ACADEMIA MILITAR DAS AGULHAS NEGRAS

ACADEMIA REAL MILITAR (1811)

Endrew Irineu Santos Silva

SEGURANÇA E DEFESA CIBERNÉTICA: LEVANTAR ASPECTOS DE POLÍTICA E SEGURANÇA APLICÁVEIS AO CONTEXTO DE UM BATALHÃO DE INFANTARIA

Resende

2019

Endrew Irineu Santos Silva

SEGURANÇA E DEFESA CIBERNÉTICA: LEVANTAR ASPECTOS DE POLÍTICA E SEGURANÇA APLICÁVEIS AO CONTEXTO DE UM BATALHÃO DE INFANTARIA

Projeto de pesquisa apresentado ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Orientador: Capitão Geraldo Magela de Oliveira Junior

Resende

2019

Endrew Irineu Santos Silva

SEGURANÇA E DEFESA CIBERNÉTICA: LEVANTAR ASPECTOS DE POLÍTICA E SEGURANÇA APLICÁVEIS AO CONTEXTO DE UM BATALHÃO DE INFANTARIA

Projeto de pesquisa apresentado ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Aprovado em ____de_____2019:

Banca Examinadora:

_____

Geraldo Magela de Oliveira Junior, Capitão

(Presidente/Orientador)

_____

Nívio Paula de Souza, Tenente Coronel

_____

Allanderson Rodrigues Teixeira, Major

Resende

2019

DEDICATÓRIA

Dedico aos meus pais.

AGRADECIMENTOS

Quero agradecer, primeiramente, ao meu bom Deus que me ajudou a chegar tão longe, concedeu-me força para ultrapassar todos os obstáculos até aqui. A caminhada foi longa, mas até aqui, Ele me sustentou. Aos meus pais, Francisco das Chagas Irineu Silva e Maria de Fatima da Silva Santos Silva, pessoas de maior sabedoria e de ótimos conselhos que não me deixaram desistir dos meus sonhos, a eles, agradeço por tudo até aqui. Ao meu irmão, Eddy Wallison Santos Silva, agradeço por todo apoio e orações pela minha vida e por também não me deixar desistir dos meus sonhos.

RESUMO

SEGURANÇA E DEFESA CIBERNÉTICA: LEVANTAR ASPECTOS DE POLÍTICA E SEGURANÇA APLICÁVEIS AO CONTEXTO DE UM BATALHÃO DE INFANTARIA.

AUTOR: Endrew Irineu Santos Silva

ORIENTADOR: Capitão Geraldo Magela de Oliveira Junior

O Batalhão de Infantaria Leve representa um inestimável instrumento de guerra para o Exército Brasileiro e serão apresentadas as suas características, possibilidades e limitações. Este trabalho tem como objetivo explorar a segurança da informação de um Batalhão de Infantaria Leve. Serão abordados o conceito de informação e formas como estas podem ser perdidas ou furtadas de equipamentos eletrônicos da organização. O trabalho consiste de pesquisas bibliográficas em fontes diversas e complementadas por cartilhas de segurança. Portanto, conclui-se que devem ser implantados requisitos mínimos de segurança no Batalhão de Infantaria Leve com o intuito de dificultar o acesso de pessoal não autorizado a informações que não lhe cabem respeito, comprometendo o grau de sigilo das informações que passam na devida unidade.

Palavras-chave: Infantaria; Segurança da Informação; Informação.

ABSTRACT

SECURITY AND CYBER DEFENSE: RAISING POLICY AND SECURITY ASPECTS APPLICABLE TO THE CONTEXT OF AN INFANTRY BATTALION.

AUTHOR: Endrew Irineu Santos Silva

ADVISOR: Capitão Geraldo Magela de Oliveira Junior

The Light Infantry Battalion represents an invaluable instrument of war for the Brazilian Army and its characteristics, possibilities and limitations will be presented. This task aims to explore the information security of a light infantry battalion and will address the concept of information, how it can be lost or stolen from the organization's electronic equipment. The work consists of bibliographical researches in several sources and complemented by safety booklets. Therefore, those minimum safety requirements should be implemented in the Light Infantry Battalion in order to make it difficult for unauthorized personnel to access information that does not concern them that does not by compromising the degree of confidentiality of the information that is passed in due course.

Keywords: Infantry; Information security; Information.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

CT	Centros de Telemática
CTA	Centros de Telemática de Aréa
DCT	Departamento de Ciência e Tecnologia
GLO	Garantia da Lei e da Ordem
OM	Organização Militar
SIC	Segurança da Informação e Comunicações
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
WWW	World Wide Web

SUMÁRIO

1. INTRODUÇÃO

Os incidentes no Japão, ao final da Segunda Guerra Mundial, envolvendo a utilização de armas para a destruição em massa em Hiroshima e Nagasaki, tornaram o mundo conhecedor de como as consequências de uma guerra podem ser devastadoras. Hoje, com os avanços tecnológicos, o mundo experimenta uma nova modalidade de Guerra, a de quarta geração, que tem se intensificado por meio de computadores, inteligência artificial e meios de comunicações. Tendo em vista a rápida propagação da informação, notou-se o surgimento das Fake News. Trata-se de notícias falsas que podem gerar conflitos em países, como aconteceu com os Rohingya, povo muçulmano originário de Myanmar, refugiado atualmente em países da Ásia. De acordo com a BBC Reality Check (2018), foram divulgadas fotos falsas da guerra civil em Ruanda , tiradas em 1975, com intuito de acusar o povo de Rohingya da prática de atitudes violentas. A propagação de imagens ilegítimas suscitou uma onda de violência que culminou no exílio de aproximadamente 600 mil pessoas rohingya, vítimas de limpeza étnica segundo a Organização das Nações Unidas.

