimentos, monitoramento de ações para elaboração de relatórios, definição de ambientes de desenvolvimento, teste e produção, etc. (NBR ISO/IEC 27002, 2013).

A seção 13 é encarregada de zelar pela Segurança nas Comunicações, tais como segurança nos serviços de rede, transferências seguras das informações através de meio telemático, integridade e confiabilidade de mensagens eletrônicas, etc. (NBR ISO/IEC 27002, 2013).

Por fim, a seção 14 refere-se à 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, 2013).

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 (2005, 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.

Através deste conceito, observa-se que o principal objetivo de implantar uma política de SI numa organização é a proteção das informações. A legislação existente é necessária para que haja um padrão nas condutas, objetivando padrões de segurança satisfatórios e o menor impacto no desempenho dos processos de negócio.

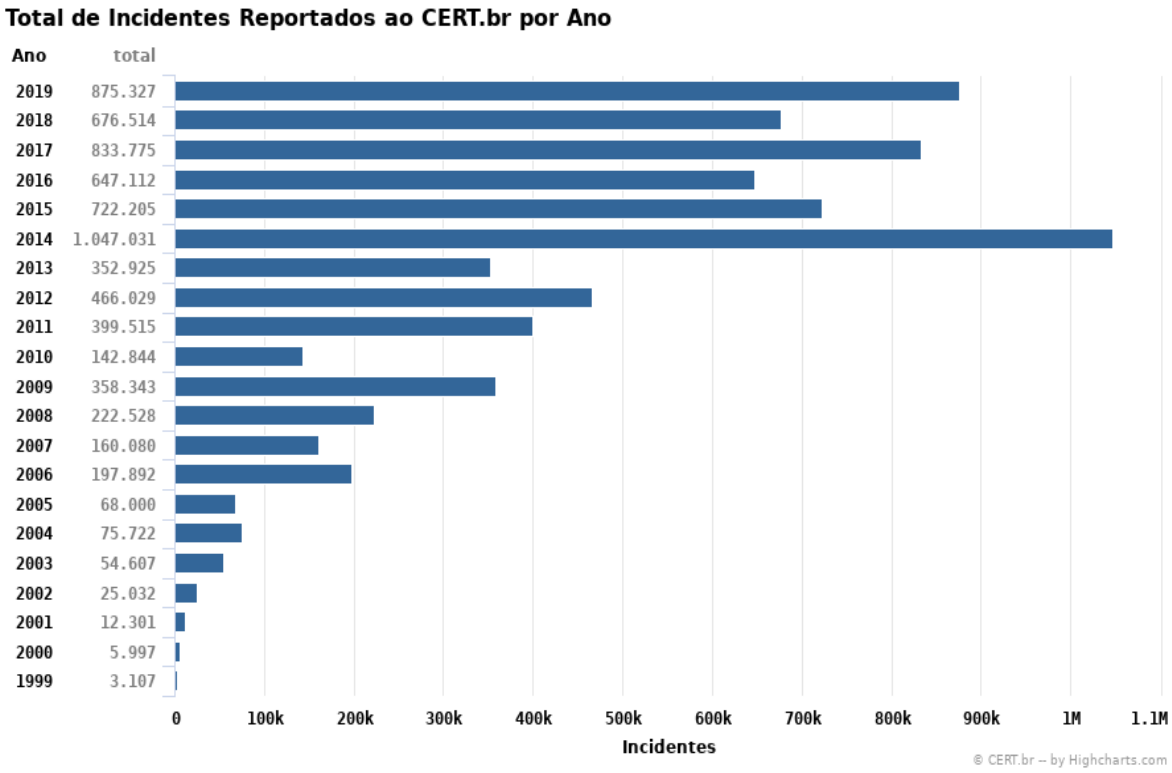
Segundo Corte (2014), a implementação é a parte mais difícil, pois envolve conhecimentos gerais em segurança, conhecimento da organização, de sua cultura, das pessoas envolvidas, das tecnologias hostilizadas, sendo considerada uma tarefa complexa e demorada. No entanto, a maior dificuldade é a compreensão de que os procedimentos estabelecidos estão sendo seguindo pelos usuários ou não.

Para Côrte (2014, p. 82):

> [...] as pesquisas mostram que os principais incidentes de segurança são originados dentro das próprias empresas, por empregados, por ex-empregados ou por terceiros insatisfeitos, ou ainda, por empregados de boa-fé que são vítimas de pessoas bem preparadas, que se utilizam da engenharia social para conseguirem informações confidenciais da empresa que é o alvo do ataque.

Desta forma, podemos verificar que a principal dificuldade em tornar eficaz uma política de segurança da informação está justamente na capacitação dos Recursos Humanos, pois os empregados de uma empresa devem estar conscientes de suas ações, adotando práticas seguras. A Figura 05 mostra a quantidade de incidentes reportados ao Cert.br, o que demonstra a necessidade de criação de políticas de Segurança da Informação nas organizações.

Figura 05: Gráfico de incidentes reportados ao CERT.br por ano



Fonte: https://www.cert.br/stats/incidentes/

4.4.2 Criptografia

Com o avanço nos meios de comunicação, as informações passaram a trafegar pelo ambiente virtual de forma mais intensa, aumentando de forma proporcional à exposição de informações sigilosas, e o consequente risco de roubo de dados. Informações sigilosas trocadas entre duas empresas, por exemplo, podem ser interceptadas por um usuário mal intencionado.

De acordo com a matéria do site G1(2014), 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 para proteção das informações armazenadas, transmitidas em computadores ou exploradas dentro das redes de comunicação.

Para Nomiya (2010), enviar e receber algum tipo de informação de caráter sigiloso é uma necessidade muito 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 desvendá-las. Sendo assim, com o transcorrer dos anos surgiu um enfrentamento entre os que guardam segredos e os que buscam revelar.

Pensando na garantia de transmitir as informações de forma confiável, tem-se hoje a criptografia, oriunda do avanço das telecomunicações, utilizada largamente nas redes de transmissão de dados, a fim de garantir que a informação chegue ao seu destino. Esse processo tenta garantir que apenas o destinatário escolhido seja o receptor da informação. Sobre isso, Kurose e Ross (2013, p. 497-498) 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, através da utilização de tokens de assinatura digital, correio eletrônico, senhas de acesso a sistemas, etc. O objetivo é manter a integridade das informações que transitam pelo meio virtual, além de assegurar a validade e a autenticidade das mensagens, tanto do emissor quanto do receptor.

Essa ferramenta transforma as informações, impossibilitando sua compreensão enquanto a informação não chega ao seu local de destino. A partir do momento que os dados estão em seu destino, eles passam para a condição de serem compreendidos pelo seu remetente, este processo é conhecido como encriptação e decriptação.

Para uma melhor compreensão é necessário distinguir as expressões cifras e códigos. Para Tanenbaum e Wetherall (2011, p.770) “Uma cifra é uma transformação de caractere por caractere ou de bit por bit, sem levar em conta a estrutura linguística da mensagem. Em contrapartida, um código substitui uma palavra por outra palavra ou símbolo”.

As cifras e os códigos têm seu funcionamento semelhante, com o mesmo objetivo: dificultar o acesso às informações. Embora tenham uma vasta história de utilização, principalmente durante as guerras, os códigos não são mais utilizados nos dias atuais. Os Estados Unidos, por exemplo, utilizou essa ferramenta durante as operações da Segunda Guerra Mundial, assim como conta Tanenbaum e Wetherall (2011, p.771):

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

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 e Ross (2013, p. 498-499):

> 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

Em criptografia, assinatura digital é uma forma de autenticação de documentos em meio eletrônico, como forma de substituição da tradicional assinatura manuscrita (com a utilização de caneta e papel), eliminando a necessidade de possuir a versão de um documento assinado fisicamente.

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 pela NBR ISO/IEC 27002:2013:

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 (KUROSE e ROSS, 2013).

Para ser feita a autenticação do documento, o sistema deve gerar um novo resumo através da mensagem armazenada e comparado com a assinatura, decriptando 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 Infraestrutura 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 às partes.

Tanenbaum e Wetherall (2011, p. 506) explicam 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*

Segundo o Cert.br (2012) são ferramentas que procuram descobrir, suprimir ou remover programas ou códigos de um computador que infectou ou estejam infectando a máquina. Antivírus, *antispyware, antirootkit e antitrojan* são exemplos de ferramentas contra intrusões.

Apesar de existirem 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 adaptar 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 computador, 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.

Inúmeras são as técnicas utilizadas para obtenção de e-mails, através de combinações nomes, utilização de varreduras com pesquisa de palavras chaves, típicas de endereços de e-mail, como “@” e ”com”, etc. Sobre essas técnicas, cita o Cert.br (2012, p. 35):

> **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.

Para Tanenbaum e Wetherall (2011) os *spammers* são os responsáveis pela coleta de e-mails, geralmente repassados aos profissionais de marketing a um baixo custo. Para evitar um grande fluxo de mensagens desse tipo, os serviços de e-mails possuem um software para filtragem de spam, que através de algumas características, conseguem e ler e descartar mensagens indesejadas.

4.5 Ataques e incidentes

Uma matéria divulgada no site MTI tecnologia (2018) relata um caso real de um banco no Chile em que os computadores dos funcionários pararam de funcionar. 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 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, buscando a penetração dentro de um sistema. Barreto e Brasil (2016) declara que não existe uma ciência capaz de eliminar de maneira definitiva os incidentes de segurança, restando como solução a vigilância e testes periódicos de verificação.

Os ataques mais conhecidos são através de programas maliciosos, geralmente por meio dos vírus de computador. Veiga (2004, p.65) conceitua vírus de computador:

> 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"

São inúmeras as motivações utilizadas por invasores digitais, que podem variar de uma simples diversão até a realização de ações criminosas. Segundo o site Cert.br (2012) as maiores motivações são a demonstração de poder (mostrar a deficiência de SI de uma empresa), o prestígio (vangloriar-se por conseguir um fato de difícil realização), motivações financeiras (através de furtos ou obtenção roubo de informações confidenciais), ideológicas (tornar inacessível sites de conteúdo que é contrária à opinião do invasor) e comerciais (diminuir a reputação de uma empresa através de ataques).

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.

