ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1810)

MARCOS VINICIUS SADOCK CARIOCA

A SEGURANÇA DA INFORMAÇÃO CONJUGADA COM O EMPREGO TÁTICO: UMA PERSPECTIVA PARA OS BATALHÕES DE COMUNICAÇÕES EM 2018

Resende
2018

MARCOS VINICIUS SADOCK CARIOCA

A SEGURANÇA DA INFORMAÇÃO CONJUGADA COM O EMPREGO TÁTICO: UMA PERSPECTIVA PARA OS BATALHÕES DE COMUNICAÇÕES EM 2018

Trabalho de Conclusão de Curso apresentado à Academia Militar das Agulhas Negras como parte dos requisitos para a Conclusão do Curso de Bacharel em Ciências Militares, sob a orientação do Miquelângelo de Souza Dias 1º Ten Com.

Resende

2018

MARCOS VINICIUS SADOCK CARIOCA

A SEGURANÇA DA INFORMAÇÃO CONJUGADA COM O EMPREGO TÁTICO: UMA PERSPECTIVA PARA OS BATALHÕES DE COMUNICAÇÕES EM 2018

Trabalho de Conclusão de Curso apresentado à Academia Militar das Agulhas Negras como parte dos requisitos para a Conclusão do Curso de Bacharel em Ciências Militares, sob a orientação do Miquelângelo de Souza Dias 1º Ten Com.

COMISSÃO AVALIADORA

_____

Miquelângelo de Souza Dias 1º Ten Com – Orientador

_____

Resende

2018

Dedico este trabalho a minha mãe, que sempre se esforçou ao máximo em me educar e me ajudar quando precisei.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a minha mãe, Simone, por todo o incentivo que me deu e por todas as vezes em que se preocupou comigo, por todos os sacrifícios que fez para que me desse a melhor educação possível.

Gostaria de agradecer também ao meu pai, Marcos, que sempre utilizei de modelo e que se esforçou para que eu conseguisse atingir meus objetivos.

Por último, gostaria de agradecer a meu irmão, João Marcos, por todas as vezes em que, mesmo com diversas tarefas, me ajudava quando precisava.

RESUMO

CARIOCA, Marcos Vinicius Sadock. **A segurança da informação conjugada com o emprego tático:** uma perspectiva para os batalhões de comunicações em 2018. Resende: AMAN, 2018. Monografia.

Este trabalho tem por finalidade verificar as medidas de segurança da informação que devem ser utilizadas nos batalhões de comunicações do Exército Brasileiro enquanto estiverem sendo empregados taticamente, a fim de que sejam realizadas suas proteções cibernéticas, por meio de uma pesquisa exploratória. Vê-se que, nos dias atuais, existem diversos tipos de vulnerabilidades conhecidas, além de muitas outras que são descobertas constantemente. Desta forma, vários mecanismos devem ser utilizados para se garantir o emprego ideal dos sistemas de informação por parte das organizações, desde a capacitação dos recursos humanos à utilização de modernos softwares que as reduzem, para que não se comprometam os sistemas do batalhão e de todo o escalão que está sendo apoiado, garantindo o bom andamento da operação.

Palavras-chave: Segurança da informação. Vulnerabilidades. Mecanismos de segurança. Batalhão de comunicações. Proteção cibernética.

ABSTRACT

CARIOCA, Marcos Vinicius Sadock. **The information's Security united with the tactical employment:** a perspective to the signals battalions in 2018. Resende: AMAN, 2018. Monograph.

The purpose of this work is to verify, through an exploratory research, the measures of the information' s security to be used by deployed Signal Battalions of the Brazilian Army, in order to guarantee their cyber protection. It is a known fact that there are currently many types of vulnerabilities while more are constantly being discovered, so many mechanisms have to be utilized in order to provide the best employment of the information's systems. Therefore, the training of human resources and the use of modern softwares should not compromise the systems of the battalion or any of the organizations that are being supported; thereby ensuring the progress of the operation.

Key words: Information's Security. Vulnerabilities. Mechanisms of security. Signal's battalion. Cyber protection.

SUMÁRIO

1 INTRODUÇÃO

Teve-se como objeto de estudo do presente trabalho a segurança da informação dos sistemas de comunicações dos batalhões de comunicações do Exército Brasileiro.

O foco da pesquisa, por sua vez, foi delimitado nas medidas de segurança da informação que devem ser tomadas, dentro dos batalhões de comunicações do Exército Brasileiro em consonância com seus empregos táticos.

Já o objetivo do corrente trabalho foi identificar as medidas de proteção de sistemas informacionais necessárias à segurança da informação de um batalhão de comunicações enquanto sendo empregado taticamente.

Serão observados, a fim de se alcançar o objetivo geral, os seguintes objetivos específicos: apresentar vulnerabilidades da segurança da informação, apresentar mecanismos que devem ser implementados nos batalhões de comunicações a fim de reduzi-las e apresentar a utilização prática dos mecanismos dentro do emprego tático da arma.

Formulou-se, então, o seguinte problema de pesquisa: o que pode ser feito para reduzir as vulnerabilidades dos sistemas informacionais utilizados nos batalhões de comunicações enquanto estiverem sendo empregados taticamente?

Com o constante avanço da tecnologia, os sistemas informacionais também se desenvolvem, e, assim, tem-se sistemas mais eficientes. Porém, mesmo com tal desenvolvimento, existe a possibilidade de informações – que podem ser sigilosas – perderem seu sigilo e serem acessadas por quem não deveria.

> As organizações, seus sistemas de informações e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. (ABNT 2005, p. x)

Ainda, tem-se que, consoante Laureano (2005), todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros.

Desta forma, este estudo é relevante para o meio militar, uma vez que se deve sempre prezar pela segurança dos dados presentes nas organizações militares enquanto estiverem sendo empregadas taticamente, visto que, caso ocorra qualquer tipo de ataque supracitado, os dados podem ser roubados, bases de dados destruídas ou, ainda, o sistema de um batalhão pode ser comprometido, o que prejudica toda a operação.

Tendo sido feita por meio de uma pesquisa bibliográfica, a presente monografia está assim estruturada:

No primeiro capítulo, apresenta-se as diversas vulnerabilidades da segurança da informação, sejam físicas sejam lógicas. Para a elaboração deste capítulo utilizou-se como fontes principais monografias realizadas como Trabalhos por Conclusão de Curso e a Norma Brasileira de Regras, além de livros de especialistas na área.

No segundo capítulo são apresentados mecanismos que podem ser utilizados a fim de que sejam minimizadas as vulnerabilidades da segurança da informação. Utilizou-se como fonte monografias realizadas como Trabalhos por Conclusão de Curso e a Norma Brasileira de Regras, além de livros de especialistas na área.