As informações do parágrafo anterior podem ser exploradas, sendo importante problematizar a questão: O Exército Brasileiro, com diversas operações em GLO (Garantia da Lei da Ordem) e intervenções federais, possui informações sigilosas que não devem ser obtidas pelo inimigo, logo, qual política da segurança da informação pode ser aplicada para aumentar o bom emprego da tropa nessas missões?

Com base nesse questionamento, este trabalho tem o propósito de levantar aspectos da segurança da informação, especialmente, sua aplicação em um Batalhão de Infantaria Leve. Requisitos mínimos de segurança serão propostos a todos que frequentam o mesmo ambiente de trabalho, com o intuito de aperfeiçoar a segurança de informações.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Levantar aspectos de segurança da informação em um Batalhão de Infantaria Leve.

1.1.2 Objetivos específicos

Caracterizar um Batalhão de Infantaria Leve

Definir Segurança da informação e comunicação

Estabelecer requisitos mínimos da segurança da informação em um Batalhão de Infantaria Leve

Avaliar a gestão de segurança da informação para um Batalhão de Infantaria Leve

2. REFERENCIAL TEÓRICO

2.1. Batalhão de Infantaria Leve

No território brasileiro, a infantaria leve eclodiu com a necessidade da Força Terrestre de uma unidade dotada de grande flexibilidade e capacidade operacional, com requisitos de locomover-se com agilidade e eficiência em qualquer zona do território nacional. Uma das tropas mais compatíveis à execução de operações de assalto aeromóvel (Op Ass Amv; BRASIL, 1996, p. 1-1).

A infantaria leve representa um inestimável instrumento de guerra, com a capacidade de cooperar para a decisão do combate nas operações. Não se estende de uma infantaria que se desvestiu de seu material, arsenal e equipamento peado de seus meios de transporte orgânicos. Refere-se a uma tropa de grande flexibilidade, propícia a guerra continuada, inclinada para o cumprimento de atividades que demandam a aplicação de estratégias especiais de combate, para abismar o inimigo e facilitar o seu extermínio. (BRASIL,1996, p.1-2)

2.1.1 Características

A infantaria leve se diferencia dos outros tipos de infantaria devido ao destaque de seus materiais de dotação e suas características que são: (BRASIL,1996, p.1-3).

a. Apropriada para executar de Op Ass Amv;

b. Apropriada para realizar infiltrações através das posições inimigas e atacar seus flancos e retaguarda;

c. Orientada para a realização de ações ofensivas;

d. Adota a surpresa como seu fundamental princípio tático;

e. Obtém a surpresa por intermédio da velocidade e agressividade;

f. Possui excelente mobilidade em terreno restrito e sob condições de pouca visibilidade;

g. Opera independentemente de eixos de suprimento e de comunicações;

h. Seus homens são dotados de elevada iniciativa e criatividade.

2.1.2 Possibilidades

A infantaria leve destaca-se, dentre outros aspectos, por sua enorme flexibilidade. O comandante da força que encaixa uma determinada unidade dessa propriedade, ciente de suas fraquezas e capacidades, possuirá uma inestimável ferramenta para ser utilizada com o intuito de agir em proveito da força como um todo, operar funções que descomplicarão ou decidirão o êxito da missão. Suas peculiaridades colaboram para que suas possibilidades se tornem transcendentes às suas fraquezas. Todavia, para que tenha um alto índice de cumprimento de missões, independentemente da categoria da operação que esteja sendo praticada, faz-se indispensável que o escalão superior fortifique essa força com meios de apoio ao combate e apoio logístico. Isso irá diminuir as possíveis chances de insucesso do cumprimento da missão. Essas necessidades de apoio serão erguidas pelo comandante do batalhão, após ter efetuado uma judiciosa análise da missão (BRASIL,1996, p. 1-3).

Dada a concepção e a forma de execução da operação, poderão ser exploradas certas possibilidades: (BRASIL,1996, p. 1-4)

> (1) Realizar operações de assalto aeromóvel, organizando-se em uma força-tarefa aeromóvel;
>
> (2) Atuar, com elevado desempenho no combate noturno e na infiltração tática;
>
> (3) Executar operações sob quaisquer condições de terreno e/ou condições meteorológicas;
>
> (4) Operar como um todo, ou parceladamente, de acordo com a missão a ser cumprida;
>
> (5) Participar de operações inerentes a uma força de ação rápida (FAR);
>
> (6) Participar de operações aeromóveis e aerotransportadas;
>
> (7) Participar de uma força combinada;
>
> (8) Realizar operações no âmbito de um quadro de defesa interna e defesa territorial;
>
> (9) Cooperar nas operações envolvendo grandes unidades (Mec, Bld e Mtz), normalmente sob o controle operacional dos escalões brigada e divisão de Exército;
>
> (10) Compor subunidades ou frações, com os meios existentes, de acordo com a missão a ser cumprida;
>
> (11) Deslocar-se rapidamente, mesmo a grandes distâncias, utilizando-se de meios aéreos adequados, ou outros meios postos à disposição;
>
> (12) Participar de operações visando desorganizar as ações inimigas.