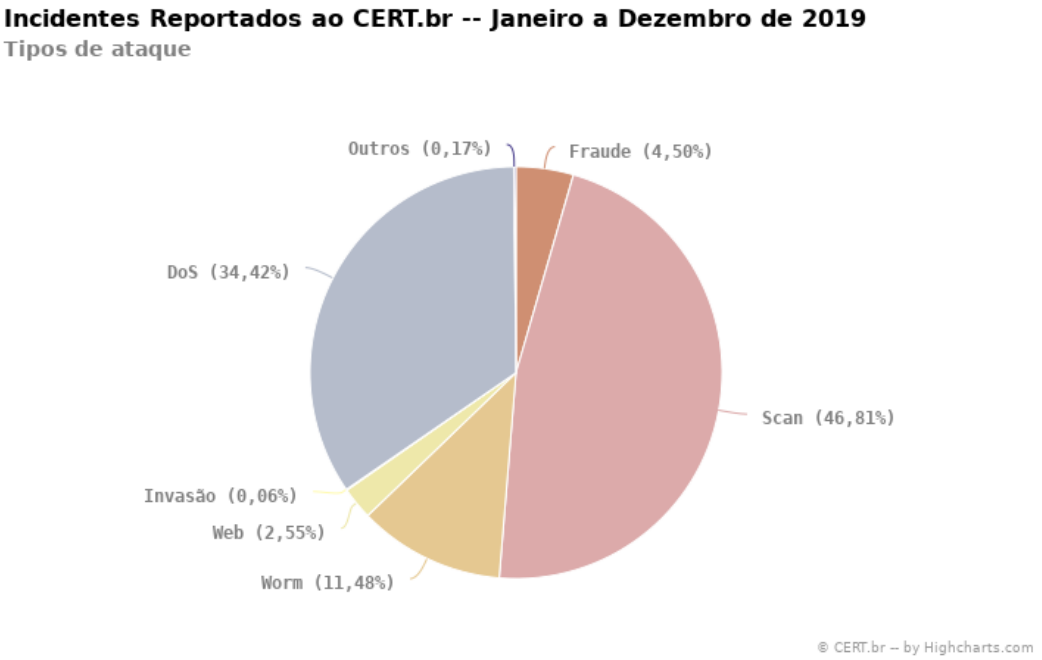
Outro ataque muito comum, é o ataque por DoS (*Denial of service*) – Negação de Serviço, cujo objetivo não é a coleta de informações, mas sim causar uma indisponibilidade de um serviço ou informação devido a uma alta sobrecarga de acessos simultâneos, como cita Tanenbaum e Wetherall (2011, p. 515) "[...] é aquela em que o intruso já entrou em centenas de computadores em outros lugares do mundo, e depois comanda todos esses computadores em um ataque ao mesmo alvo ao mesmo tempo." Já o Cert.br (2012, p. 21), descreve:

> Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*).

A Figura 06 mostra um infográfico de ataques a usuários em todo Brasil, sendo que 46,81% corresponde ao ataque do tipo Scan, 34,42% corresponde ao ataque DoS, 11,48% tipo *worm*, 4,5% fraudes, 4,5% fraudes, 2,55% dizem respeito a um caso particular de ataque

que visa especialmente os servidores Web ou desfigurações de páginas que se encontram na Internet e por fim 0,17% fraudes e 0,06% invasão.

Figura 06: Infográfico de ataques reportados ao CERT.br no ano de 2019



Fonte: https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html

Legenda, conforme p Cert.br (2019):

> **Worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
> **Dos** (DoS -- Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
> **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
> **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
> **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
> **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
> **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores. (grifo nosso).

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*

Jesus e Milagre (2016, p. 34) definem:

> Código malicioso implantado pelo cracker ou trojan, que permite o escalonamento de privilégio, a invasão, a tomada do sistema ou o desligamento de mecanismos de segurança. Para alguns especialistas, backdoor não é vulnerabilidade, mas um código malicioso que permite acesso facilitado ao sistema ou máquina. Em outras palavras, backdoor é um meio não documentado de acessar um sistema, burlando os mecanismos de autenticação.

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 Tróia

Jesus e Milagre (2016, p. 33) descrevem como:

> Espécie de malware. Programa que faria algo além do que parece. "Cavalo de troia" é uma instrução ou código malicioso comumente ocultado em outro software, que, instalado, torna um computador ou sistema vulnerável ou mesmo explora vulnerabilidades já existentes. Dependendo do trojan, é possível não só acessar um sistema, como se tornar administrador, copiar informações confidenciais.

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 que "*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.

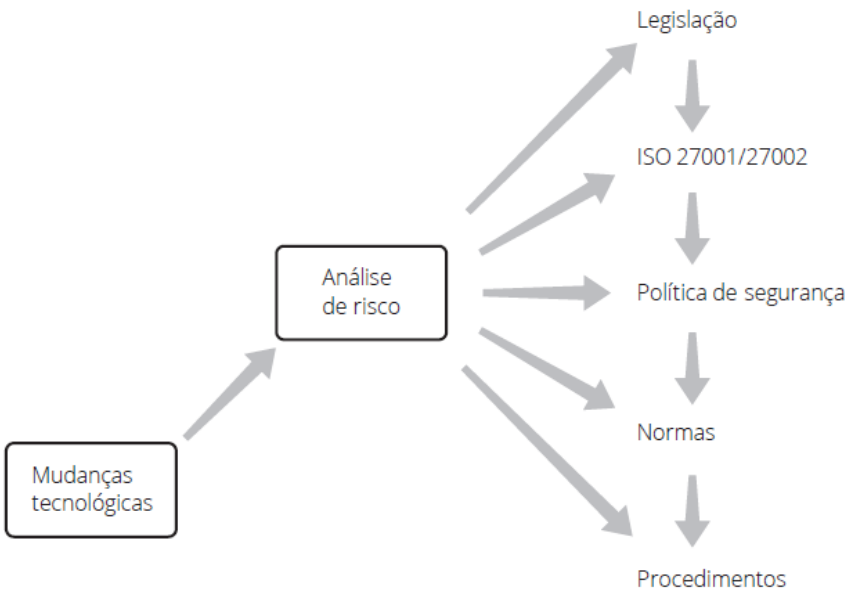
4.6 Ameaças, vulnerabilidades e riscos

De acordo com Sêmola (2003) as ameaças são possiblidades, eventos ou atitudes indesejáveis que podem comprometer as informações, danificar ou excluir um recurso. Já sobre vulnerabilidades Sêmola (2003, p. 48) conceitua que "são as fragilidades existentes ou

associadas a ativos que processam ou armazenam informações e que, ao serem exploradas por uma ameaça, podem comprometer a Segurança da Informação".

Segundo Coelho e Araújo (2013, p. 3), risco é a "combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização. Algo que pode ocorrer e seus efeitos nos objetivos da organização".

Figura 07: Visual Geral na Segurança da Informação



Fonte: Coelho e Araújo (2013, p. 8).

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 27002:2013, 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.

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. Para Coelho e Araújo (2013, p. 3) "A partir desta falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais".

Para Laudon e Laudon (2014), os sistemas de informação e os bancos de dados são os principais pontos de vulnerabilidade e risco. Sendo assim, é necessário monitoramento constante da segurança nas estações de trabalho, no meio de transporte (infraestrutura), servidores, etc. Contudo, outro grande fator gerador de vulnerabilidades é o recurso humano, pois funcionários sem a mínima qualificação podem gerar muitos prejuízos ao sistema com vazamentos de informação e má utilização de recursos de TI.

4.6.1 *Smartphones*

A preocupação em se proteger contra cibercrimes está se tornando um hábito entre os usuários da tecnologia, devido à grande quantidade de incidentes anualmente. Desta forma, haja vista a atual convergência de tecnologias com acesso a internet, os *smartphones* também passaram a ser invadidos.

Segundo pesquisa da empresa Kaspersky (2020), as ameaças à segurança de dispositivos móveis só aumentam a cada ano. Só em 2014, foram detectados quase 3,5 milhões de *malwares* distribuídos em um milhão de dispositivos dos usuários. Em 2017, foram 360 mil arquivos maliciosos reportados diariamente, todos oriundos de dispositivos móveis, especificamente de *smartphones*.

Esses dispositivos possuem diversas informações pessoais, tais como senhas de e-mail, de contas bancárias, endereços, conversas, fotos e informações sensíveis. Assim, é um erro os usuários não se adotarem medidas de proteção, evitando um comportamento de risco.

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, 2020).

A segurança da informação é um tema de estudo constante, haja vista grandes atualizações em matéria de tecnologia da informação, onde constantemente, as formas de invasão aos dispositivos evoluem, necessitando de intervenções mesmo para os experientes especialistas em segurança.

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* são empregados com utilização de engenharia social, sempre levando em conta, informações de um usuário, tal como banco do qual é cliente, comunidade da qual a vítima faz parte, nome de amigos, etc.

Para Coelho e Araújo (2013), num ambiente organizacional, o mal uso de uma estação de trabalho por um funcionário acabam sendo uma porta de entrada para falhas de segurança. 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. 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 (COELHO e ARAÚJO, 2013).

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 (COELHO e ARAÚJO, 2013).

4.7 Sistemas Operacionais Linux

O Linux é um sistema operacional gratuito, onde os usuários podem utiliza-lo sem a necessidade de pagar uma licença, ao contrário de sistemas operacionais proprietários, como o Windows. Sobre o Linux, cita Silva (2020, p. 3):

> O Linux é um sistema operacional criado em 1991 por Linus Torvalds na universidade de Helsinki na Finlândia. É um sistema Operacional de código aberto distribuído gratuitamente pela Internet. Seu código fonte é liberado como *Free Software* (software livre), sob licença GPL, o aviso de copyright do kernel feito por Linus descreve detalhadamente isto e mesmo ele não pode fechar o sistema para que seja usado apenas comercialmente.

Desta forma, o Linux se torna uma opção economicamente viável para uma instituição, pois, por se tratar de tratar de um sistema de código aberto, não é crime a cópia, o download e a instalação.

Outra grande vantagem citada por Silva (2020) é que os sistemas operacionais Linux não costumam executar aplicações e serviços de forma automática, sempre solicitando a permissão do usuário antes de qualquer instalação, muitas delas, através de linha de código, o que permite ter um maior controle sobre o usuário comum, evitando que este faça instalações de programas maliciosos ou que prejudiquem o funcionamento do computador e consequentemente, aumentar a segurança do sistema. Assim, um usuário administrador, responsável pela instalação do sistema operacional e manutenções, pode definir quais aplicativos serão utilizados pelo usuário final, restringindo o uso.

4.8 Crimes Virtuais

Dentro do Código Penal Brasileiro, não há definição legal sobre o conceito de crime virtual, porém a lei conhecida como Lei Carolina Dieckmann (2012), traz alguns tipos de crimes que são praticados no Ambiente Virtual:

> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita

Antes desta lei, os crimes praticados através do meio virtual não tinham essas características específicas (tipificação), onde dispositivos móveis e conexões com a rede eram apenas instrumentos utilizados para execução da conduta delituosa. Como exemplo, antes da lei, se um criminoso obtivesse dados bancários de um usuário, utilizando-se do meio virtual, sua conduta estava tipificada no artigo 155 do Código Penal, “Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel”, as utilizações da rede e de técnicas de invasão eram vistas como agentes qualificadores. Após a Lei Carolina Dieckmann, como mostrado na citação anterior, já tipifica esse exemplo como “Invasão de dispositivo informático”.

A Lei Carolina Dieckmann ainda apresenta dois outros crimes, que é a Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, descrita como "§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento", e a falsificação de cartão (LEI Nº 12.737, 2012).

Doutrinadores do direito costumam classificar os crimes virtuais (ou informáticos) em próprios (com definição própria e específica) e impróprios (com definição no código penal, apenas praticado através de recursos tecnológicos), conforme citam Jesus e Milagre (2016, p. 52-53):

> Assim, classificamos os crimes informáticos em:
> a) **crimes informáticos próprios**: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
> b) **crimes informáticos impróprios**: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais; (**grifo nosso**)

Jesus e Milagre (2016) ainda citam que grande parte dos crimes virtuais são praticados devido à ignorância dos usuários, falta de capacitação das polícias investigativas e pela falsa sensação de anonimato por parte do criminoso virtual. É um crime sem contato físico com a vítima.

Outro ponto importante a se destacar é o Marco Civil da Internet (2014), conhecido popularmente como "constituição da internet", onde são definidos os direitos e deveres dos cidadãos e das empresas no uso da internet. Essa lei cita, por exemplo, acerca das obrigações de provedores na guarda de registro de acesso a aplicações, feitas pelos usuários, clientes dos serviços das operadoras, conforme o artigo 15 da Lei 12.965 (2014, [não paginado]):

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Assim, sempre que for necessário realizar diligências, no sentido de identificar um criminoso virtual, a autoridade policial poderá oficiar os provedores de serviços de internet, para que forneçam os logs de registro, onde poderá ser identificado, por exemplo, o IP do criminoso virtual, o horário de acesso, nome da máquina, endereço físico da placa de rede e

demais informações que poderão ser de fundamental importância para elucidação do crime e materialização da autoria.