No terceiro e último capítulo apresenta-se a aplicação prática dos mecanismos de redução das vulnerabilidades nos batalhões de comunicações conjugados com o emprego tático das organizações. Foram utilizados, como fonte, manuais do Exército Brasileiro, artigos e livros de especialistas na área e trabalhos realizados a respeito do assunto.

Faz-se necessário definir o conceito de sistema de informação (SI), que entende-se como fundamental para o desenvolvimento do assunto. Segundo Ralph (2002), são componentes inter-relacionados que coletam, manipulam, armazenam e disseminam dados e informações, fornecendo um mecanismo de realimentação a fim de atingir um objetivo.

Isto é, o sistema de informação de um batalhão de comunicações refere-se a todos os componentes pelos quais a informação — qualquer tipo de documento, relatório, manual, planilhas, arquivos, planos do batalhão, ordens verbais e escritas, normas e portarias — trafega, desde sua coleta até seu uso para atingir um objetivo. Como exemplo, tem-se o Plano de Defesa do Aquartelamento, o PDA, de um batalhão, que representa a informação. O sistema de informação, no caso, abrange desde a recepção dos dados por parte de quem o confeccionou, seu desenvolvimento propriamente dito, o lugar onde é guardado – seja em mídia, seja impresso – e sua disseminação aos militares do batalhão, que devem ter ciência do plano. Ao receber tal plano, os militares do batalhão iniciam um novo SI no momento da coleta.

Além disso, deve-se ter em mente que as Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI) regulam os procedimentos do militar ou do servidor civil ao utilizar recursos de Tecnologia de Informação de propriedade do Exército Brasileiro.

> Art. 2º Constitui objetivo destas Normas controlar o conteúdo das informações ou dados armazenados ou veiculados em pastas, arquivos ou mensagens, utilizando dispositivos de TI de propriedade do Exército, de modo a coibir a inserção de assunto ou matéria considerada ilícita, contrária à disciplina militar, à moral e bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros, e buscar a utilização mais adequada daqueles dispositivos. (BRASIL, 2007, p.2)

As mesmas normas, ainda, descrevem, em seu artigo 6º, como matéria ilícita a pornografia, o erotismo ou qualquer forma de discriminação, seja étnica, religiosa, ideológica, política, ou de gênero humano. No artigo 7º, por sua vez, há a expressa proibição de manter, distribuir ou veicular arquivos que estejam relacionados com os assuntos descritos em seu segundo artigo. Há a proibição, ainda, do constante no artigo 15:

> Art. 15. Não é permitida a utilização dos dispositivos de TI - de propriedade do Exército - durante o expediente da OM, para o acesso a sítios ("sites") da Internet com a finalidade de realizar cópias ("download") de jogos, filmes, música ou imagens, bem como para utilizar serviços eletrônicos ("on-line") de mensagem instantânea, com conteúdo estranho ao serviço, bem como a utilização dos mesmos dispositivos de TI para a realização de jogos eletrônicos e freqüentar salas de conversação ("chat"). (BRASIL, 2007, p.4)

2 REFERENCIAL TEÓRICO-METODOLÓGICO

O trabalho estará contido na grande área Defesa/Ciências Militares, na área 3.Cibernética, na subárea 3.1.Segurança da Informação com o tema 3.1.2.Política de Segurança da Informação.

2.1 Revisão da literatura e antecedentes do problema

Buscando identificar o que de mais relevante e atualizado tem sido produzido sobre o tema segurança da informação, foram pesquisados alguns autores; dentre eles, Dantas (2011) que conclui que a política de segurança da informação é a materialização da intenção do que se deseja fazer a fim de alcançar um padrão desejável de proteção para as informações.

Já conforme Rezende e Abreu(2000), as empresas estão procurando dar mais atenção ao ser humano, visto que ele é o responsável pelas engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório para ambas as partes, com objetivos comuns. Araújo(2014), por sua vez, aborda o tema chegando à conclusão de que a segurança cibernética é mais efetiva quando implementada pela própria organização, que deve possuir uma política de segurança da informação.

Dessa forma, pode-se abordar a teoria existente sobre o tema em questão da seguinte maneira: há uma corrente que defende que “as vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior vulnerabilidade” (DANTAS, 2011, p.30). Outra corrente, não menos importante, segundo Manduca (2015), parte da premissa de que mais do que processos bem definidos e recursos humanos capacitados, a segurança da informação necessita de mecanismos de proteção específicos, considerando que muitos requisitos de controle e prevenção só podem ser seguidos com o uso de soluções de hardware e software. A norma NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança da Informação (2005) aborda o tema de maneira a englobar as duas vertentes, levando em consideração tanto a importância dos recursos humanos quanto a parte de ferramentas de hardware e software.

A teoria que ampara a pesquisa pode ser assim resumida: diversos mecanismos devem ser utilizados a fim de que uma organização militar consiga reduzir suas vulnerabilidades da segurança da informação.

2.2 Referencial metodológico e procedimentos

Visando a confirmar o que é apresentado pela literatura formulou-se o seguinte problema de pesquisa: o que pode ser feito para reduzir as vulnerabilidades dos sistemas informacionais utilizados nos batalhões de comunicações enquanto estiverem sendo empregados taticamente?

Partiu-se da hipótese de que, conforme exposto anteriormente consoante Laureano(2005), não existem ambientes completamente seguros.

O objetivo foi identificar as medidas de proteção de sistemas informacionais necessárias à segurança da informação de um batalhão de comunicações enquanto empregado taticamente, e, especificamente, objetivou-se apresentar as vulnerabilidades que podem existir nos batalhões de comunicações, apresentar mecanismos os quais reduzem as vulnerabilidades que podem ser utilizados nos batalhões e apresentar a utilização prática dos mecanismos nos batalhões conjugados com seu emprego tático.

Para isso, foi realizada uma pesquisa bibliográfica visando a rever a literatura que fornecesse base teórica para prosseguir na pesquisa. Desse levantamento, destacam-se a NBR ISO/IEC 27002 - Código de Prática para a Gestão de Segurança da Informação (2005), Segurança da informação: uma abordagem focada em gestão de riscos, de Marcus Dantas(2011) e Gestão de segurança da informação, de Marcos Laureano(2005), além de Segurança da informação em ambientes organizacionais: uma abordagem bibliográfica, de Felipe Antônio Manduca (2015).

3 VULNERABILIDADES DA SEGURANÇA DA INFORMAÇÃO

Para que se entendam as vulnerabilidades da segurança da informação, faz-se necessário entender a definição de segurança da informação. Segundo a ABNT (2005), é definida como sendo a preservação da confidencialidade, da integridade e da disponibilidade da informação. Além disso, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Desta forma, precisa-se saber os seis conceitos: de confidencialidade, de integridade e de disponibilidade, além de autenticidade, responsabilidade, não repúdio e confiabilidade.