2.1.3 Limitações

Criada para ser utilizada de forma particular, o Batalhão de Infantaria Leve – BIL, possui mudanças relevantes em contraposição às demais unidades de infantaria. Aponta individualidades, basicamente no que tange à estrutura organizacional, pessoal, material, de armamento e equipamento (BRASIL,1996, p. 1-4).

É perceptível que essas características, somadas ao propósito da unidade em especial, resultam em limitações que necessitarão ser levadas em conta quanto a sua utilização. Essas limitações estão listadas abaixo: (BRASIL,1996, p. 1-4)

> (1) Capacidade de durar na ação, com seus meios orgânicos, restrito a um período de 48 (quarenta e oito) horas;
>
> (2) Vulnerável quando operando em terrenos abertos;
>
> (3) As operações de assalto aeromóvel são dependentes das condições climáticas e meteorológicas;
>
> (4) Mobilidade tática restrita a do homem a pé;
>
> (5) Reduzido apoio de fogo e apoio logístico orgânicos que limitam sua capacidade de durar na ação;
>
> (6) A maioria de seus meios orgânicos de transporte destinam-se, basicamente, ao comando e controle, ao apoio de fogo e apoio logístico;
>
> (7) Limitada proteção antiaérea;
>
> (8) Limitada proteção contra blindados;
>
> (9) Limitada ação de choque;
>
> (10) Limitada proteção contra os efeitos de armas químicas, biológicas e nucleares.

2.1.4 Missões

As missões características ao Batalhão de Infantaria Leve serão enumeradas, dada a apresentação de possibilidades e limitações elencadas no tópico anterior. Concerne de tarefas de caráter geral, com que essa unidade está direcionada, e se destinam às operações ofensivas e às defensivas: (BRASIL,1996, p. 1-5)

> a. Conquistar e manter, por tempo limitado, objetivos à retaguarda do inimigo, sob quaisquer condições ambientais, realizando operações de assalto aeromóvel e infiltrações terrestres, a fim de cooperar com a manobra do escalão superior.
>
> b. Infiltrar-se através das posições defensivas inimigas, durante a noite, antecedendo o ataque, para:
>
> (1) neutralizar seu comando/controle, apoio de fogo e apoio logístico;

> (2) bloquear uma vias de acesso de suas reservas;
>
> (3) abrir brechas através de obstáculos preparados;
>
> (4) assegurar vias de acesso, principalmente, em terreno difícil de ser transposto, para forças consideradas pesadas;
>
> (5) atuar contra os flancos e retaguarda;
>
> (6) fixar formações inimigas maiores, por meio da manobra, do seu apoio de fogo orgânico e dos fogos colocados em reforço, para permitir que outras forças possam manobrar.
>
> c. Isolar localidades, por meio da conquista de acidentes capitais e controle das vias penetrantes.
>
> d. Ser empregado em ações que devam ser desencadeadas no interior de localidades, tais como graves perturbações da ordem; controle e defesa de instalações vitais (de utilidade pública), e proporcionar segurança e/ou isolamento de algumas instalações.

2.2 Segurança da informação

2.2.1 Segurança da informação e comunicação

"Segurança da informação é a proteção da informação de diversos tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio" (ABNT, 2005).

Observa-se que são muitos os indivíduos que acreditam que a segurança da informação se refere à obtenção de ferramentas e sistemas com preços exorbitantes como, por exemplo, firewalls, sistemas de localização de intrusos ou antivírus. Muitos presumem que a adoção de políticas de defesa e a implantação de cuidados funcionais ao mecanismo tecnológico é suficiente. Entretanto, nenhum desses questionamentos é capaz de prevenir perdas se forem aplicados de forma solitária e imprudente (SÊMOLA, 2014).

A segurança da informação pode ser vista como uma ciência não exata devido à forte influência do fator humano. Na hipótese de classificá-la, a mesma estaria na área da gestão de risco. Segundo Sêmola (2014, p. xviii), "E para gerir riscos é preciso conjugar vários verbos: conhecer, planejar, agir, auditar, educar, monitorar, aprender e gerenciar não apenas alguns deles."

2.2.2 Informação

A informação é uma coleção constituída de dados que estabelece uma mensagem sobre um decidido acontecimento ou episódio. As informações permitem que problemas sejam resolvidos e

a tomada de decisões possa se tornar mais fácil, aliada ao conhecimento, e por isso, devem ser defendidas (SÊMOLA, 2014).

No momento em que falamos da segurança da informação, um pequeno número de perguntas sucintas deve ser respondido:

- O que defender? Ter noção de que não é somente uma reunião de dados, e sim ativo de dados de enorme valor para a instituição.

- Por que defender? Essas informações são o alicerce para a tomada de medidas, visto que sem as medidas de proteção certas, tais informações podem cair em mãos erradas, lesando desta maneira o prosseguimento da instituição.

- Defender de quê? Posto que as informações não se criam, mexem ou se anulam sozinhas, existe o contato com indivíduos e/ou sistemas computacionais de processamento ou dispositivos de armazenamento e esse contato deve ser fiscalizado e controlado para impedir que o próprio efetivo ou terceiros roubem, corrompam ou eliminem informações de suma importância para o batalhão.