5 METODOLOGIA

Até agora foram apresentados conceitos e características pertinentes à segurança da informação no local especificado para que possam servir de base para a realização de estudos de identificação de possíveis ameaças e vulnerabilidades presentes e gere soluções inteligentes, de acordo com a literatura e normas vigentes.

Desta forma, o estudo do tema "Análise da Segurança da Informação no Complexo do Comando Geral da Polícia Militar do Maranhão" tem como objetivo principal analisar a segurança da informação no CCG da PMMA, sendo necessária uma pesquisa de campo para coleta dos dados.

Levando em consideração a importância 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 problemas, mas também servirem de modelo ou oferecer subsídios para outros trabalhos.

5.1 Métodos Utilizados

O estudo foi elaborado da seguinte maneira:

- Quanto à natureza, a pesquisa foi aplicada. Pois não se limita a estudos apenas teóricos, sendo utilizadas pesquisas de campo para análise;
- Quanto à abordagem, trata-se de uma pesquisa mista (quali-quanti), pois utiliza análises qualitativas, e também quantitativas, através da análise de gráficos;
- Quanto aos procedimentos, foram utilizados levantamentos bibliográficos e pesquisa de campo;
- Quanto aos objetivos, a pesquisa foi exploratória e descritiva;
- O método utilizado foi o indutivo.

Inicialmente realizou-se uma pesquisa bibliográfica nos livros pertencentes à Biblioteca Central da Universidade Federal do Maranhão, para que assim, fosse possível elencar obras relacionadas aos vários assuntos citados neste estudo. Além disso, alguns trabalhos científicos foram consultados no intuito de obter um direcionamento, para que não

houvesse fuga ao tema e organização dos assuntos. Por fim, consultas em sites especializados e informativos, para subsidiar o referencial teórico.

Por se tratar de uma pesquisa aplicada, a seguir serão mostrados os detalhes sobre o local, a amostra e o delineamento da pesquisa.

5.2 Detalhamento da Pesquisa

A pesquisa foi realizada no CCG da PMMA, localizada na Avenida Jerônimo de Albuquerque, s/nº, bairro Calhau durante o mês de maio de 2020. Este local foi escolhido, pois apresenta todos os requisitos necessários para uma boa coleta de dados, tais como: grande fluxo de atividades administrativas, estrutura de rede e internet e presença do alto comando da corporação, responsável pelas tomadas de decisão a nível estratégico.

Importante ressaltar que o contexto ao qual a Polícia Militar do Maranhão está inserida é de fator relevante em relação à Segurança Pública, pois tem o dever constitucional de instituição responsável por garantir a ordem pública em nível estadual. Conforme cita o artigo 144 da Constituição Federal Brasileira de 1988, § 5º: "Às polícias militares cabem a polícia ostensiva e a preservação da ordem pública" (CF, 1988). Desta forma, criminosos podem se aproveitar de fragilidades encontradas para assim obter informações necessárias para a prática de crimes de maior escalão, como assaltos, roubos e homicídios.

Além disso, verifica-se a enorme sensibilidade de muitas informações utilizadas na PM, que se obtidas por pessoas mal intencionadas, pode levar ao cometimento de crimes. Imagine por exemplo, um criminoso dispor de informações sobre a quantidade de viaturas utilizadas em um determinado município do Estado e onde as barreiras policiais são realizadas: seria uma informação que facilitaria supostos criminosos a assaltarem uma agência bancária ou executar um desafeto.

Na coleta dos dados, foram escolhidos usuários que no serviço administrativo da corporação policial que utilizam computadores com acesso à Internet. Foi aplicado um questionário com 08 (oito) perguntas fechadas sobre assuntos relacionados à segurança da Informação a 55 (cinquenta e cinco) policiais, sendo classificados como usuários comuns, realizando atividades de cunho administrativo. Também foi realizada uma entrevista direcionada à chefia da Diretoria de Tecnologia da Informação da PMMA, que é responsável pela gestão da TI dentro dessa Organização Militar, com 08 (oito) perguntas abertas. Por último, informações foram coletadas através de observações diretos do campo a ser estudado.

5.3 Etapas da pesquisa

O processo da pesquisa teve início, com a busca de referenciais teóricos em livros e das normas NBR ISO/IEC 27001:2013 e NBR ISO/IEC 27002:2013, para que nas próximas fases o pesquisador tenha embasamento em seus estudos realizados.

Esta pesquisa foi dividida em três partes:

- Questionário com 08 (oito) perguntas objetivas fechadas, destinado a uma amostra de 55 (cinquenta e cinco) policiais militares que desempenham atividades administrativas com a utilização do parque computacional local;
- Entrevista com 08 (oito) perguntas subjetivas abertas, destinada à chefia da Diretoria de Tecnologia da Informação da PMMA, com dois oficiais PM, para que posteriormente fosse feito um comparativo das informações coletadas com o que diz o referencial teórico e a norma NBR ISO/IEC 27002:2013;
- Observação direta intensiva, para registro de imagens e demais informações relevantes. As visitas foram feitas no mês de maio de 2020, das 07h30min às 17h00min. Foi feito um levantamento dos ativos de informática e procedimentos adotados, registrando-se todos os dados de relevância para a pesquisa, além de registros fotográficos.

Após a realização do comparativo, na etapa de análise dos resultados, será elaborada uma relação de aspectos positivos e negativos observados, bem como a análise das vulnerabilidades e ações de melhorias, apontando medidas preventivas, corretivas e mitigadoras, satisfazendo aos objetivos gerais e específicos desta pesquisa.

5.4 Pesquisa de Campo

As perguntas estarão baseadas de acordo com a bibliografia e as normas da ABNT. A entrevista será direcionada à chefia do setor técnico, para esclarecimento de informações pontuais, que não necessitam de análise gráfica. Já o questionário, servirá para traçar dados estatísticos sobre a atual conjuntura dos operadores dos ativos de informática que trabalham nos setores administrativos do CCG da PMMA.

A entrevista e o questionário farão referências aos tópicos da NBR ISO/IEC 27002:2013:

- Seção5 Políticas de segurança da informação;
- Seção 6 Organização da segurança da informação;
- Seção 7 Segurança em recursos humanos;

- Seção 8 Gestão de ativos;
- Seção 9 Controle de acesso;
- Seção 10 Criptografia;
- Seção 11 Segurança física e do ambiente;
- Seção 12 Segurança nas operações;
- Seção 13 Segurança nas comunicações;
- Seção 14 Aquisição, desenvolvimento e manutenção de sistemas;
- Seção 15 Relacionamento na cadeia de suprimento;
- Seção 16 Gestão de incidentes de segurança da informação.

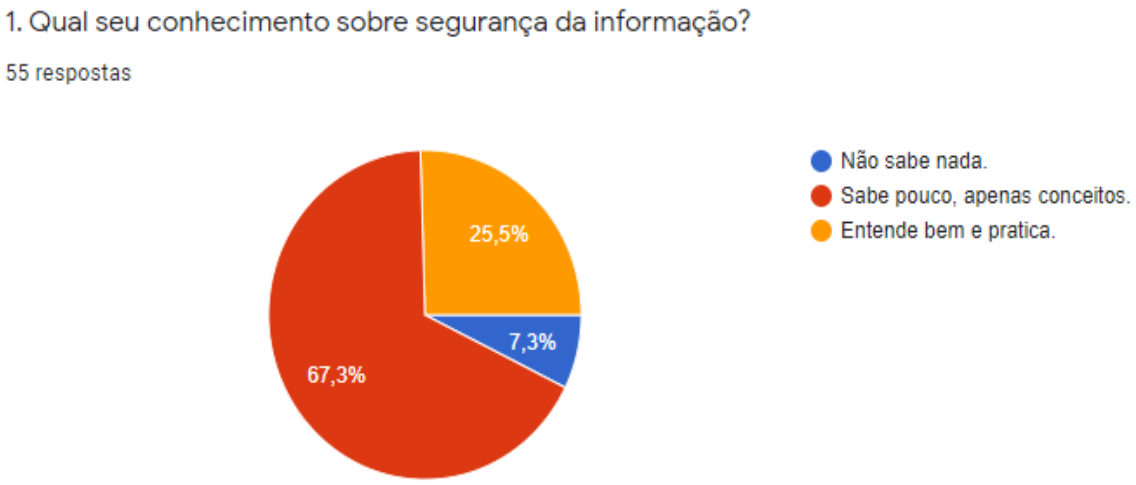
O questionário está no apêndice A, já a entrevista, no apêndice B. As fotos da pesquisa de campo estão nos anexos deste estudo.

6 ANÁLISE DOS RESULTADOS

6.1Questionário

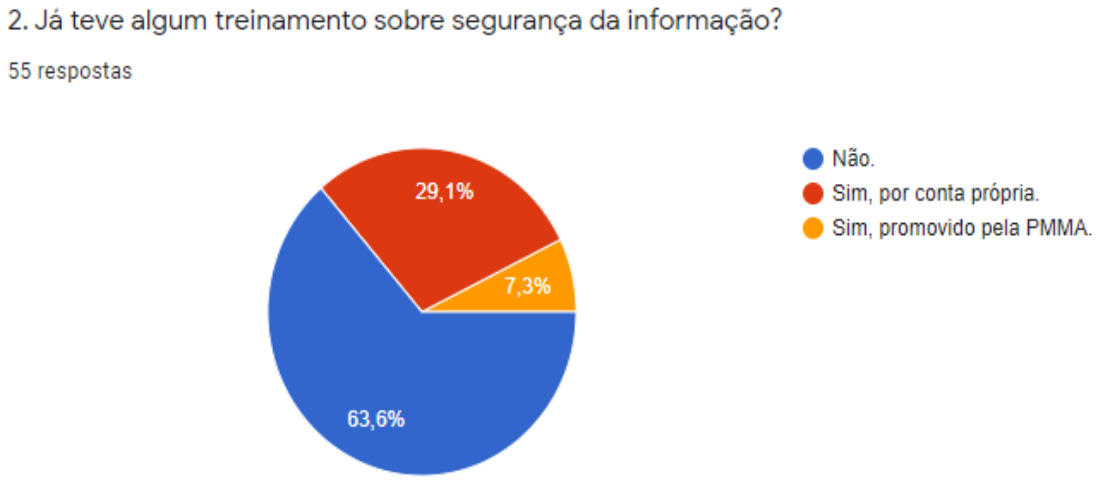
Foi aplicado um questionário com 08 (oito) perguntas fechadas (ver APÊNDICE A), no intuito de aferir informações sobre os policiais militares acerca de procedimentos e informações relacionadas à segurança da informação. O local escolhido foi o Complexo do Comando Geral da PMMA, através de solicitação anexa, em que 55 (cinquenta e cinco) militares participaram da pesquisa.

Gráfico 01: Conhecimento sobre Segurança da Informação



Fonte: Próprio autor.

Gráfico 02: Treinamento em Segurança da Informação



Fonte: Próprio autor.