Segundo a ABNT (2005), o primeiro é a certeza de que a informação é acessível somente por pessoas autorizadas a terem acesso. O segundo, por sua vez, é a garantia da exatidão da informação e dos métodos de processamento. Já o terceiro é a garantia de que os usuários autorizados obtenham acesso à informação e aos dados sempre que necessitarem.

> Confiabilidade é a garantia de que a informação é confiável, oriunda de uma fonte autêntica e que expressa uma mensagem verdadeira. Tal conceito se relaciona diretamente com o de autenticidade, sendo este relacionado à fonte enquanto que aquele se relaciona com o conteúdo, se é verídico. (DANTAS, 2011, p.15)

Não repúdio, "a garantia de que a informação chegará ao destino certo e não será repudiada" (DANTAS, 2011, p.15). Por último, responsabilidade é a coparticipação de responsabilidades por todos os que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho (DANTAS, 2011, p.15).

"Cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança. Desta forma, podemos concluir que são as vulnerabilidades as principais causas das ocorrências de incidentes de segurança" (LAUREANO, 2005, p.18).

Para alcançar tal segurança, é preciso, então, que os sistemas de informações não possuam vulnerabilidades, que são definidas como "um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (ABNT, 2005, p.3), enquanto que um ativo é "qualquer coisa que tenha valor para a organização" (ABNT, 2005, p.1)

> Identificar as vulnerabilidades que podem contribuir para as ocorrências de incidentes de segurança é um aspecto importante na identificação de medidas adequadas de segurança. As vulnerabilidades estão presentes no dia-a-dia das empresas e se apresentam nas mais diversas áreas de uma organização. (LAUREANO, 2005, p.17)

Assim sendo, é de vital importância verificar os tipos de vulnerabilidades que podem prejudicar as organizações. Dantas classifica as vulnerabilidades em oito grupos, sendo as

principais para objeto de estudo, visando melhorias que podem ser feitas nos batalhões de comunicações, as físicas, de software, humanas e nas comunicações.

3.1 Físicas

Dantas(2011) define as vulnerabilidades físicas como as que dizem respeito aos ambientes em que estão sendo processadas ou gerenciadas as informações. Analisando outros autores do assunto, temos que, consoante Justi(2016, p.7), "A segurança física é muito importante para segurança dos dados também. Após definir a política de segurança, fica então determinado o que será protegido e como será protegido. É de extrema importância fazer com que os Centros de Processamento de Dados estejam fortemente seguros".

Além disso, temos ainda que:

> Além dos problemas que podem ser ocasionados pela natureza ou sem intenção de ocasionar danos, há outro fator que se deve ter um cuidado especial, o controle de acesso às instalações. Este controle visa impedir que estranhos ao ambiente, possuam acesso às dependências que armazenam e tratam dados e informações. Se não houver um rígido controle de entrada e saída, principalmente nos ambientes em que as informações estão armazenadas estas podem estar expostas a graves riscos. (MANDUCA, 2014, p.23)

Nota-se, assim, que este tipo de vulnerabilidade é muito relevante, necessitando, assim, de métodos de proteção, visto que podem ocorrer riscos tanto com relação à confidencialidade das informações – caso, por exemplo, alguém sem a devida autorização consiga acesso – como com relação à disponibilidade – caso, por exemplo, haja um incêndio não-controlado no ambiente.

3.2 De Software

> As vulnerabilidades de software são constituídas por todos os aplicativos que possuem pontos fracos que permitem acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede. Os principais pontos de vulnerabilidade encontrados estão na configuração e instalação indevida, programas, inclusive o uso de email, que permitem a execução de códigos maliciosos, editores de texto que permitem a execução de vírus de macro. (DANTAS, 2011, p.27)

As vulnerabilidades de software, então, podem vir a prejudicar todas as propriedades da segurança da informação: a confidencialidade, a integridade, a disponibilidade, a autenticidade, a responsabilidade, o não repúdio e a confiabilidade, visto que no caso de um

sistema ser acessado indevidamente, pode-se ocorrer qualquer tipo de ação com as informações ali presentes, desde exclusões até acréscimos de informações falsas.

3.3 Humanas

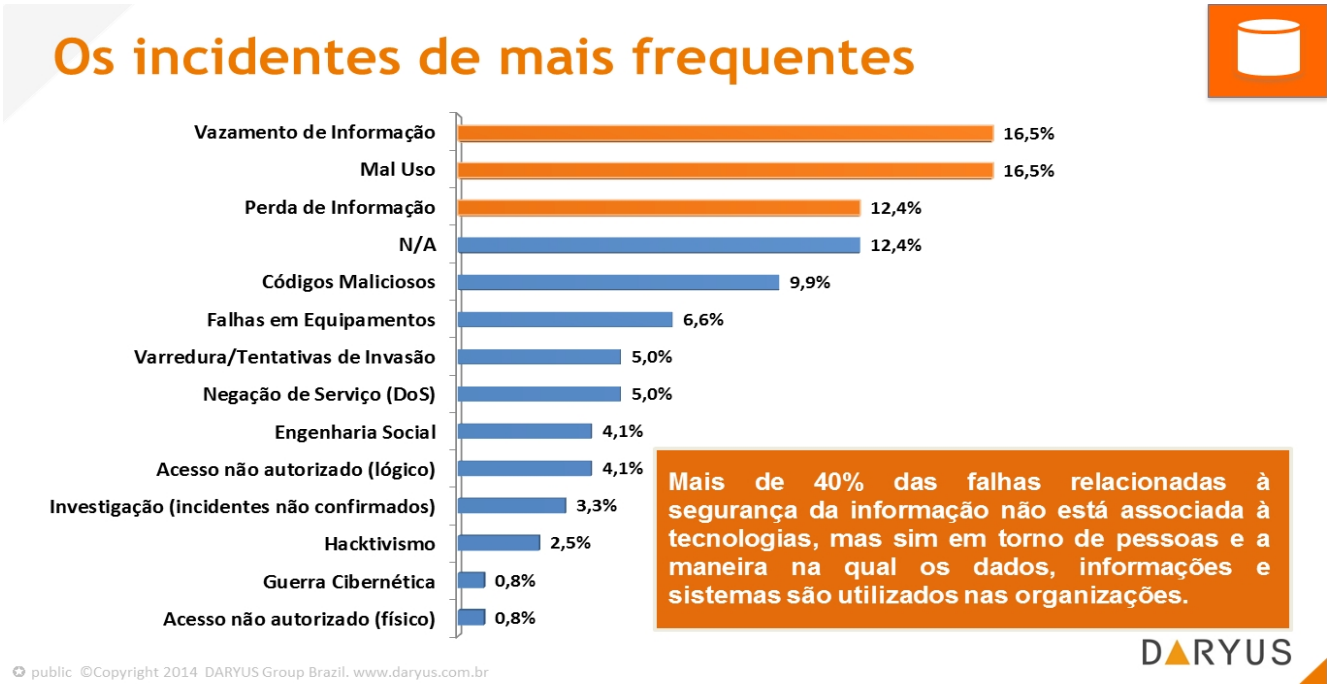

Figura 1: Pesquisa Nacional de Segurança da Informação 2014 – Principais Incidentes

É visto na Pesquisa Nacional de Segurança da Informação realizada no ano de 2014 que mais de 40% dos incidentes ocorridos estão relacionados às pessoas, sendo, então, as vulnerabilidades humanas de elevada importância para as organizações militares.