Como defender? A preservação da informação não se restringe a dados, papéis ou dispositivos de armazenamento, é necessário a existência de normas dentro de um batalhão que definam quem, como, quando e onde possa ocorrer permissão a sistemas, arquivos ou documentos (SÊMOLA, 2003).

2.2.3 Tratamento da informação

Provindo da suposição que não há dados cem porcento seguros, é substancial para as organizações dar atenção ao seu ativo mais valioso, a informação. O segredo para o êxito na segurança da informação é a administração aliada a estratégias de segurança, visto que ambas em concordância fornecerão uma ampla qualidade de serviço. (SÊMOLA, 2003; MARCIANO, 2006).

Um Batalhão de Infantaria Leve preparado para realizar missões em qualquer lugar do Brasil possui uma grande rotação de informações de cunho estratégico e que não devem ser expostas. É de suma importância que se busque uma ótima gestão de segurança por todo efetivo que circula no Batalhão, desde o mais moderno ao mais antigo da unidade, e também aos que não circulam. Impor requisitos mínimos de segurança à unidade é válido para evitar que informações e

dados sejam furtados dos equipamentos eletrônicos como, por exemplo, celulares e notebooks, ou transmitidos pelos próprios militares em diversas mídias sociais existentes na atualidade.

2.3 Riscos de perda de informações

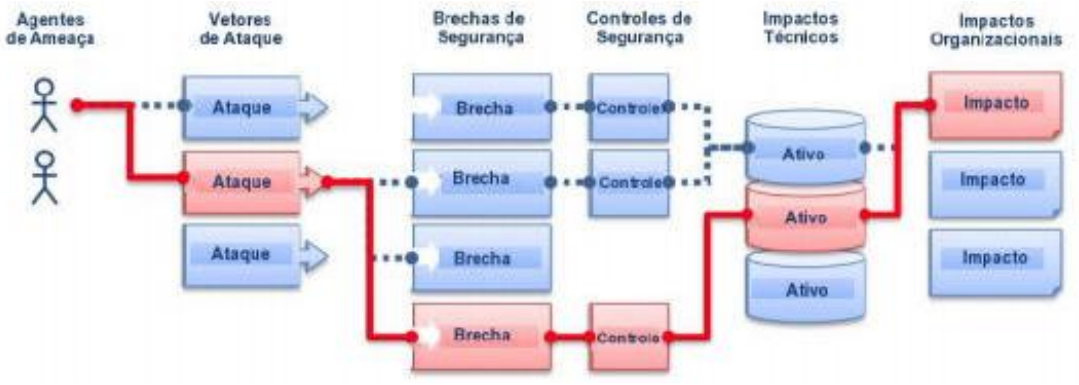
2.3.1 Softwares Maliciosos

A vulnerabilidade da rede permite que diversos indivíduos a explorem de inúmeras formas, através de falhas no projeto, efetivação ou configuração de um software ou um sistema operacional. O acesso irrestrito permite que os sistemas sejam explorados por pessoas que detém o conhecimento informático, essas redes acabam sendo violadas, deixando exposta a segurança do computador (MARTINS, 2012). Segundo Alves:

> Uma rede mal configurada seria comparável a deixar uma porta entreaberta numa vizinhança perigosa: Mesmo que não aconteça nada por um tempo, eventualmente alguém notará e tentará usar tal brecha oportunamente. Para isso, contam com diversos meios de ludibriar a rede, captando informações ou abrindo brechas para futuros ataques, de modo a pôr em risco a segurança e integridade da rede. (AZEVEDO, 2007, p.4)

A redes do Exército Brasileiro e dos batalhões não estão imunes aos problemas de exploração de seus sistemas e roubos de suas informações sigilosas. Os invasores utilizam-se de várias técnicas para iniciar uma invasão ou derrubar um sistema através da análise minuciosa da forma mais eficiente para o ataque, assentado, é claro, nas vulnerabilidades encontradas. Observe a figura 1.

Figura 1: Diagrama de invasão.



Fonte: <https://www.owasp.org/index.php/Top_10_2010-Main> Acesso em abril de 2019.

Os principais meios utilizados para a invasão e interferência nas informações de outrem e redes de indivíduos que carregam em seu dia a dia dados de suma importância para a Organização Militar, todos focados nas deficiências do sistema, serão expostos a seguir.

1)Vírus

Todos os dispositivos móveis possuem informações dentro de si. O pendrive é um grande expoente dentro das unidades militares, porém os mesmos devem ser usados de forma correta para que as informações que estão contidas não sejam corrompidas por vírus. O que exatamente é um vírus?