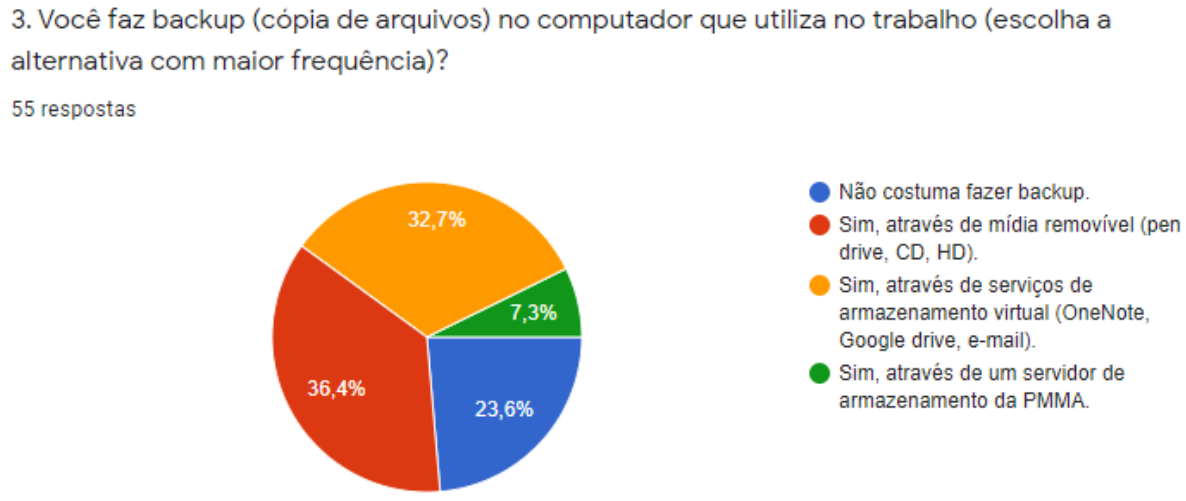
Na pergunta 01, observa-se que a maioria dos policiais questionados sabe pouco ou não sabem nada sobre segurança da informação, e apenas 25,5 %, praticamente a quarta parte dos entrevistados, se julgam entendedores e praticantes desses conhecimentos.

As respostas da pergunta número 02 justificam em parte as repostas obtidas na pergunta 01, haja vista o fato de apenas 7,3% dos policiais terem tido algum tipo de treinamento pela corporação e a maioria, exatamente 63,6%, não tiveram nenhum tipo de capacitação. Ainda existiram aqueles que buscaram capacitação por conta própria, 29,1%.

Laudon e Laudon (2014) alega que 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.

A recomendação é que em toda organização haja uma política de segurança da informação, conforme ABNT 27002 (2013, p. 2) “Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”. Assim, na Polícia Militar do Maranhão, recomenda-se adotar a nível institucional, em todas as unidades operacionais e administrativas, uma política de segurança da informação, e que seja repassada a todos os policias subordinados, durante as disciplinas dos cursos de ingresso ou através de treinamentos a serem realizados pela própria DGTI.

Gráfico 03: Backup de arquivos

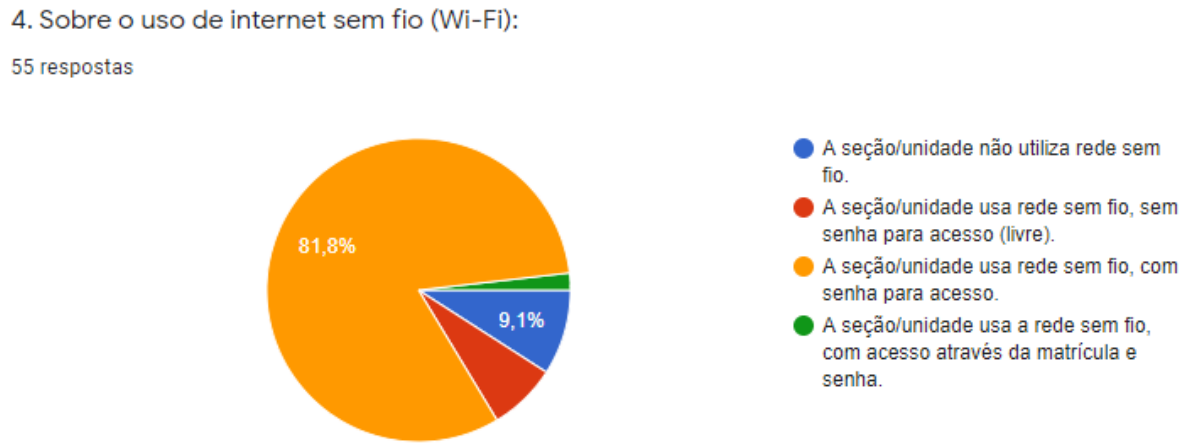


Fonte: Próprio autor.

Através das respostas, verifica-se que 23,6% não costumam fazer backup, 36,4% faz através de mídias removíveis, 32,7% através de serviços de armazenamento virtual e a grande minoria, 7,3%, através de um servidor de armazenamento. Essa pergunta se faz necessária, haja vista ser uma recomendação recorrente, constante na ABNT 27002:2013, como forma de minimizar os riscos de perdas de informações importantes, inclusive citando na página 53, a implantação de diretrizes para cópias de segurança como forma de proteção contra perda de dados.

Desta forma, entre as respostas citadas, a que possui maior segurança, é o backup dos arquivos coma utilização de um servidor de armazenamento/backup, haja vista evitar que o usuário misture documentos particulares com organizacionais e vice versa. O de backup através do uso de mídias removíveis traz maior risco de proliferação de infecções por vírus de computador, sem falar no risco de perda ou furto desses dispositivos.

Gráfico 04: Segurança nas redes *Wi-Fi*

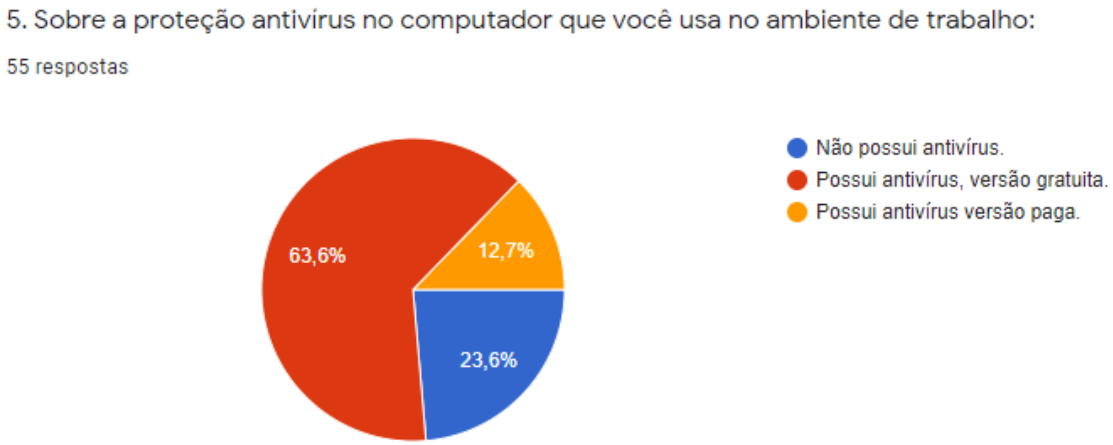


Fonte: Próprio autor.

Sobre a segurança das redes, a seção 13 – Segurança nas Comunicações, da ABNT 27002 (2013, p. 61), cita que se deve “Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam”. Observa-se através do gráfico que a grande maioria dos dispositivos de rede são configurados para acesso através de senha 81,8% que, conforme visto por Tanenbaum e Wetherall (2011), pode ser uma rede configurada através de segurança WEP, WPA ou WPA2, pois o acesso através de usuário e senha pode ser feito através da criptografia 802.1X EAP, o que proporciona uma maior segurança nas redes sem fio (*Wi-Fi*), uma vez que é possível identificar, no ambiente da

PMMA, de qual matrícula partiu um suposto ataque, e desta forma, limitar a autoria de um possível crime virtual.

Gráfico 05: Uso de antivírus.



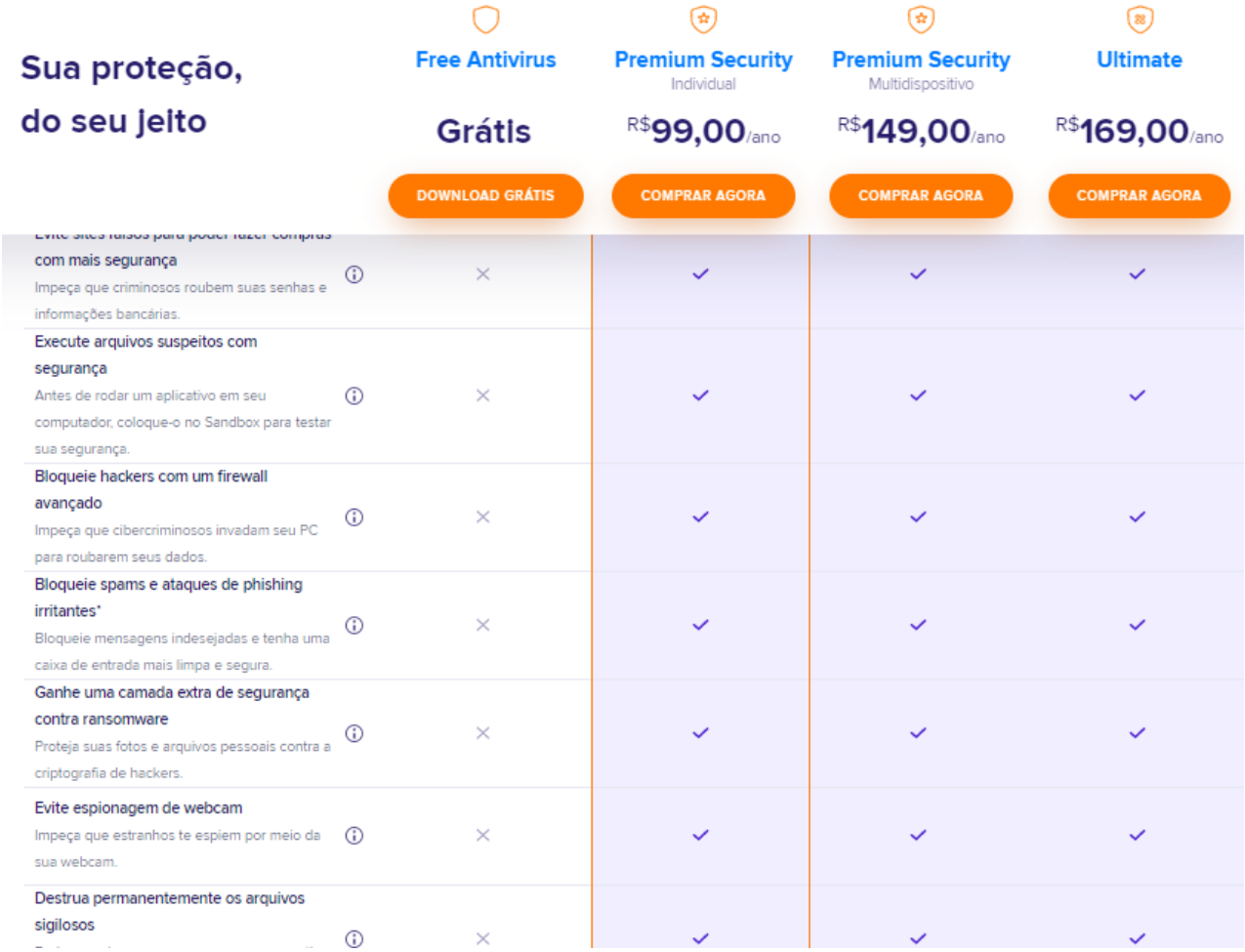
Fonte: Próprio autor.