> As vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior vulnerabilidade. Sua origem pode ser: falta de capacitação específica para a execução das atividades inerentes às funções de cada um; falta de consciência de segurança diante das atividades de rotina; erros; omissões; descontentamento; desleixo na elaboração e segredo de senhas no ambiente de trabalho; não utilização de criptografia na comunicação de informações de elevada criticidade, quando possuídas na empresa. (DANTAS, 2011, p.28)

Desta forma, é essencial que sejam feitos esforços nos batalhões para que seja reduzido este tipo de vulnerabilidade. Ainda, temos a afirmação de Rosa (2012, p.30): "Declara-se que o 'elo mais frágil' da segurança de dados e informações confidenciais não está no sistema, e sim, na pessoa que interage com este sistema."

Vulnerabilidades deste tipo, quando exploradas, podem colocar em risco diversas propriedades da segurança da informação, visto que podem prejudicar a confidencialidade, no

caso de vazamento de informações, a disponibilidade, caso haja a perda de informação e todas as outras propriedades, caso alguma senha seja elaborada com desleixo – como aborda Dantas.

3.4 Nas Comunicações

> Está relacionado com o tráfego de informações. Estes tráfegos podem ser realizados através de fibra óptica, ondas de rádio, satélite ou cabos. O sistema de comunicação escolhido deve ser seguro de modo que as informações transmitidas alcancem o destino desejado e que não sofra nenhuma intervenção alheia. As informações deverão ser criptografadas e após alguma falha no processo a informação não deverá ficar disponível para pessoas não-autorizadas e muito menos perder sua confiabilidade. (NASCIMENTO)

Como aborda Nascimento, uma falha no processo do tráfego das informações poderá prejudicar tanto o indivíduo que não receberá a informação, perdida no processo, ferindo sua disponibilidade, como também a confidencialidade, visto que poderá estar disponível a quem não era autorizado, crescendo de importância a utilização de mecanismos que reduzam as vulnerabilidades desta categoria.

4 MECANISMOS DE PROTEÇÃO À SEGURANÇA DA INFORMAÇÃO

Segundo a ABNT (2005), a segurança da informação é conquistada com a implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Desta forma, é de grande importância que sejam estabelecidos todos os mecanismos possíveis para que se tenha a segurança da informação. Dentre todos os mecanismos existentes, podem ser destacados:

4.1 Firewall

> O firewall é uma solução formada por um ou vários componentes localizados em uma extremidade da rede organizacional por onde passa todo o fluxo de dados entre a organização e o mundo exterior, incluídos a Internet e outras redes corporativas. Ele tem por finalidade realizar a segurança, o controle, a autenticação e os registros de todo o tráfego realizado. Esse ponto único constitui um mecanismo para proteger a rede organizacional de uma rede pública não confiável. (ARAÚJO, 2014, p.48)

Thomas, (2007, p.125) por sua vez, aborda que "um firewall examina o tráfego enquanto ele entra em uma das suas interfaces e aplica regras ao tráfego, essencialmente, permitindo ou impedindo o tráfego baseado nestas regras". Assim sendo, o firewall é uma importante ferramenta que atua principalmente na redução das vulnerabilidades de software, tendo em vista que regula o tráfego da rede baseado nas regras previamente determinadas. É essencial, então, que essas regras de firewall sejam configuradas por pessoal capacitado, visto que, caso não seja configurado adequadamente, perderá sua eficácia.

Segundo Laureano (2005), podem ser divididos em duas grandes classes, sendo elas filtro de pacotes e servidores proxy.

Araujo (2014, p.48) expõe que "Os filtros realizam o roteamento de pacotes de maneira seletiva, ou seja, aceitam ou descartam pacotes por meio da análise das informações de seus cabeçalhos. Essa decisão é tomada de acordo com as regras de filtragem definidas na PSI da organização", sendo PSI a Política de Segurança da Informação.

> Um servidor Proxy caracteriza-se por agir como um sistema intermediário entre a Internet e a rede interna. É ele que faz a intermediação das solicitações entre os usuários e o mundo externo. À medida que o servidor Proxy faz estes encaminhamentos ele também pode iniciar o processo de cache das páginas web em disco local. Com isso, da próxima vez que um usuário fizer a requisição para a mesma página web, o servidor Proxy não precisa mais ir a Internet para obter a

> página, pois ela já está armazenada localmente, proporcionando economia de banda de Internet e maior agilidade para as pesquisas dos usuários. (ARAÚJO, 2014, p.49)

4.2 Criptografias

De um modo geral, a criptografia se define como, segundo Marciano (2006, p.176), "processo de cifragem (embaralhamento) dos dados de modo tal a permitir que apenas os conhecedores da chave associada sejam capazes de reverter o processo e ter acesso ao conteúdo em texto pleno" e é divida em criptografia simétrica, na qual tanto o transmissor como o receptor da mensagem utilizam a mesma chave, e assimétrica, na qual cada indivíduo possui um par de chaves – uma pública, para conhecimento de todos, e uma privada, de conhecimento exclusivamente próprio – sendo que apenas a pública é capaz de reverter o processo de criptografia feita com a privada e vice-versa.

Desta maneira, este processo é relativo às vulnerabilidades nas comunicações e provê os princípios da confidencialidade e da autenticidade, principalmente.

4.3 Capacitação de pessoal

Sendo basicamente relativo às vulnerabilidades humanas, este mecanismo, como já exposto, é considerado, por muitos, o mais importante. A capacitação de pessoal é o constante adestramento e preparo da tropa para que esteja apta a operar os mais diversos sistemas de comunicações. Desta forma, vê-se que não é valido empregar diversos equipamentos com modernas tecnologias de segurança se o usuário não consegue operá-los de maneira adequada.

> O estabelecimento de regras para o uso de computadores, e o entendimento dos riscos que a empresa esta exposta, é primordial para que os usuários comecem a entender os danos que eles podem causar usando de forma incorreta os recursos disponíveis. (MANDUCA, 2014, p.29)

4.4 Backups

Segundo Manduca (2014), os backups são cópias de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados. Desta forma, envolve o princípio da disponibilidade da informação.