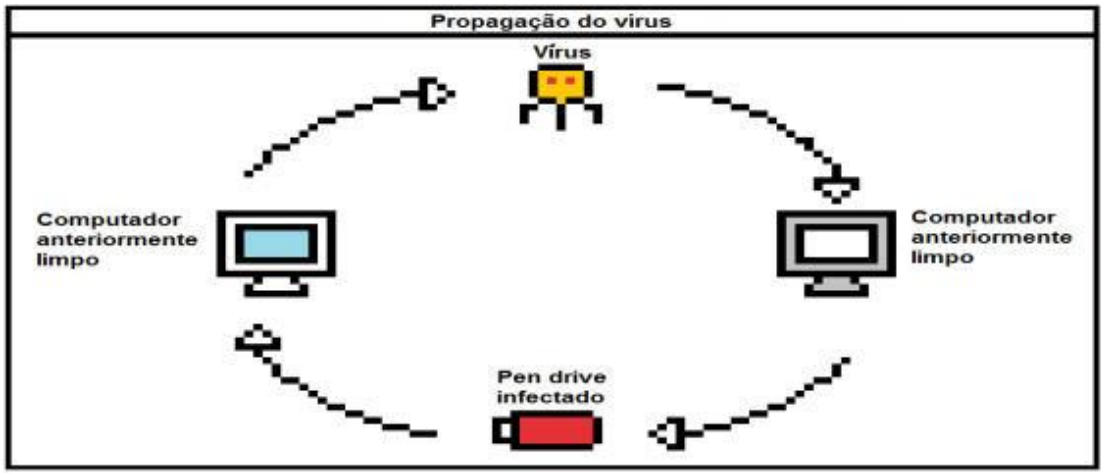
Vírus, habitualmente, são minúsculos programas instalados no computador do utilizador com a finalidade de causar danos, sejam roubando dados pessoais, senhas ou mesmo lesando o computador que esteja instalando.

Segundo Costa et al (2009),

> Spyware, Spy em inglês, significa espião e foi com essa característica que os spywares surgiram. Ele funciona com um simples objetivo roubar informações pessoais como login e senha, em devidos casos o spyware também agem para a modificação de configurações do computador (como a pagina home do seu navegador). Trojan Horse significa (cavalo de Tróia) é um código malicioso que faz passar por outro programa qualquer e que acaba criando vulnerabilidade no computador infectado, possibilitando na maioria dos casos, a infecção deste por outros malwares.

De certa forma, o efetivo de um Batalhão de Infantaria ou qualquer unidade do Exército Brasileiro não deduz que o vírus está instalado no computador ou, quando percebem, o dispositivo computacional já se encontra contaminado pelo invasor. Uma forma simples desses de infectar o computador é inserindo mídias contaminadas, como por exemplo, pendrives que são os mais vistos na rotina do militar. Observe na figura 2 como é feita a propagação do vírus:

Figura 2: A propagação de um vírus



Fonte: OLIVEIRA, 2015.

Pelos dados expostos, deve-se orientar o efetivo do batalhão ao manuseio dos pendrives nas máquinas da unidade, pois há possibilidade de o vírus ter acesso aos conteúdos sensíveis da unidade, senhas e informações que de fato são importantes para o cumprimento da missão.

Segundo MEDEIROS et al (2001, p.35):

> Uma vez conhecidos as principais ameaças e técnicas utilizadas contra a segurança da informação, podem-se descrever as principais medidas e ferramentas necessárias para eliminar essas ameaças e garantir a proteção de um ambiente computacional.

A predominante ameaça à segurança das informações nos batalhões são as próprias pessoas. No século atual, problemas decorrentes da intervenção humana não costumam estar associados a atos que têm por finalidade prejudicar a unidade de serviço. De outro modo, o maior número das intercorrências de segurança acontece por ausência de informação, processos e prescrições ao recurso humano, muitas vezes não explicitadas ao novo contingente da organização militar.

2) Trojan

Segundo o site Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil o Cavalo de Troia, trojan ou trojan horse:

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

São exemplos de trojan programas habitualmente instalados por usuários de internet, advindos de websites, simulando gifs, álbuns de fotos, jogos e propagandas. Não obstante, rotineiramente esses programas necessitam de apenas um clique dos usuários para serem instalados e executados automaticamente no sistema do atual computador, por isso o efetivo do Batalhão deve estar atento quanto à utilização de sites com tais ameaças à segurança da informação.

Os trojans também podem ser inseridos por agressores que, após invadir a máquina, modificam programas já existentes na mesma e, apesar de manter suas atribuições originais, também executam condutas maliciosas.

Existem diferentes tipos de trojan classificados de acordo com as respectivas ações maliciosas que habitualmente desempenham ao infectar o sistema do computador. Observe o quadro 1.

QUADRO 1 – Classificação dos Trojans.

Tipo	Função
Trojan Downloader	Instala outros códigos maliciosos, obtidos de sites na Internet.
Trojan Dropper	Instala outros códigos maliciosos, embutidos no próprio código do trojan.
Trojan Backdoor	Inclui backdoors, possibilitando o acesso remoto do atacante ao computador.
Trojan DoS	Instala ferramentas de negação de serviço e as utiliza para desferir ataques.
Trojan Destrutivo	Altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
Trojan Clicker	Redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
Trojan Proxy	Instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.
Trojan Spy	Instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
Trojan Banker ou Bancos	Coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy porém com objetivos mais específicos.

Fonte: Elaborado pelo autor, baseado no site cartilha.cert.br. Abril, 2019.