Verifica-se que no ambiente da PMMA, a maioria dos usuários utiliza computadores com versões de antivírus gratuitas (63,6%), uma parte nem usa antivírus (23,6%) e a minoria utiliza uma versão paga (12,7%).

Segundo informação dos sites de antivírus populares, tais como o Avast Software (2019) e AVG (2019), as versões pagas têm muito mais recursos e ferramentas para combate a *malwares* que os de versão gratuita, estas que funcionam de forma bem limitada, geralmente relacionada à promoção do produto final ou para utilização temporária, como amostra ou *demo*. Assim, apesar de mais caro para a instituição, optar pela utilização de uma versão paga de um software antivírus acaba sendo a opção ideal, se consideramos os princípios de segurança da informação. É o que mostra o comparativo da Figura 08.

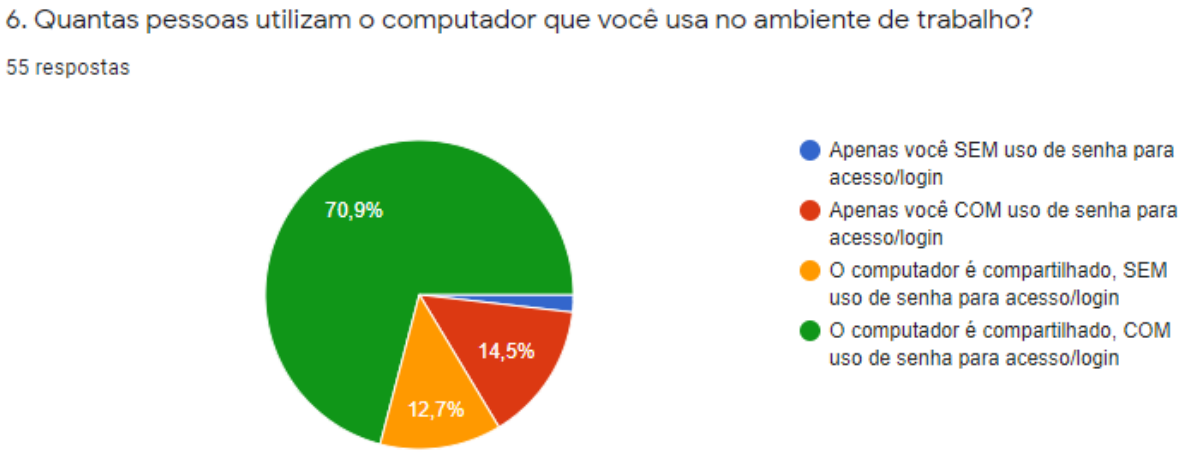
A ABNT 27002:2013 cita que para proteção de informações em local de trabalho é sempre recomendado a utilização de softwares antivírus. Já o Cert.br (2012) cita que *softwares* antivírus são essenciais, a medida que detectam e anulam ou removem códigos maliciosos de um computador.

Figura 08: Comparativo entre as versões grátis e pagas do antivírus Avast.



Fonte: www.avast.com/pt-br/compare-antivirus

Gráfico 06: Logon / Login em computador utilizando senha para acesso



Fonte: Próprio autor.

A seção 9 da ABNT 27002:2013, que trata sobre o controle de acesso, tem como objetivo limitar o acesso às informações e aos recursos responsáveis pelo processamento das informações. Ainda segundo a ABNT 27002 (2013, p. 31), "Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (*log-on*)", desta forma, é importante que em todo acesso a sistema ou recurso computacional sejam implantados controles para acesso através de usuário e senha.

A partir dos dados do Gráfico 06 verificamos que 70,9% dos usuários obedecem a essa regra mesmo utilizando o computador compartilhado, 14,5% utilizam o computador de forma exclusiva e com uso de *log-on*, que traz uma segurança a mais, pois os dados não são compartilhados com outros usuários. E apenas uma minoria, mas considerável, quantidade de usuários utiliza o computador sem uso de senha, facilitando a utilização do computador por outras pessoas que não necessitam saber de informações potencialmente importantes. A recomendação é que 100% dos usuários utilizem sistemas da forma mais segura.

Gráfico 07: Utilização de e-mail para atividades administrativas

Fonte: Próprio autor.

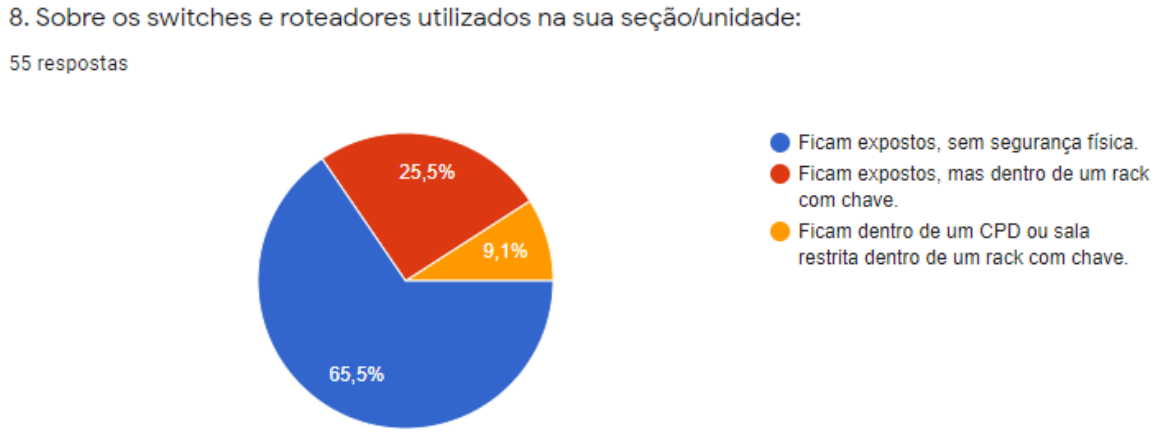
Pelo Gráfico 07 verificamos que a grande maioria dos policiais utiliza e-mail, porém não institucional, totalizando 72,7% dos questionados. Já 23,6% afirmam que utilizam e-mail institucional na unidade em que servem, e uma minoria não expressiva utiliza e-mail próprio ou não utiliza e-mail na realização de suas atividades. Segundo a ABNT 27002:2013, seção 6, que trata sobre a organização da segurança da informação, reconhece a ferramenta de correio eletrônico como importante recurso para utilização nas atividades administrativas. Porém, o uso de e-mail não institucional para auxilio nessas rotinas, fere uma política de

negócio com as empresas provedoras desse serviço, pois existem planos específicos para serviços corporativos, sendo pagos.

Além disso, utilizar e-mails corporativos auxilia a administração nos casos de auditoria interna, quando necessitar de monitoramento e checagem das atividades desenvolvidas. Fica mais fácil a formalização de pedidos através de um e-mail corporativo, pois é um meio oficial para relacionamento entre clientes e fornecedores e eficiências nas comunicações internas, é o que elenca a *homepage* do siteblindado.com (2018).

Durante as diligências constatou-se que os e-mails institucionais utilizados pelos usuários não eram gerenciados pela PMMA, mas sim, pela secretaria de segurança pública.

Gráfico 08: Estado de Switches e Roteadores no ambiente de trabalho



Fonte: Próprio autor.

O Gráfico 08 refere-se à segurança física de equipamentos de rede, especificamente, de switches e roteadores, responsáveis pela conexão de dispositivos móveis e computadores dentro da rede. Neste questionário, 65,5% afirmaram que os equipamentos ficam expostos, 25,5% disseram que apesar de ficarem expostos estavam dentro de um rack com chave, e para 9,1% dos questionados, esses equipamentos ficam acondicionados em local específico, dentro de um rack.

A seção 11 da norma ABNT 2007 (2013, p. 38) trata especificamente sobre a segurança física e do ambiente, cujo objetivo é "Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização", portanto, é indispensável que toda organização utilize dos meios necessários para evitar que pessoas não autorizadas tenham acesso aos ativos de rede de uma organização.

Ter acesso à rede interna de uma organização aumenta os riscos de obtenção de dados sensíveis por pessoas mal intencionadas.

Ainda segundo a norma ABNT (2013, p. 41), afirma que “Convém que os equipamentos sejam protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado”, ou seja, a utilização de proteção física, controle de acesso de pessoas através de videomonitoramento ou agente de segurança se tornam fatores que diminuem esses riscos.

6.2 Entrevista

A segunda parte desta pesquisa envolve uma entrevista aplicada à chefia da Diretoria de Gestão da Tecnologia da Informação, com 08 (oito) perguntas abertas (ver APÊNDICE B). Importante enfatizar que o princípio da publicidade, previsto no Direito Administrativo, é aplicado dentro das organizações públicas, garantindo a legalidade neste tipo de coleta de dados, que não visa obter dados sensíveis ou sigilosos, mas apenas saber sobre informações e procedimentos adotados pela DGTI. Nessa etapa, dois comandantes da DGTI foram entrevistados, um Coronel PM (Entrevistado A) e um Capitão PM (Entrevistado B).

Foi necessário entender a abrangência dos serviços realizados pela DGTI, para assim, comparar com a literatura e normas vigentes, no sentido contribuir positivamente com o crescimento da corporação, citando vantagens, desvantagens e sugerir melhorias.

Buscou-se inicialmente saber se existe na PMMA algum protocolo ou portaria sobre a implantação de uma política de segurança da informação (pergunta 01), haja vista ser a primeira recomendação prevista na ABNT 27002:2013, seção 5, sendo obtida a seguinte resposta:

> Não existe formalmente em nível de PMMA, porém em nível de Estado protocolos de acesso são regulamentados pela Secretaria Adjunta de Tecnologia da Informação (SEATI), que é responsável pela administração de alguns serviços, como monitoramento de links de internet, fluxo de banda e hospedagem de servidores. (ENTREVISTADO A)

Desta forma, verifica-se a necessidade de implantação de uma política de segurança da informação na organização policial militar, pois a PMMA difere de outros órgãos do Estado com relação à sensibilidade das informações, tendo suas peculiaridades.

Buscando-se atestar a informação, foi constatado que a SEATI realmente tem essas atribuições dentro de seu escopo de serviço, conforme Decreto 16.677 de 26 de junho de 2003 (MARANHÃO, 2003).

Já a pergunta 02, questiona sobre as áreas de atuação da DGTI, obtendo-se:

> Manutenção – Conserto de equipamentos com troca de peças (PCs, impressoras e nobreaks) e configuração de equipamentos;
> Rede – Administração da rede interna, de serviços de rede e configuração de equipamentos;
> Desenvolvimento – Criação e manutenção de softwares utilizados pela corporação policial;
> Suporte – Atendimento ao usuário.
> (ENTREVISTADO A)

Verifica-se assim um ponto muito positivo, haja vista que os próprios profissionais responsáveis por gerenciar a TI, e consequentemente, questões referentes à Segurança da Informação são da corporação, atendendo a vários dispositivos previstos na ABNT 27002:2013, seções 6, 11, 12 e 14, (2013, p. 5) "provisão de suporte e manutenção de hardware e software", como citado também na ABNT 27002 (2013, p. 44):

> Convém que sejam implementados controles apropriados, na época programada para a manutenção do equipamento, dependendo de a manutenção ser realizada pelo pessoal local ou por pessoal externo à organização; onde necessário, convém que informações sensíveis sejam eliminadas do equipamento, ou o pessoal de manutenção seja de absoluta confiança.