Justi (2016) cita três tipos de *backups*, sendo eles o *backup full,* o *backup incremental* e o *backup diferenciado.* No primeiro, é realizada a cópia de todos os arquivos, sem exceções. No segundo caso, é feita a cópia somente dos dados que foram alterados desde a última cópia completa ou último *backup incremental*. O terceiro, por sua vez, é cumulativo, todos os dados que foram alterados desde o último *backup full* são copiados. Assim sendo, uma vez feito uma alteração em um arquivo, este constará em todos os diferenciais até que seja feito uma nova cópia completa. Apesar de mais demorado que o segundo, com este tipo e com o *backup full* é possível realizar a restauração completa dos dados, sem precisar procurar em cada cópia os arquivos que foram alterados, fato que ocorre com o incremental.

4.5 Controle de acesso

O controle de acesso, que é o controle de ingresso em determinado local, permitindo ou não a entrada do solicitante, deve ser realizado tanto fisicamente como na esfera virtual. No primeiro caso, segundo Manduca (2014, p.23), o mecanismo "visa impedir que estranhos ao ambiente possuam acesso às dependências que armazenam e tratam dados e informações. Se não houver um rígido controle de entrada e saída, principalmente nos ambientes em que as informações estão armazenadas, estas podem estar expostas a graves riscos", sendo nitidamente vista a redução das vulnerabilidades físicas.

No segundo caso, Justi (2016, p.2) trata que o controle de acesso "visa ter um controle dos usuários que estão acessando ou modificando as informações. Através do login, poderemos ter a hora e sua identificação para termos certeza de saber quem fez algo (intencionalmente ou não) de errado." Desta forma, vê-se que nas duas situações são afetados principalmente o princípio da confidencialidade, mas podem também prejudicar outros, como o da disponibilidade.

4.6 Sistema de Detecção de Intrusão - SDI

> A maneira mais comum para descobrir intrusões é a utilização dos dados das auditorias gerados pelos sistemas operacionais e ordenados em ordem cronológica de acontecimento, sendo possível à inspeção manual destes registros, o que não é uma prática viável, pois estes arquivos de logs apresentam tamanhos consideráveis. Nos últimos anos, a tecnologia de detecção de intrusão (*Intrusion Detection System – IDS*) tem se mostrado uma grande aliada dos administradores de segurança. Basicamente, o que tais sistemas fazem é tentar reconhecer um comportamento ou uma ação intrusiva, através da análise das informações disponíveis em um sistema

> de computação ou rede, para alertar um administrador e / ou automaticamente disparar contra-medidas. (LAUREANO, 2005, p.24)

Segundo Laureano (2005), os sistemas de detecção de intrusão podem ser classificados tanto quanto à origem dos dados tanto quanto à forma de detecção. No primeiro caso, podem ser tanto baseados no host, os quais monitoram tentativas de acesso à própria máquina em que se encontra, como baseados na rede, os quais monitoram a rede como um todo. Ressalta-se, ainda, que existem sistemas de detecção híbridos, que combinam ambas as técnicas.

No segundo caso, por sua vez, podem ser feitos por comparação com uma base de registros de ataques conhecidos, no caso da detecção por assinatura, ou por comparação com registros históricos de atividades consideradas normais, sendo qualquer desvio considerado uma ameaça, no caso de detecção por anomalia. Há ainda os híbridos, que combinam as duas abordagens supracitadas.

Podem, ainda, ser passivos ou reativos, como cita Santos (2010). O primeiro, ao detectar uma atividade suspeita, gera um alerta e o envia ao administrador da rede, enquanto que o segundo não só realiza o alerta como também responde à ameaça com ações pré-definidas, que costuma bloquear todo o tráfego do IP suspeito.

Em todos os tipos do sistema, são mitigadas as vulnerabilidades de software, já que monitora uma possível tentativa de explorar tal vulnerabilidade, garantindo diversos princípios, tais como de confidencialidade, disponibilidade e autenticidade, uma vez que, caso o acesso não fosse impedido, seria possível realizar qualquer tipo de alteração na informação presente naquele dispositivo.

4.7 *Virtual Private Network* - VPN

> A Virtual Private Network - VPN permite que informações, normalmente de negócios, trafeguem com segurança pela Internet. Os conceitos fundamentais da VPN são a criptografia e o tunelamento. A criptografia é utilizada para garantir a autenticidade, o sigilo e a integridade das conexões e é a base da segurança dos túneis, que permitem que os dados organizacionais trafeguem por uma rede pública através de um túnel criptografado. (ARAÚJO, 2014, p.50)

Laureano (2005, p.31), expõe que "a segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados." A VPN, então, conecta dois pontos por meio de um túnel, pelo qual os dados trafegam criptografados.

Assim, com o tunelamento e criptografia dos dados, mitiga vulnerabilidades relacionadas ao trâmite da mensagem, isto é, nas comunicações, garantindo diversas propriedades, como a confidencialidade, a integridade e a autenticidade.

4.8 Antivírus

> Um bom antivírus deve: identificar e eliminar todos os vírus conhecidos por seu banco de dados, fazer análise em tempo real dos arquivos que estão sendo baixados da internet, verificações agendadas de unidades de armazenamento como discos rígidos, e verificações transparentes ao usuário de unidades removíveis, como CDs, DVDs e pen drives, verificar os e-mails e anexos, atualizar sua base de dados diariamente de forma silenciosa. (MENDONÇA et al., 2010, p.2)

Conforme Justi (2016), "os antivírus possuem uma base de dados com os códigos dos vírus mais conhecidos. Faz-se necessário mantê-lo sempre atualizado para que o antivírus possa estar sempre detectando uma possível ameaça."

Vê-se que são de extrema importância, visto que, ao eliminar algum tipo de vírus, podem estar contribuindo para a manutenção de diversos princípios, tais como confidencialidade, integridade e disponibilidade, sendo mitigadas as vulnerabilidades de softwares.

4.9 *Network Address Translation* – NAT

> O NAT não foi criado com a intenção de ser usado como um componente de segurança, mas sim, para tratar de problemas em redes de grande porte nas quais a escassez de endereços IP representa um problema. Dessa forma, a rede interna pode utilizar endereços IP privados, sendo o NAT o responsável pela conversão desses endereços inválidos e reservados para endereços válidos e roteáveis quando a rede externa é acessada. Sob o ponto de vista de segurança, o NAT pode esconder os endereços dos equipamentos da rede interna e, consequentemente, sua topologia de rede, dificultando os eventuais ataques externos. (ARAÚJO, 2014, p.49)

Assim sendo, o NAT auxilia na segurança exercendo-a "por obscuridade", já que não é possível que elementos externos à rede consigam realizar qualquer tipo de ataque a um cliente da rede, somente ao equipamento que realiza esta função. Deve-se ressaltar que é mais seguro ter apenas um equipamento ligado à rede externa, visto que somente ele poderá ter suas vulnerabilidades exploradas, sendo mais fácil realizar a "hardenização" de apenas um equipamento do que de todos os clientes da rede. Assim sendo, vê-se que são mitigadas as vulnerabilidades de softwares, que não conseguirão ser explorados, garantindo a disponibilidade e confidencialidade das informações.