2.4. Prevenção

A melhor forma de prevenção seria através da elaboração de uma cartilha de segurança aos novos militares que estão chegando ao batalhão, instruindo-os quanto à utilização dos dispositivos de mídia, com intuito de não perder informações ou as mesmas serem corrompidas por vírus. Outra forma de prevenção é atualização periódica do software de segurança, providenciando soluções cabíveis ao decorrer do tempo com a descoberta de novos problemas. É recomendada a utilização de Firewall e Antivírus de licença paga. Segundo MARTINS (2012, p.18):

> Este ambiente é um verdadeiro chamariz para um atacante ou intruso. Inúmeros são os tipos de ataques aos quais estas redes são submetidas diariamente e um ataque bem-sucedido pode ser bastante prejudicial para uma organização. Em geral, um atacante pode simplesmente testar os seus conhecimentos, pode coletar informações, pode causar danos financeiros à empresa, pode destruir os dados da organização, pode publicar informações sensíveis da empresa, pode utilizar a estrutura da empresa para invadir outra, entre outras possibilidades.

Baseado na Cartilha de segurança para internet, Cert.br. , acesso em 2019.

1) Firewall

O Firewall já vem incluso na maioria dos sistemas operacionais com intuito de negar acesso a usuários não permitidos em seus respectivos ficheiros, examinando cada pacote e entregando a sua origem. Se o pacote estiver catalogado, é permitido o acesso, caso contrário, o acesso é negado.

O Firewall tem por missão proteger internamente o sistema de ataques externos, entretanto, não protege de ataques internos. Com a possibilidade de o invasor conseguir quebrar o código de segurança ou em caso de desconfiguração do firewall, o invasor conseguirá o acesso ao sistema.

2) Antivírus

Ferramenta de suma importância e muito utilizada por todas as Organizações Militares. O Antivírus verifica o sistema operacional da máquina avaliando a presença de vírus e, caso encontre, fica incumbido de efetuar a eliminação dos mesmos. Há diversas formas de adquirir vírus, principalmente por sites de conteúdo erótico, download de arquivos, utilização de mídias ou programas infectados. Portanto, o antivírus tem o papel fundamental de bloquear a entrada e expansão do código malicioso, emitindo um alerta ao usuário sobre a existência de uma ameaça.

3) Backup e Restore

Software de grande importância para as unidades militares, possui a função de gerar cópias de segurança das informações e sistemas anteriormente gravados e recupera-los, caso necessário. A cópia pode ser guardada em CD-R, pendrive ou até mesmo, em uma forma mais segura, na nuvem, permitindo que as informações não sejam roubadas por hackers. Essa ferramenta oferece a possibilidade de restaurar todas as informações que foram transferidas para o dispositivo através do backup. Segundo Kevin Mitnick (2003, p.181):

> As informações valiosas devem estar protegidas independente da forma assumida ou do local onde estão armazenadas. A lista de clientes de uma organização tem o mesmo valor seja na forma impressa seja em um arquivo eletrônico no seu escritório ou em um cofre.05 engenheiros sociais sempre preferem o ponto de ataque mais fácil e menos defendido. As instalações de armazenamento de backup externas a uma empresa são vistas como menos arriscadas. Cada organização que armazena dados valiosos, confidenciais ou críticos com terceiros deve criptografar seus dados para proteger a sua confidencialidade.

Hoje em dia, há diversas ferramentas de proteção contra agentes maliciosos que podem ajudar na segurança das informações, fundamentais às unidades de infantaria para melhor proteção de conteúdos sigilosos. As máquinas encontram-se em contínuo processo de atualização, com a criação constante de novas alternativas de detecção de invasão e proteção. Não obstante, novas metodologias de invasão e softwares maliciosos também são desenvolvidos periodicamente. Não há sistema totalmente seguro, os invasores costumam utilizar-se de falhas humanas para invasão de sistemas e aquisição de informações valiosas e estratégicas.

2.4.1 LOGOFF

A World Wide Web (WWW) é constituída por uma grande rede de computadores interconectados, na qual empresas, governos, grupos e pessoas em todo o mundo mantêm arquivos de computador interligados conhecidos como páginas da web. As pessoas navegam nestas páginas por meio de programas de software de computador trivialmente conhecidos como navegadores da Internet. Devido à grande quantidade de sites da WWW, muitas páginas da web têm uma exorbitância de informações. A vastidão da WWW não estruturada faz com que os usuários dependam principalmente dos mecanismos de busca da Internet para recuperar informações. Esses

mecanismos de pesquisa usam vários meios para determinar a relevância de uma pesquisa definida pelo usuário para obtenção de informações.

Disponíveis para todos os usuários, as informações são públicas. Outras informações são de cunho privado e o acesso deve ser limitado. Contudo, a mesma interconectividade que torna a informação tão imediatamente disponível coloca um encargo especial sobre os sistemas envolvidos na mudança ou armazenamento de informações privadas. Essa questão de segurança é importantíssima em ralação às invasões generalizadas, ou seja, o uso de computadores para adquirir acesso não autorizado a outros sistemas de computador e para roubar, destruir ou corromper ativamente informações. (GAL ASHOUR, 2006, tradução nossa)

As unidades militares que operam com internet ou intranet devem confiar nas mudanças cliente servidor pela internet, em oposição às interações face a face que, na atualidade, são menos utilizadas devido ao avanço da tecnologia. Atualmente, o logon e o logoff do cliente servidor, referentes ao nosso sistema, redes ou computadores e término da sessão iniciada, respectivamente, são considerados transação comercial com vantagens e desvantagens para o usuário que está utilizando o servidor. Não obstante, para que os dados permaneçam seguros, deve-se utilizar o método de logon e logoff para a troca de informações não públicas e de caráter privado ao ambiente militar.