Por conseguinte, ter profissionais habilitados na corporação, dá autonomia à administração da rede local para utilizar e configurar ferramentas de bloqueio de conteúdo, como a utilização de servidores *proxy*, *firewalls,* anti-malwares, etc. Também, trabalhar com efetivo disponível para o desenvolvimento e manutenção das aplicações necessárias à corporação policial militar.

Com relação à pergunta 03, objetivou entender a existência de restrições ou bloqueios de acesso à internet aos usuários nos computadores dos usuários, a exemplo de redes sociais como YouTube ou demais sites que fujam do interesse da administração (facebook, Instagram, Twitter, etc.). Sendo respondido pelo Entrevistado B que "Sim. Sites de compras, de conteúdo pornográfico e redes sociais são bloqueados através de um servidor Proxy, que age filtrando conteúdo, intermediando requisições de clientes a outros servidores", o que configura, mais uma vantagem dentro do escopo da segurança da informação, evitando que usuários exponham informações pessoais, e sensíveis, acidentalmente nas redes sociais, ou até percam tempo que seria dedicado ao expediente de trabalho com entretenimento e distrações.

Com relação à pergunta 04, questiona-se acerca dos sistemas utilizados pela PMMA e suas respectivas finalidades, sobre este tema foi obtida a seguinte resposta:

> Frota Log – Gerenciamento e controle de viaturas;
> SGI – Sistema de Gerenciamento de Informações, para confecção de boletim eletrônico;
> PM Doc – Sistema para gerenciamento de Recursos Humanos (RH);
> Cis Doc – Sistema interno da DGTI, para controle e acompanhamento de ordens de serviço.
> (ENTREVISTADO B)

De acordo com as respostas obtidas, pode-se observar que a PMMA possui sistemas essenciais responsáveis, principalmente, pelo controle de viaturas, de pessoal e de informações sobre rotinas administrativas, haja vista que o SGI citado, é responsável pela confecção eletrônica de boletim eletrônico, usado para publicação de portarias e informações da rotina policial militar. Laudon e Laudon (2014) ressalta que toda empresa deve informatizar suas rotinas, a fim de obter melhor controle de suas ações e resultados, desta forma, seria interessante, que outras atividades administrativas que são realizadas de forma manual, fossem também informatizadas, não foi observado, por exemplo, um sistema para controle e cadastro de ocorrências policiais, algo que já é realidade em polícias de outros Estados, como em Santa Catarina, onde é utilizado o Sistema Integrado de Segurança Pública (SISP, 2020).

Outro ponto importante seria a utilização de algum sistema para economia de papel e uso de assinaturas eletrônicas, a exemplo do Sistema Digidoc, utilizado pelo Tribunal de Justiça do Maranhão, em que os processos, documentos e requisições são enviados e respondidos virtualmente, sem a necessidade de impressão e gastos com logística para recebimento e entrega de documentos físicos (ANTÔNIO, 2011).

Com relação à pergunta 05, saber se DGTI atua em todas as unidades da PMMA, foi respondido que:

> A Diretoria foi criada através da Medida Provisória nº 264, de 18 de dezembro de 2017, com a finalidade de gerenciar toda a Tecnologia da Informação das unidades pertencentes à PMMA, porém, na prática, pelo baixo efetivo e o fato das unidades do interior possuírem independência orçamentária, a DGTI atua apenas nas unidades da região metropolitana.
> (ENTREVISTADO A)

Pela resposta, verifica-se que a extensão da gestão desta Diretoria não se estende a todas as unidades da PMMA, o que se torna um problema, haja vista que as unidades do interior se tornam independentes para adotarem práticas de uso dos equipamentos de TI da forma que mais for conveniente, e caso seja implantada uma política de segurança da

informação, não haveria adesão dessas unidades independentes. Desta forma, se torna imprescindível à unificação e integração dos procedimentos e medidas preventivas de segurança da informação em toda corporação, para que não hajam falhas. Como cita Carvalho (2009, p. 26) "A política de segurança da informação define um padrão de segurança a ser adotado por toda organização, pessoal técnico, gerencial, operacional e usuários internos e externos".

Com relação à pergunta 06, sobre a existência de servidores web, de rede, de correio eletrônico, de programas e de armazenamento na DGTI, foi respondido:

> Web, pois administram seu próprio Website. De rede, pois possuem domínio próprio, com acesso a serviços de *active directory* e de armazenamento de arquivos (para backup e compartimentação de pastas). De programas, mas administrado pela SEATI. Não possui servidor de correio eletrônico.
> (ENTREVISTADO B)

A disponibilização de serviços por pessoal da própria corporação se torna um fator de bastante relevância, pois a informação está sendo gerenciada num ambiente interno e protegida. Com relação aos serviços, seria interessante, como já foi citado, a disponibilização de um serviço de correio eletrônico para os usuários, gerenciado pela PMMA. O site Cert.br (2016) 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.

Serviços de rede são interessantes, pois o próprio administrador pode criar usuários e senhas, inserindo-os dentro de um domínio, para que possam acessar os sistemas operacionais dos computadores e também incrementar regras de acesso, como bloqueio através de proxy, configuração de *firewall* e do gerenciamento de equipamentos de rede, como switches, pontos de acesso, impressoras, etc. 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 das informações da PMMA.

Com relação à pergunta 07, sobre a DGTI capacitar os usuários da PMMA para o bom uso dos computadores, em especial, sobre segurança da informação, foi respondido:

> Não. A DGTI não costuma capacitar os servidores nesta área de TI, porém existem projetos em andamento para treinamento e capacitação. Ressalta-se que nos cursos de formação, oferecidos no ingresso dos policiais, existem disciplinas de informática e tecnologia da informação aplicada à segurança pública.
> (ENTREVISTADO B)

A capacitação é necessária para repasse de todas boas práticas de usabilidade e medidas de prevenção para seguranças das informações por parte dos usuários. É muito comum a exposição das informações pelos funcionários, sendo os principais responsáveis pelas falhas de segurança. Por esse motivo, é importante existir orientações e treinamentos constantes para educar os profissionais pelas boas práticas dos conceitos relacionados à segurança da informação. As orientações podem ser estabelecidas diante das normas de uma política de segurança e através de cartilhas divulgadas nos meios digitais da corporação, por exemplo.

Com relação à pergunta 08, sobre a PMMA utilizar software livre para atividades administrativas, especificamente Linux e Libre Office, foi respondido pelo Entrevistado A que "Sim, por razões de viabilidade econômica".

Segundo Cardoso (2010) em matéria para o site vivaolinux, a utilização de softwares livres pela administração pública já é um fator positivo, pois além de ser uma vantagem econômica, o sistema operacional Linux, como foi citado na literatura, traz grandes vantagens em relação à segurança das informações, principalmente por apresentar menos riscos à exposição a *malwares, spywares*, vírus, etc. Como esses programas do tipo código aberto já são utilizados dentro da instituição, deve ser expandido a todos os setores, de forma gradual, sendo dado o treinamento necessário aos usuários. O pacote Libre Office, por sua vez, evita que a administração policial militar tenha gastos extras com a aquisição de softwares proprietários para escritório, uma vez que é compatível com o sistema operacional Linux e realiza operações similares aos pacotes Office da empresa Microsoft.

6.3 Observação Direta Intensiva

A terceira desta pesquisa diz respeito a uma coleta de dados *in loco*, observadas no local da pesquisa. Para melhor similaridade, algumas fotos foram retiradas, a fim de melhor descrever o cenário (ver ANEXO A).

6.3.1 Pontos positivos observados

- Foi observado existência de segurança armada 24h em todas as regiões do complexo, com a realização de abordagens e identificação de pessoas;
- Os profissionais que integram o serviço do corpo da guarda possuem uma grande consciência da importância que se sem proteger o espaço físico, sabendo que é essencial para a proteção do patrimônio, das pessoas e das informações contidas no CCG, sendo esse um assunto constantemente discutido entre eles;
- Foi verificada a existência de um dispositivo que o policial militar pode utilizar para reportar possíveis elementos que possam comprometer a segurança: livro do comandante da guarda;
- Os funcionários militares que adentram o CCG estão sempre fardados. Já os visitantes são cadastrados e identificados antes de acessarem as dependências;
- Foi constatado que as chaves que dão acesso às salas, escritórios e instalações de todas as instalações estudadas do CCG, ficam devidamente armazenado em um claviculário que permanece trancado, quando se necessita de alguma chave, o funcionário ou visitante precisa pedir aos profissionais da guarda;
- Foi verificado que o corpo da guarda possui estrutura para funcionar como recepção para identificação de visitantes, em todas as regiões;
- Foram encontradas sinalizações dispostas nas proximidades de algumas áreas consideradas restritas, indicando que apenas pessoas que possuem credencial de segurança podem acessar;
- Foram constatadas áreas consideradas restritas, quando não ocupados são devidamente trancadas;
- Foi verificada a existência de alguns locais específicos para o armazenamento de materiais e equipamentos de acesso restrito;

- Foi observado que na Diretoria de Gestão da Tecnologia da Informação, quaisquer mídias de armazenamento que não são mais utilizadas, são fisicamente destruídas, ao invés de apenas apagados;
- Quando na realização de um embarque ou desembarque de material para transporte, tem-se o cuidado de manter por perto apenas pessoas autorizadas para a execução do trabalho, e num local centralizado;
- O CCG, através da DGTI, realiza a manutenção interna de quase todos os seus equipamentos tecnológicos;
- O CCG conta com profissionais especializados em manutenção em equipamentos de rede e TI;
- Foi observado que a manutenção dos equipamentos utilizados na unidade é realizada somente por pessoas autorizadas;
- Foi observado que após a manutenção de um determinado equipamento da unidade, são realizadas inspeções para averiguar se o equipamento está em perfeitas condições de operação;
- Foi observado que os agentes de segurança realizam comunicação através de equipamentos de radiofrequência;
- Foi observado que existem sistemas de videomonitoramento em todo perímetro do CCG;
- Foi observado que alguns equipamentos de rede, como switches e roteadores, estavam expostos;
- Foi observado que os equipamentos de informática estão inventariados, possuem tombamento e incluídos na carga da administração;
- Foi observada a utilização de guaritas e bloqueios de acesso físico, como portões e cancelas automáticas para restrição de acesso.