5 O BATALHÃO DE COMUNICAÇÕES: O QUE DEVE SER REALIZADO A FIM DE SE GARANTIR A SEGURANÇA DA INFORMAÇÃO CONJUGADO COM SEU EMPREGO TÁTICO

O Manual de Campanha EB70-MC-10.232 (2017), que trata sobre a Guerra Cibernética, define proteção cibernética como sendo a capacidade de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito, sendo uma atividade de caráter permanente.

> 5.1.3 No espaço cibernético, devido à complexidade e a permeabilidade dos sistemas de informação, torna-se imprescindível a realização de esforços para que haja uma organização e definição de responsabilidades. É necessária, ainda, a integração dos diversos setores envolvidos na operação, desenvolvimento e proteção dos sistemas computacionais.
> 5.1.4 Em situação de normalidade, caberá a cada órgão, civil ou militar, governamental ou privado, que possua atribuições ou seja integrante do espaço cibernético, realizar todas as ações necessárias para assegurar a existência e a continuidade da sociedade da informação da nação, garantindo e protegendo seus ativos de informação e suas infraestruturas críticas. (BRASIL, 2017, p..5-1)

O manual de guerra cibernética, ainda, define como missão do Batalhão de Comunicações a realização da proteção cibernética dos sistemas de informação do grande comando apoiado, sendo o comandante do batalhão responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da Força Terrestre Componente (BRASIL, 2017).

Consoante o manual do emprego das comunicações, “cada escalão da Força Terrestre possui seu elemento de comunicações, o qual tem por missão o planejamento, a instalação, a exploração e a manutenção do respectivo sistema de comunicações, bem como prover a segurança física das suas instalações” (BRASIL, 1997, p.1-1). O mesmo manual, ainda, cita a “necessidade de um sistema de comunicações confiável, de grande capacidade de tráfego, muito flexível, permitindo transmissão de mensagens em tempo real e que ofereça segurança face às atividades de guerra eletrônica (GE) do oponente” (BRASIL, 1997, p.1-2).

Nota-se, ainda, no emprego das comunicações, o princípio da segurança, definido por:

> Segurança - Todas as medidas são tomadas para proteger os sistemas de comunicações, de modo a impedir ou pelo menos dificultar a obtenção de informações pelo inimigo. A segurança das comunicações contribui significativamente para preservar a liberdade de ação do comando e garantir a surpresa (BRASIL, 1997, p.1-3).

Desta forma, a fim de cumprir sua missão, os batalhões devem utilizar diversos meios, métodos, procedimentos, tecnologias e mecanismos para assegurar o princípio supracitado,

sendo o chefe da seção de inteligência, o S2 da organização, o principal militar responsável por garantir a segurança da informação.

5.1 Firewall

A implantação deste mecanismo em um batalhão é de grande importância por causa de sua dupla finalidade exposta no capítulo anterior. Em primeiro lugar, o filtro de pacotes deve ser configurado de modo a seguir as prescrições contidas nas NORTI, visando coibir diversos tipos de ações que essas regras proíbem, como citado na introdução do presente trabalho. Desta forma, ao bloquear certos itens do cabeçalho durante a análise da informação, impede-se que sejam acessados os conteúdos, estando de acordo com o artigo 16 das mesmas normas, que expõe que as organizações militares que dispuserem de rede interna de transmissão de dados (LAN), com acesso franqueado à Internet, devem prover restrição de acesso a sítios ("sites") externos que contenham matéria ilícita.

Em segundo lugar, tem-se a funcionalidade dos servidores proxy, que atuam como intermediadores entre a internet e a rede interna. É possível, graças ao proxy, que o gerente da rede de cada batalhão realize o monitoramento das respectivas LAN e uma melhor análise forense computacional, tendo em vista que todas as requisições feitas por cada usuário da rede são registradas pelo proxy antes de serem encaminhadas às redes externas. Assim, cada militar da organização deve possuir seu próprio login e senha.

5.2 Criptografia

Conforme a Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações, deve-se **"**utilizar serviços criptográficos para o intercâmbio de informações (correio eletrônico corporativo, transferência de arquivos, etc.)" (BRASIL, 2011, p.7). A criptografia é um mecanismo indispensável quando da transmissão de mensagens esteja em operações ou não.

> Art. 26. Toda informação com classificação sigilosa, que seja armazenada, processada ou trafegue por ambientes de rede, deve ser submetida a processos que assegurem a sua confidencialidade, considerando não só o grau de sigilo da informação mas também a classificação, com base na importância da informação circulante, daqueles ambientes. (BRASIL, 2001, p.6)

Quando em operação, deve-se sempre seguir as Instruções para a Exploração das Comunicações e Eletrônica (I E Com Elt) que estiverem em vigor, visto que nelas estão previstos os processos, as senhas e outras padronizações a serem utilizados a fim de corroborar com a segurança das transmissões.

Assim, aplicativos que realizam a criptografia, como o Kleopatra, devem ser disponibilizados para todos os militares da organização que necessitarem realizar o trâmite de informações na rede.

5.3 Capacitação de pessoal

> Um dos primeiros passos para o processo de educação é o estabelecimento de políticas e regras de segurança. Fazer com que todos compreendam os riscos que o uso indevido de redes sociais, e-mails com conteúdo suspeito, download de arquivo, troca de informações sobre a empresa podem trazer, e assim aceitem completamente às regras e restrições estipuladas pelo administrador da rede. (MANDUCA, 2014, p.29)

A capacitação dos recursos humanos deve ser constantemente feita, prezando sempre pelo correto uso dos mecanismos de segurança e pelas normas de utilização dos equipamentos que o Exército Brasileiro prevê. Deve-se dar ênfase às instruções relativas à segurança da informação, que devem ser ministradas pelos chefes das seções de informática de cada organização, quando previstas na capacitação de quadros, e deve ser incluso na capacitação este tipo de instrução dos batalhões que não as possuírem. Além disso, deve ser solicitado aos militares que estiverem gerenciando a rede da organização ou qualquer rede de uma operação que realizem cursos no Instituto Rondon de Capacitação Continuada, o IRCC, que são feitos à distância, a fim de adquirirem maior conhecimento na área.

Também, deve-se cobrar dos militares que exercerem qualquer tipo de função que utilize dispositivos conectados a rede que tomem ciência da Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações, feita pelo Departamento de Ciência e Tecnologia do Exército Brasileiro, no ano de 2011, visto que nela estão presente diversas prescrições de uso da rede e ações que devem ser tomadas.