Os militares que buscam acessar informações privadas em suas devidas seções, habitualmente, iniciam seu expediente realizando primeiro o login em um recurso de login padrão. Nesta questão, eles podem acessar as informações seguras fornecendo uma senha ou outras informações ao servidor de sua respectiva seção que os identifica como tendo acesso legítimo a determinadas informações. Idealmente, o militar trocaria informações com o servidor e, em seguida, efetuaria logoff expressamente, terminando a conexão segura. Na verdade, podem ocorrer períodos em que o dono daquela conta está completamente inativo, entretanto, permanece conectado, talvez enquanto distraído. Pode haver outras situações em que o militar opte por acessar outro site que não seja seguro.

No caso de uma operação multiusuário, com outro militar utilizando o mesmo computador, o mesmo pode inadvertidamente sair sem terminar sua sessão fazendo logoff. Em cada um desses casos, os resultados são os mesmos: (GAL ASHOUR, 2006)

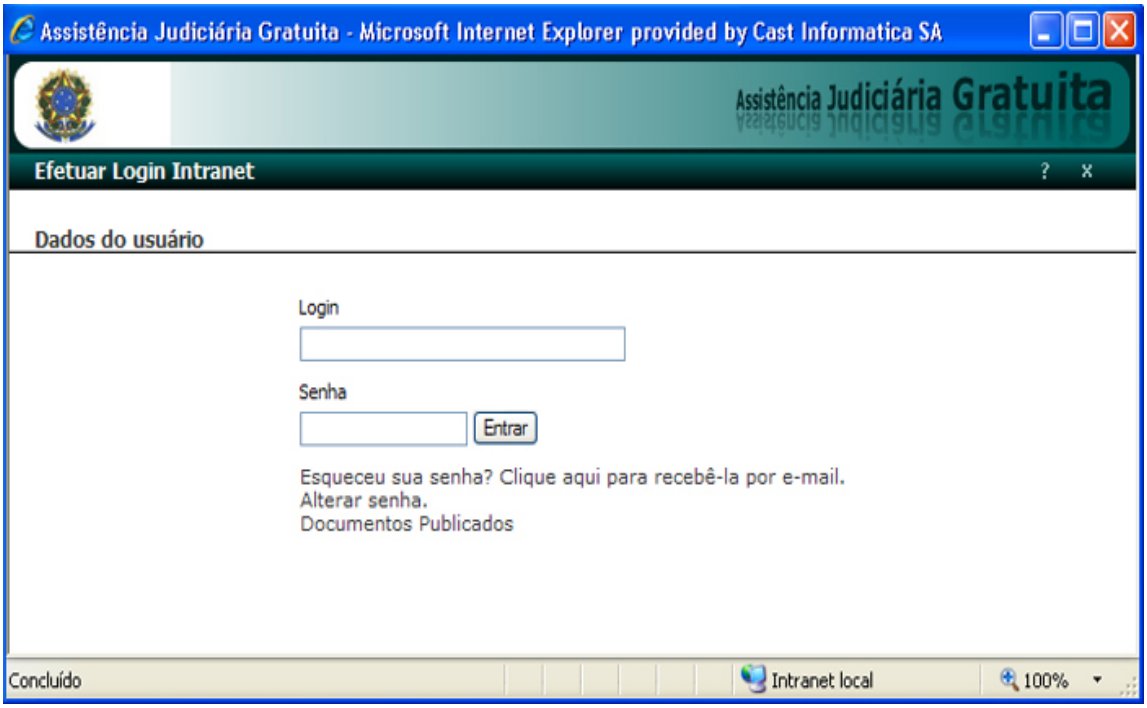
> 1.The client remains connected to the site even if not actively using it.
>
> 2.The client becomes prone to the theft or corruption of electronic information.

> 3.The ebusiness expends valuable resources maintaining a secure connection that is either under-utilized or un-utilized.
> 4.If the user goes to another site and then shortly thereafter returns back to the secure site, the user might not be able to reconnect before the previous session has expired or timed out.

Períodos de inatividade são inevitáveis, no entanto representam uma ameaça real à segurança da transação. A dificuldade em resolver o problema reside em determinar como e quando uma sessão segura não uniforme e amplamente imprevisível deve ser encerrada. (GAL ASHOUR, 2006, tradução nossa).

É evidente que os problemas explicitados ocorrem em praticamente todas as OM militares espalhadas pelo Brasil. O fluxo de militares que acessam a internet ou até mesmo a intranet do batalhão aumenta a susceptibilidade de ataques dirigidos ao sistema e suas informações. Imprescindível que os militares possuam conhecimento sobre a segurança da informação e que avaliem efetivamente se houve o logoff de suas contas, para preservação dedados pessoais e dados exclusivamente relacionados a atividades do batalhão que não devem ser expostos a terceiros que trabalham na unidade e não estão inseridos no efetivo profissional do batalhão. Observe a figura 03:

Figura 3- Efetuar Login Intranet.



Fonte: www.cjf.jus.br. Acesso em abril, 2019.

2.4.2 Redes Sociais

As modificações no relacionamento entre pessoas e, de forma conseguinte, entre públicos e instituições foram alteradas pela internet. Vive-se conectado em rede e nesta cena, se articula a comunicação humana. Os vigentes modelos de interatividade, participação e sociabilidade conquistaram espaço na sociedade com o surgimento dos novos instrumentos tecnológicos. Aumentou-se a aptidão do cidadão de manifestar seus pensamentos e de propaga-las diante de uma coletividade.