6.3.2 Recomendações a serem implementadas

- Criar uma política de segurança da informação no CCG;
- Definir procedimentos para incremento da segurança física, segundo as ABNTS 27001:2013 e 27002:2013;

- Para fins de melhor controle de responsabilidade e atribuição, que seja definida uma pessoa responsável pela administração dos processos de segurança física da unidade, assim como sua equipe de trabalho;
- Criar sistemas informatizados para cadastro de pessoas e veículos, que registre data, hora, motivo e nome do visitante;
- Ampliar os sistemas de videomonitoramento para as áreas internas;
- Aumentar a altura da barreira física existente, a fim de fornecer uma maior proteção ao perímetro (ampliar o tamanho do muro);
- Acrescentar à barreira física, elementos que possam desencorajar ou dificultar uma transposição não autorizada. Como exemplo temos cercas elétricas, alarmes, concertinas, entre outros;
- Eliminar obstáculos encontrados em alguns pontos da área interna do perímetro, onde deveria apresentar uma zona neutra, mas que apresentam árvores e arbustos que prejudicam a visão dos agentes de segurança;
- Criar barreiras tecnológicas que protejam o perímetro que circunda o CCG, através da utilização de aparelhos como sensores de movimento, sensores de presença, alarmes sonoros ou visuais, entre outros;
- Adquirir racks para instalação de switches e roteadores, bem como estabelecer locais próprios para acondicionamento (sala com ar condicionado);
- Confeccionar crachás para a identificação de visitantes que venham a entrar no CCG, por qualquer motivo;
- Reforçar a segurança interna através da instalação de grades nas portas e janelas existentes nas salas, escritórios e demais setores existentes no CCG a fim de impedir o acesso não autorizado;
- Criar um sistema de entrada e saída de materiais que registre data, hora, detalhes do material recebido, responsável pela entrega do material e responsável pelo recebimento do material;
- Demarcar as vagas dos estacionamentos para a utilização de visitantes, separando-as em áreas específicas;
- Acrescentar uma maior proteção às áreas seguras, implementando um sistema que restrinja o acesso, liberando a livre passagem apenas para pessoas que possuam credenciais de segurança (ex.: portas com fechaduras eletrônicas controladas por leitores biométricos, ou códigos numéricos, cartões magnéticos ou outros);

- Projetar e implementar uma nova rede LAN/WAN em todo o complexo, que atenda a requisitos de segurança, escalabilidade e tolerância a falhas;
- Orientar os funcionários que trabalham com sistemas que necessitam de autenticação, para que, ao encerrar seus trabalhos ou necessitar se ausentar do local por alguns instantes, fechem suas seções para que uma terceira pessoa não tenha acesso;
- Padronizar o uso de bloqueio temporizado nos computadores da unidade que se mantiver em ócio;
- Disponibilizar e-mail funcional aos servidores;
- Criar um cronograma anual de capacitação sobre procedimentos de segurança da informação, além da inclusão da matéria nos cursos de formação;
- Definir que o acesso à rede sem fio seja feito através de matrícula e senha;
- Definir que os acessos aos computadores sejam feitos através de *login* e senha;
- Instalar e manter atualizados os antivírus dos computadores;
- Utilizar soluções tecnológicas através de software livre (Linux, Libre Office, etc.), visando economia e segurança.

7 CONSIDERAÇÕES FINAIS

Após o referencial teórico apresentado e análise das informações obtidas através da coleta de dados, foi possível estabelecer uma série de ações, que estão de acordo com a literatura e as normas técnicas vigentes. Através desses apontamentos, é possível estabelecer diretrizes a outros trabalhos, no sentido de propor melhorias na utilização dos recursos computacionais de forma segura e eficiente.

Este estudo está alinhado com os objetivos gerais e específicos definidos, para que esteja dentro de um escopo delimitado. As questões técnicas estão em nível facilitado de compreensão, para o melhor entendimento por gestores que queiram implementar diretrizes básicas envolvendo a segurança da informação em outras instituições, pois trata-se de um estudo rico em teorias.

Outro ponto importante, é que neste estudo não há citações acerca da Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), por um motivo considerado plausível, que seria a fuga da temática técnica e inserção em outra área do conhecimento, a do Direito, haja vista ser uma lei repleta de vetos, com a iminente criação de novas cláusulas e sem previsão para entrar em vigor. Além disso, várias medidas foram interpostas para que as empresas e instituições possam ter um tempo maior para adequação.

Em todo estudo foi possível perceber que, para que se obtenha uma política de segurança da informação, é necessário a participação dos usuários, gestores e pessoal técnico. É necessário orientar usuários das mais diversas organizações, para que seja possível identificar as possíveis ameaças e riscos, criando programas educativos que orientem sobre essas vulnerabilidades. Logo, assim como os sistemas físicos ou lógicos que impedem os intrusos de invadirem os computadores, a conscientização é fundamental para que haja um progresso nesse aspecto.

Por fim, ao se pensar em segurança da informação, deve-se entender que as ameaças possuem um poder de se desenvolver, de criar novos caminhos, de explorar novas vulnerabilidades a fim de atingir o seu objetivo. Para evitar seu sucesso, é necessário, trabalhar com um processo de construção de um modelo de segurança padronizado, que esteja de acordo com as normas vigentes, de forma persistente, constante, cíclico, que procure sempre melhorar e aperfeiçoar suas técnicas.

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: 2013.

_____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: 2013.

ALENCAR, Márcio A. S. **Fundamentos de redes de computadores.** Manaus: Universidade Federal do Amazonas, CETAM, 2010.

BARRETO, Alesandro G.; Brasil, Beatriz S. **Investigação Cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

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

BONIATI, Bruno B.; SILVA, Letícia S. **Fundamentos de desenvolvimento web.** Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2013.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 abr. 2020.

_____. Código Penal Brasileiro (1940). **Decreto Lei nº 2.848 de 1940**. Brasília: Presidência da República, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 30 abr. 2020.

_____. Lei Carolina Dieckmann (2012). **Lei nº 12.737 de 2012.** Brasília: Presidência da República, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 30 abr. 2020.

_____. Marco Civil da Internet (2014). **Lei nº 12.965 de 2014**. Brasília: Presidência da República, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 30 abr. 2020.

_____. MP nº 2.200-2 (2001). Medida Provisória nº 2.200-2. Brasília: Presidência da República, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm>. Acesso em: 21 abr. 2020.

BRITO, Edivaldo. **Segurança Wi-Fi: descubra qual é a melhor configuração para seu roteador.** Techtudo: 02 set. 2017. Disponível em < https://www.techtudo.com.br/dicas-e-tutoriais/2017/09/seguranca-wi-fi-descubra-qual-e-a-melhor-configuracao-para-seu-roteador.ghtml >. Acesso em: 16 abr. 2020.

CAMPOS, André. **Sistema de segurança da informação.** 2. ed. Florianópolis: Visual Books, 2007.

CARDOSO, André. **Por que há mais vantagens em usar o Linux.** Viva o Linux: 06 out. 2010. Disponível em: < https://www.vivaolinux.com.br/artigo/Por-que-ha-mais-vantagens-em-usar-o-Linux>. Acesso em 08 mai. 2020.

CARLOS, ANTÔNIO. **Sistema agiliza e dá tramitação de documentos no Tribunal.** Assessoria de Comunicação do TJMA, 2011. Disponível em: <https://tj-ma.jusbrasil.com.br/noticias/2523143/sistema-agiliza-e-da-tramitacao-de-documentos-no-tribunal>. Acesso em: 06 mai. 2020.

CERT.BR. **Cartilha de segurança para internet**. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 20 jan. 2020.

COELHO, Flávia E. S.; ARAÚJO Luiz G. S.; **Gestão da Segurança da Informação: NBR 27001 e 27002.** Rio de Janeiro: Escola Superior de Redes, 2013.

CÔRTE, Kelson. **Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos.** Brasília, 2014, 212p. Tese (Doutorado em Ciência da Informação). Faculdade de Ciência da Informação da Universidade de Brasília, Brasília, 2014.

Descubra todos os produtos AVG. **AVG**, 2019. Disponível em <https://www.avg.com/pt-br/store>. Acesso em: 04 mai. 2020.

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

Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. **G1**, 2014. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 21 abr. 2020.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2019. **Cert.br**, 2020. Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html>. Acesso em: 24 abr. 2020.

JESUS, Damásio; MILAGRE, José A.; **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down**. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais.** 11. ed. São Paulo: Pearson Prentice Hall, 2014.

LAUREANO, Marcos A. P. **Gestão de Segurança da Informação.** Curitiba: Pontifícia Universidade Católica, 2005.

MARANHÃO. Decreto de Criação da UNIREMA (2003). **Decreto 16.677 de 2003.** São Luís: Governo do Estado do Maranhão, 2020. Disponível em: <https://seati.ma.gov.br/decreto--de--criacao--da--unirema/>. Acesso em: 05 mai. 2020.

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

MARTINS, Elaine. **O que é Adware?.** Tecmundo, 24 set. 2008. Disponível em: <https://www.tecmundo.com.br/spyware/271-o-que-e-adware-.htm>. Acesso em: 22 abr. 2020.

MAZZOLA, V. B. **Arquitetura de redes de computadores**. Santa Catarina: Universidade Federal de Santa Catarina, 2000.

Melhores práticas para uso do e-mail corporativo. **Site Blindado**, 2018. Disponível em: <https://blog.siteblindado.com/melhores--praticas--para--uso--do--e--mail--corporativo/>. Acesso em: 04 mai. 2020.

MORIMOTO, Carlos E. **Redes, guia prático.** 2. ed. GDH Press e Sul Editores, 2008.

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

NOMIYA, Diogo V. **AES – Advanced Encryption Standard**. Dissertação (Mestrado em redes de computadores). Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010.

PANDINI, Willian. **Primeiros passos com a norma ISO 27000**. OSTEC Segurança Digital de Resultados. 02 jul. 2015. Disponível em: < https://ostec.blog/padronizacao-seguranca/primeiros-passos-iso-27000>. Acesso em 18 abr. 2020.

PAIM, Rodrigo R. **WEP, WPA e EAP.** Dissertação (Mestrado em redes de computadores). Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2011.

Segurança da Informação: Como foi o ataque dos sistemas de um grande banco chileno. **MTI Tecnologia**, 2018. Disponível em: <https://www.mtitecnologia.com.br/seguranca-da-informacao-como-foi-o-ataque-dos-sistemas-de-um-grande-banco-chileno/>. Acesso em: 23 abr. 2020.

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

SILVA, Gleydson M. S. **Guia Foca Linux**. v. 5.01. Gleydson Mazioli da Silva, 2020.

SILVA, Leonardo W. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA.** Folha de São Paulo, São Paulo: 12 ago. 2011. Disponível em: <https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml>. Acesso em: 12 abr. 2020.

SISP – Sistema Integrado de Segurança Pública. **Governo de Santa Catarina**, 2020. Disponível em: <https://www.ciasc.sc.gov.br/produto/sisp--sistema--integrado--de--seguranca--publica/>. Acesso em: 06 mai. 2020.

Sua proteção, do seu jeito. **Avast Software,** 2019. Disponível em: <https://www.avast.com/pt br/compare antivirus>. Acesso em: 04 mai. 2020.

TANENBAUM, Andrew S.; WETHERALL, David. Redes de Computadores. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

Top 7 Mobile Security Threats in 2020. **Kaspersky Lab**, 2020. Disponível em: < kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store>. Acesso em: 26 abr. 2020.

VEIGA, Pedro. **Tecnologias e Sistemas de Informação, Redes e Segurança.** Porto: Sociedade Portuguesa de Inovação, 2004.

APÊNDICES

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

APÊNDICE A – QUESTIONÁRIO DESTINADO AOS POLICIAIS MILITARES USUÁRIOS DOS COMPUTADORES DO QUARTEL DO COMANDO GERAL DA POLÍCIA MILITAR DO MARANHÃO

Seção Unidade do Policial Militar:

_____

Pergunta 01: Qual seu conhecimento sobre segurança da informação?

Não sabe nada ( )

Sabe pouco, apenas conceitos ( )

Entende bem e pratica ( )

Pergunta 02: Já teve algum treinamento sobre segurança da informação?

Não ( )

Sim, por conta própria ( )

Sim, promovido pela PMMA ( )

Pergunta 03: Você faz backup (cópia de arquivos) no computador que você utiliza no trabalho (escolha a alternativa com maior frequência)?