Por último, como expõe Araújo (2014), a organização deve assegurar que os funcionários, prestadores de serviço e terceirizados entendam as suas responsabilidades e estejam capacitados a desempenhar as funções para quais foram selecionados. Desta forma, antes de cada operação, devem ser testados os conhecimentos dos operadores de cada serviço,

a fim de que se garanta a correta utilização desses, sempre com a utilização dos mecanismos segurança da informação previstos.

5.4 Backups

Como aborda Justi (2016), as organizações realizam backups diários, mas infelizmente em alguns casos, os responsáveis pelo gerenciamento dos backups não se preocupam em realizar testes, para confirmar se o backup do correspondente dia foi feito com sucesso. Desta forma, cresce de importância que sejam testados antes de armazenados.

> Geralmente, uma atualização diária é pouco diante das necessidades da empresa, caso venha a sofrer algum dano. É recomendável também fazer um backup mensal, pois se por algum evento, a corporativa necessitar de dados passados, certamente os terá no backup mensal. (JUSTI, 2016, p.8)

Então, recomenda-se que os batalhões realizem um *backup full* mensalmente e, diariamente, um diferenciado. Assim sendo, facilmente o chefe da seção de informática da organização conseguirá recuperar qualquer dado que seja necessário.

Além de realizar os *backups*, é de grande importância que se tomem alguns cuidados, como cita Manduca (2014). Em primeiro lugar, ele expõe que nas cópias de segurança devem contar apenas arquivos confiáveis, citando que arquivos do sistema operacional ou que façam parte da instalação de softwares não devem fazer parte dos backups, visto que eles podem haver sido modificados ou substituídos por versões infectadas por vírus ou outras ameaças, para que não infectem um computador quando forem restauradas.

> Ao armazenar os backups, deve-se certificar que eles não ficarão expostos ao frio, calor, poeira ou umidade, pois estes agentes podem inutilizar a cópia. Por uma questão se segurança adicional deve haver um cuidado com acessos não autorizados onde os backups são armazenados e para prevenção contra incidentes naturais com incêndios e inundações que podem afetar a empresa. Os backups devem ser armazenados em dois ou mais lugares distintos.
> Para evitar que elas caiam em mãos erradas, o descarte das cópias antigas deve ser feito com cuidado, e em local adequado, de preferência deve-se inutilizar a cópia para depois descartá-la. (MANDUCA, 2014, p.28)

5.5 Controle de acesso

O controle realizado na esfera virtual é feito por meio do proxy do sistema, como exposto anteriormente. Na esfera física, Justi (2016) aborda que os Centros de Processamento de Dados (CPD) devem estar longe de materiais combustíveis, tubulações de água e esgoto, antenas de telecomunicações e estações de energia elétrica. Além disso, o mesmo autor ainda

cita que os centros devem conter também portas corta fogo. Recomenda, ainda, que a energia elétrica seja fornecida por no-breaks e que se faça a instalação de um gerador, para caso falte energia externa. Justi ainda menciona quatro mecanismos que os CPD devem conter:

> Sistema anti-incêndio - para que num possível incêndio não ocorra a perda dos dados;
> Refrigeração na sala - muito recomendável ter ar-condicionado para que o CPD1 tenha um controle de temperatura e umidade em torno de 22º C;
> Câmeras de Vigilância - estas filmagens devem ser gravadas e armazenadas para consultas futuras. É recomendado ter vigilância constante tanto internamente quanto no perímetro externo, configurando para que o alarme seja acionado com detecção de movimentos;
> Controle de Acesso – o CPD1 deve contar um sistema de controle eletrônico com mais de um nível de segurança, como por exemplo, cartão magnético e senha de acesso. Identificações como impressões digitais e íris são bem recomendadas. (JUSTI, 2016, p.7)

5.6 Sistema de detecção de intrusão - SDI

Como forma de aplicar o sistema de detecção de intrusão nas organizações, Santos (2010) cita duas principais ferramentas: o Snort e o OSSEC, que devem ser utilizadas em conjunto a fim de proporcionar ao gestor um controle tanto da rede como um todo tanto como de cada dispositivo nela conectado.

> O Snort é um sistema de detecção de intrusão Open Source baseado em redes, capaz de realizar análise de tráfego e captura de pacotes em tempo real em redes que utilizam o protocolo IP. Ele pode analisar protocolos, buscar por conteúdo específico, e pode ainda ser utilizado para detectar uma variedade de ataques e sondas. (SANTOS, 2010)

O mesmo autor ainda expõe que é possível integrar o Snort com Firewalls, transformando-o em um SDI reativo, por meio do SnortSam e o Snort-inline. Assim, esta ferramenta permite ao chefe da seção de informática do batalhão monitorar toda a rede do batalhão, dando-lhe ciência de possíveis ameaças e agindo ativamente contra elas.

A segunda ferramenta, por sua vez, é baseada em Host, monitorando e analisando o computador no qual se encontra. Tem como principais funções, segundo Santos (2010), a análise dos logs, a detecção de software malicioso, a integridade de sistemas e o envio de alertas e respostas ativas. Assim sendo, deve ser instalada, prioritariamente, em todos os servidores do batalhão, e, se possível, em todos os computadores.

5.7 *Virtual Private Network* – VPN

Como principal aplicação da VPN nos batalhões de comunicações tem-se a possibilidade de utilização da rede interna da organização sem a necessidade de se encontrar fisicamente no local, sendo os dados enviados por meio de tunelamento e criptografados, consequentemente com mais segurança. Assim, diversos militares podem utilizar serviços disponíveis na intranet do batalhão e do exército de suas casas, podendo cumprir tarefas em horários fora do expediente que demandem o acesso.

O OpenVPN é uma das ferramentas que podem ser utilizadas a fim de se montar a própria VPN, devendo o militar informar ao chefe da seção de informática a fim de que se tenha um controle sobre esse tipo de mecanismo.

5.8 Antivírus

O antivírus corporativo de uso das três Forças: a Marinha, o Exército e a Aeronáutica é o software fabricado pela Kaspersky Lab. Desta forma, deve ser solicitado, seguindo a cadeia de comando, que se adquira tal mecanismo a fim de se proteger os dispositivos do batalhão, sempre priorizando as máquinas que tenham informações sigilosas.

Em se tratando de sua configuração, deve ser priorizada a segurança da informação ao desempenho da máquina, tendo em vista que o mecanismo, que age constantemente, utiliza recursos do computador. Para que se tenha um equilíbrio, é recomendado que se faça uma verificação de todos os arquivos armazenados ao inicializar qualquer dispositivo e programar o antivírus para realizar uma varredura apenas nos arquivos novos, isto é, baixados na rede ou criados por qualquer tipo de programa.

5.9 *Network Adress Translation* - NAT

Apesar de todas as vantagens do mecanismo de NAT, visto que poderia ser utilizado no dispositivo que realiza a ponte entre a rede externa da organização e a rede interna, não é recomendado seu uso dentro da rede interna do Exército, devido à obscuridade que proporciona. No caso deste mecanismo for utilizado a fim de segregar a rede interna, sendo colocado por seções do batalhão, por exemplo, o chefe da seção de informática da organização não conseguirá executar um eficaz gerenciamento da rede, visto que ele não

saberá quantas máquinas estarão conectadas em determinada parte, apenas visualizará o dispositivo que estará realizando o NAT.

6 CONCLUSÃO

Esta pesquisa teve como objetivos apresentar as vulnerabilidades da segurança da informação, apresentar mecanismos que devem ser implementados nos batalhões de comunicações a fim de reduzi-las e apresentar a utilização prática dos mecanismos dentro do emprego tático da arma.

Os resultados encontrados foram que há quatro grupos de vulnerabilidades mais relevantes aos batalhões de comunicações quando em operação, sendo eles as físicas, as de software, as humanas e nas comunicações. Para que se possa reduzir essas vulnerabilidades, diversos tipos de mecanismos foram elencados: o firewall, as criptografias, a capacitação de pessoal, a utilização de backups, o controle de acesso físico e lógico, os sistemas de detecção de intrusão, as VPN's e os antivírus, considerando que o NAT não deve ser utilizado nas redes internas do Exército.

Dentre todas as vulnerabilidades, foi vista que a humana requer maior atenção, tornando de elevada importância a eficiente capacitação de pessoal dentro das organizações, visto que não adianta ter os mais modernos mecanismos se os recursos humanos não possuem capacidade de operá-los com eficiência em termos de segurança da informação. Apesar disso, cabe ressaltar que, dentro das operações táticas, todos os mecanismos devem ser utilizados, sendo as vulnerabilidades humanas apenas as de maior relevância.

Comparando os resultados desta pesquisa com a teoria que a sustentou, ressalta-se a afirmação de Dantas (2011, p.30): "as vulnerabilidades humanas constituem a maior preocupação dos especialistas, já que o desconhecimento de medidas de segurança é a sua maior vulnerabilidade" em detrimento da afirmação de Manduca (2015), o qual afirmou que a segurança da informação necessita, mais do que recursos humanos capacitados, de mecanismos de proteção específicos, considerando que muitos requisitos de controle e prevenção só podem ser seguidos com o uso de soluções de hardware e software. Desta forma, podem ser realizados trabalhos futuros sob a ótica específica das vulnerabilidades humanas, tendo seu foco em engenharia social e no processo de adestramento dos recursos humanos.

Diante dos resultados, pode-se afirmar que garantir a segurança da informação não é fácil, tampouco simples. Todos os mecanismos possíveis devem ser utilizados, e os chefes das seções de inteligência e de informática da organização em conjunto com sua equipe, bem

como todos os integrantes do batalhão, devem sempre estar preocupados com a missão do batalhão de comunicações prevista no manual do emprego das comunicações - o planejamento, a instalação, a exploração e a manutenção do respectivo sistema de comunicações – observando a necessidade de um sistema confiável, de grande capacidade de tráfego e muito flexível, que permita a transmissão de mensagens em tempo real e que ofereça segurança frente às atividades de guerra eletrônica do oponente, visto que pode-se prejudicar toda a operação do escalão apoiado caso algum procedimento seja negligenciado.

REFERÊNCIAS

ARAÚJO, Rubens Ferreira de. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:** Instrumento de defesa cibernética. 2014. 67 f. Tese (Doutorado) - Curso de Altos Estudos de Política Estratégia, Escola Superior de Guerra, Rio de Janeiro, 2014.

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

BRASIL. Ministério da Defesa. **EB70-MC-10.232**: GUERRA CIBERNÉTICA. Brasília: EGGCF, 2017.

BRASIL. Ministério da Defesa. **C11-1**: EMPREGO DAS COMUNICAÇÕES. Brasília: EGGCF, 1997.

BRASIL. Ministério da Defesa. **Cartilha Emergencial de Segurança** / Tecnologia da Informação e Comunicações, Versão 1.0. Brasília: EGGCF, 2011.

DODT, Cláudio. **Pesquisa Nacional de Segurança da Informação:** Divulgação dos resultados!. 2014. Disponível em: <https://www.profissionaisti.com.br/2014/11/pesquisa-nacional-de-seguranca-da-informacao-divulgacao-dos-resultados/>. Acesso em: 03 jan. 2018.

JUSTI, Ricardo de Melo. **SEGURANÇA DA INFORMAÇÃO NAS REDES CORPORATIVAS.** 2016. 10 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Presidente Antônio Carlos (unipac), Barbacena, 2016.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação.** 2005.

MANDUCA, Felipe Antõnio. **SEGURANÇA DA INFORMAÇÃO EM AMBIENTES ORGANIZACIONAIS**: UMA ABORDAGEM BIBLIOGRÁFICA. 2015. 43 f. Tese

(Doutorado) - Curso de Curso de Especialização em Redes de Computadores e Segurança de Redes, Universidade Tuiuti do Paraná, Curitiba, 2014.

MARCIANO, João Luiz Pereira. **Segurança da Informação:** uma abordagem social. 2006. 211 f. Tese (Doutorado) - Curso de Ciência da Informação, Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006.

MENDONÇA, Mônica Gonçalves De. et al. **Segurança em sistemas de informação**: Um estudo comparativo sobre os programas de antivírus e sistemas de firewall. 2010. 4 f. X Encontro latino Americano de Pós-Graduação. Universidade de Taubaté – UNITAU, Programa de Pós-graduação em Gestão e Desenvolvimento Regional. Taubaté, 2010.

NASCIMENTO, Nelson José do. **Ameaças e vulnerabilidades da informação**: Como precaver!. Disponível em: <https://www.portaleducacao.com.br/conteudo/artigos/educacao/ameacas-e/48819>. Acesso em: 25 mar. 2018.

RALPH, M. Stair e George W. Reynolds. **Princípios de sistemas de informação**: uma abordagem gerencial. 4a ed. Rio de Janeiro: LTC, 2002.

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação aplicada a Sistemas de Informação Empresariais**. Editora Atlas. São Paulo, 2000.

ROSA, Adriano Carlos. **Engenharia Social**: o elo mais frágil da segurança nas empresas. REAVI-Revista Eletrônica do Alto Vale do Itajaí, v. 1, n. 2, p. 29-40, 2012.

SANTOS, Victor. **Sistemas de Detecção de Intrusões (IDS – Intrusion Detection Systems) usando unicamente softwares Open Source.** 2010. Disponível em: <https://seginfo.com.br/2010/06/21/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-softwares-open-source/>. Acesso em: 15 jun. 2018.

THOMAS, Tom. **Segurança de Redes** – Primeiros Passos. Rio de Janeiro: Ciência Moderna, 2007.