Não costuma fazer backup ( )

Sim, através de mídia removível (pen drive, CD, HD) ( )

Sim, através de serviços de armazenamento virtual (OneNote, Google drive, e-mail) ( )

Sim, através de um servidor de armazenamento da PMMA ( )

Pergunta 04: Sobre o uso de internet sem fio (Wi-Fi):

A seção/unidade não utiliza rede sem fio ( )

A seção/unidade usa rede sem fio, sem senha para acesso (livre) ( )

A seção/unidade usa rede sem fio, com senha para acesso ( )

A seção/unidade usa a rede sem fio, com acesso através da matrícula e senha ( )

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

Pergunta 05: Sobre a proteção antivírus no computador que você usa no ambiente de trabalho:

Não possui antivírus ( )

Possui antivírus, versão gratuita ( )

Possui antivírus versão paga ( )

Pergunta 06: Quantas pessoas utilizam o computador que você usa no ambiente de trabalho?

Apenas você SEM uso de senha para acesso/login ( )

Apenas você COM uso de senha para acesso/login ( )

O computador é compartilhado, SEM uso de senha para acesso/login ( )

O computador é compartilhado, COM uso de senha para acesso/login ( )

Pergunta 07: Com relação ao e-mail utilizado nas atividades administrativas:

Não utiliza e-mail para atividades administrativas ( )

Utiliza e-mail próprio/particular ( )

A seção possui um e-mail, porém não é institucional (@google, @hotmail) ( )

Utiliza um e-mail institucional para atividades administrativas (@pm, ou @ssp) ( )

Pergunta 08: Sobre os switches e roteadores utilizados na sua seção/unidade:

Ficam expostos, sem segurança física ( )

Ficam expostos, mas dentro de um rack com chave ( )

Ficam dentro de um CPD ou sala restrita dentro de um rack com chave ( )

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

APÊNDICE B –ENTREVISTA DESTINADA À CHEFIA DA DIRETORIA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO (DGTI) DA PMMA.

Pergunta 01: Existe algum protocolo ou portaria sobre a implantação de uma política de segurança da informação na Polícia Militar do Maranhão?

Pergunta 02: A DGTI presta serviços em quais áreas da TI?

Pergunta 03: Existe restrição ou bloqueio de acesso à internet aos usuários? A redes sociais, YouTube ou demais sites que fujam do interesse da administração?

Pergunta 04: Quais são os sistemas utilizados pela PMMA? E para quais finalidades?

Pergunta 05: A DGTI atua em todas as unidades da PMMA?

Pergunta 06: A DGTI possui servidores web, de rede, de correio eletrônico, de programas, e de armazenamento?

Pergunta 07: A DGTI capacita os usuários da PMMA para o bom uso dos computadores? Em especial, sobre segurança da informação?

Pergunta 08: A PMMA utiliza software livre para atividades administrativas? Especificamente Linux e Libre Office?

ANEXOS

ANEXO A: RELAÇÃO DE FOTOS RETIRADAS DO CAMPO DE PESQUISA

Figura 09: Vista aérea do Complexo do Comando Geral (CCG).

Fonte: Google Maps.

A Figura 07 mostra a vista aérea das áreas do comando geral, pois assim facilita o entendimento do que foi observado durante a pesquisa de campo.

REGIÃO A: Fachada principal do comando geral, local onde ficam as principais diretorias e seções administrativas, inclusive o gabinete do comandante geral.

Figura 10: Fachada do CCG A

Fonte: Próprio autor.

Figura 11: Fachada do CCG B

Fonte: Próprio autor

Figura 12: Fachada do CCG C

Fonte: Próprio autor.

Figura 13: Fachada do CCG D

Fonte: Próprio autor.

REGIÃO B: Lateral Direita do CCG, onde ficam situados o Regimento de Polícia Montada, acesso ao Centro Tático Aéreo e Presídio Militar.

Figura 14: Curral da Cavalaria da PMMA

Fonte: Próprio autor.

Figura 15: Sede da Cavalaria da PMMA

Fonte: Próprio autor.

REGIÃO C: Lateral Esquerda do CCG, onde ficam situados o Centro de Saúde da Polícia Militar, a quadra poliesportiva e a Diretoria de Apoio Logístico.

Figura 16: Lateral Esquerda do CCG A

Fonte: Próprio autor.

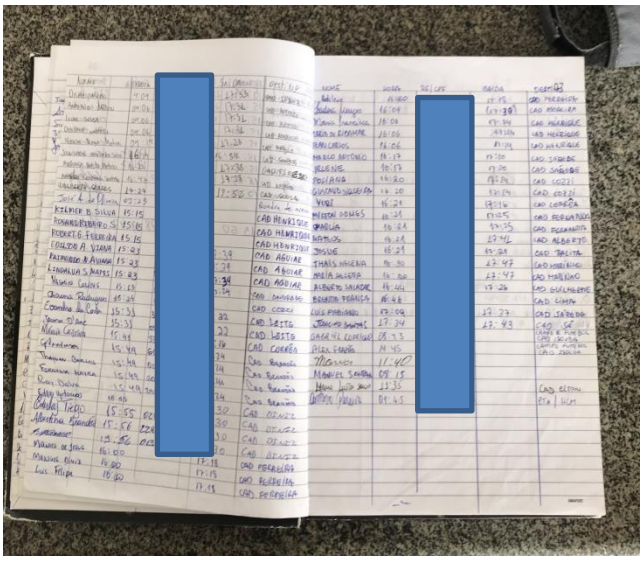
Figura 17: Lateral Esquerda CCG B

Fonte: Próprio autor.

REGIÃO D: Lateral Esquerda do CCG, onde ficam situados o Centro de Saúde da Polícia Militar, a quadra poliesportiva e a Diretoria de Apoio Logístico.

Academia de Polícia Militar Gonçalves Dias (APMGD):

Figura 18: Livro para cadastro de visitantes APMGD



Fonte: Próprio autor.

Figura 19: Sistema de Videomonitoramento APMGD

Fonte: Próprio autor.

8º Batalhão de Polícia Militar:

Figura 20: Fachada 8º BPM

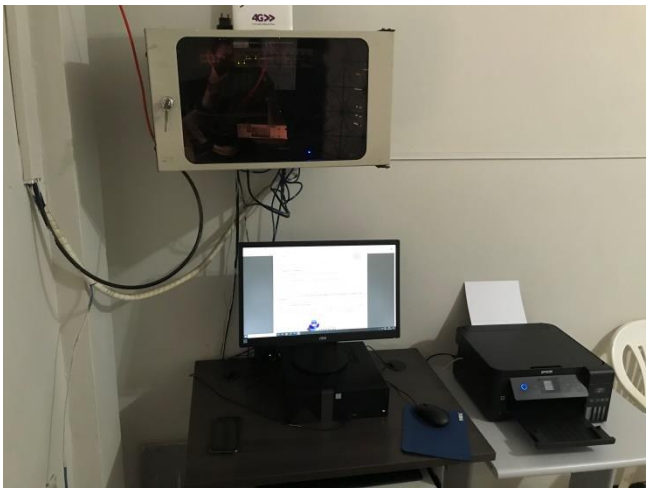
Fonte: Próprio autor.

Figura 21: Sistema de videomonitoramento 8º BPM

Fonte: Próprio autor.

ÁREAS INTERNAS:

Figura 22: Switch de rede com rack no 8º BPM



Fonte: Próprio autor.

Figura 23: Switch com função Wi-Fi na Diretoria de Pessoal, sem rack

Fonte: Próprio autor.

Figura 24: Roteador armazenado em rack

Fonte: Próprio autor.

Figura 25: Roteador Wi-Fi com Switch, exposto.

Fonte: Próprio autor.

Figura 26: Acesso único para carga e descarga

Fonte: Próprio autor.

Figura 27: Acesso restrito credenciado.

Fonte: Próprio autor.

ANEXO B: AUTORIZAÇÃO DA PESQUISA

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

Ofício nº 01/2020 – Monografia

São Luís, 04 de maio de 2020.

AO ILMO SENHOR
CORONEL QOPM PEDRO DE JESUS RIBEIRO DOS REIS.
COMANDANTE GERAL DA POLÍCIA MILITAR DO MARANHÃO
POLÍCIA MILITAR DO MARANHÃO

Assunto: Solicitação de levantamento de informações para monografia.
Anexo: Apêndice A (questionário) e Apêndice B (entrevista).

Ilustríssimo Comandante Geral,

Cumprimentando Vossa Senhoria, venho através deste solicitar informações referentes aos trabalhos desenvolvidos na Diretoria de Gestão da Tecnologia da Informação (DGTI), mais especificamente, sobre a aplicação de conceitos da Segurança da Informação.

Um dos objetivos desta pesquisa é propor medidas para o aumento da Segurança da Informação no Quartel do Comando Geral, aliando conceitos da literatura e das normas vigentes às atividades administrativas dos policiais militares durante o expediente, com o uso do computador e, assim, contribuir de forma positiva com as ações desenvolvidas pela DGTI.

Desta forma, para que esse objetivo seja alcançado de forma eficiente, faz-se necessário o emprego de diversas ferramentas para coleta dessas informações, tais como entrevista, questionário, análise do ambiente e consultas ao acervo (portarias e boletins).

Ao término, será enviado um relatório para a DGTI com propostas de melhorias para gestão, que analisará a possibilidade de implementar essas diretrizes.

Respeitosamente,

Paulo Edson Cutrim Silva

Paulo Edson Cutrim Silva – Graduando em Ciência da Computação
Capitão QOPM. Matrícula 1692243.
Universidade Federal do Maranhão

POLÍCIA MILITAR DO MARANHÃO
Gabinete do Comandante Geral
RECEBIDO
DATA 04/05/20 HORA 14:00
Protocolista

ESTADO DO MAR ANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
DIRETORIA DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO
Av. Jerônimo de Albuquerque s/n, Calhau – São Luís / MA - Cep: 65 074-200
Fone: 98 3227-5174 – email: cis@pm.ma.gov.br

RECEBIDO 25/05/20 17 15

AUTORIZO EM: 26/05/2020

São Luís - MA, 22 de maio de 2020.

Oficio Nº 135/2020 – DGTI

Do Cel QOPM Diretor da DGTI
Ao Sr. Cel QOPM CMT Geral da PMMA
Assunto: Consulta sobre aplicação de questionário - Of. 001/2020 - Monografia

Senhor Comandante Geral,

Em resposta ao despacho de seu gabinete sobre a análise e deliberação do Oficio nº 001/2020 – Monografia, confeccionado pelo Cap Edson Cutrim Silva, que versa sobre solicitação de informações referentes aos trabalhos desenvolvidos pela DGTI, especificamente, sobre a aplicação de conceitos da Segurança da Informação, passamos as seguintes observações:

1. Que as questões contidas no **Apêndice A**, endereçadas aos policiais militares usuários dos computadores do Quartel do Comando Geral foram analisadas e não incorrem em nenhum atentado no tocante aos procedimentos administrativos e operacionais da corporação;

2. De modo análogo, as questões contidas no **Apêndice B** que são endereçadas à chefia da Diretoria de Gestão da Tecnologia da Informação, também não trazem incompatibilidades e nem prejuizos nos âmbitos administrativos e operacionais da nossa Instituição.

Diante das análises, salvo melhor juizo, somos favoráveis a aplicação do questionário e da entrevista e recomendamos que o pesquisador, após o término contemple os resultados com o Comando da PMMA, a fim de que os mesmos sejam remetidos a esta Diretoria para que possamos utilizá-los em prol de análise da realidade e melhorias para a instituição.

Respeitosamente,

Cel QOPM – Eurico Alves da Silva Filho
Diretor da DGTI