Atualmente, as redes sociais são bem vindas no Exército Brasileiro, porém devem ser utilizadas da forma correta, pois o mal uso pode fornecer informações importantes sobre o perfil do usuário, criar, gerenciar e compartilhar um tipo de diário com informações do tipo - quem você é? Onde você está? Quem você conhece? Onde você tem estado?. Com a rápida velocidade de propagação de informações, esses dados podem ser disseminados em questão de minutos por toda a sociedade e isso é um problema paras operações que são feitas na rotina de um batalhão de infantaria, pois uma mensagem em uma rede social revelando o dia da operação, por exemplo, poderia condicionar a operação a um possível fracasso caso a informação chegue ao conhecimento

de inimigos que logo se prepararíam para o recebimento da tropa. As informações sigilosas ou não que circulam dentro da OM (Organização Militar) não devem ser compartilhadas com os indivíduos que não fazem parte da rotina, pois a emissão de opiniões destes podem comprometer a imagem do Exército. Os riscos que as redes sociais podem trazer para uma Organização Militar são diversas sendo elas:

a) Invasão de privacidade
b) Furto de identidade
c) Invasão de perfil
d) Instalação de programas maliciosos
e) Disponibilização de informações para criminosos
f) Uso indevido de informações
g) Danos a imagem e à reputação
h) Vazamento de informações
i) Recebimento de mensagens contendo códigos maliciosos e phishing

Há um termo conhecido como engenharia social, um dos artifícios utilizados para buscar informações elementares sobre um indivíduo, produto ou organização como uma elaboração de um ataque. Pode ser classificado como espionagem. Essas informações são oriundas de pessoas próximas de compartilham da mesma familiaridade.

As redes sociais colaboraram com o trabalho dos engenheiros sociais, visto que aglutinam inúmeras quantidade de informações particulares dos indivíduos ou das organizações, já relacionados, no ambiente ao qual foi exposto aquelas informações como, por exemplo, publicações, fotografias, videoclipes e planilhas. As redes de navegação são encarregadas por mais da metade do tráfego da Rede Mundial.

Deve-se tomar cuidado que, mesmo em ambiente privado, as redes socias não oferecem cem porcento de segurança, mesmo os militares sendo treinados a apagar as informações sigilosas ou não, alguns criminosos estão atentos a aqueles recursos. De acordo com Kevin Mitnick (2003, p.3)

> Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.

2.5 Requisitos mínimos de segurança da informação

É de concordância que as OM, Batalhões e outras organizações não militares devem possuir requisitos mínimos de segurança para garantir a segurança de suas informações para as mesmas não caírem nas mãos indesejadas como de hackers.

2.5.1 Determinações fundamentais de segurança para os sistemas computacionais do comandante da OM

Segundo a Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações as básicas de segurança computacional aos comandantes de OM são:

> 1) Cada OM deverá organizar, publicando em Boletim Interno, um Comitê permanente de auditoria interna das medidas de segurança preconizadas na regulamentação vigente, constantes ao final desta Cartilha e parcialmente abordadas no texto, cabendo ao DCT a realização de verificações externas de caráter programado ou inopinado, como autoridade validadora dos níveis de segurança dos sistemas sustentados pela TI do Exército Brasileiro
>
> 2) Controlar o acesso à Internet na OM, restringindo-o, apenas, às estações de trabalho que efetivamente necessitarem de tal acesso. Ainda assim, devem ser bloqueados os sítios que reduzam a produtividade, ou que sejam incompatíveis com a seriedade e a responsabilidade esperada no ambiente de trabalho.
>
> 3) Estabelecer uma rotina de permanente conscientização dos integrantes da organização quanto ao emprego adequado dos recursos de Tecnologia da Informação e Comunicações (TIC) à disposição da OM.
>
> 4) Solicitar o apoio técnico à OM de Telemática do Exército (CTA ou CT) que atende à OM considerada, sempre que houver dúvidas.
>
> 5) Proibir a utilização de dispositivos móveis de armazenamento (pendrives, HD externos ou cartões de memória), particularmente em ambientes onde operam máquinas com dados sensíveis. Quando absolutamente necessário, liberar o acesso de tais dispositivos, sob supervisão, somente nas máquinas com antivírus configurado para verificar, automaticamente, qualquer dispositivo removível conectado ao computador
>
> 6) Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. Os cadastros de usuários que acessam os sistemas devem ser mantidos atualizados e supervisionados pela contra inteligência da OM.
>
> 7) Estabelecer uma política clara e supervisionada relativa ao descredenciamento de usuários que tenham sido transferidos de OM ou de função.

> 8) Divulgar com regularidade o cumprimento das diretrizes, manuais, instruções e normas em vigor no âmbito do Exército que tratam da Segurança da Informação e Comunicações (SIC).

2.5.2 Segurança dos computadores da OM

Vale ressaltar que os militares ou funcionários terceirizados que trabalham na OM que fazem proveito da rede da OM são encarregados da proteção, cuidado e a boa utilização das informações às quais tem alcance. Logo, todas as acomodações e máquinas necessitam de proteção, em oposição a pessoas não credenciadas. É de grande valia, portanto, que o Batalhão de Infantaria Leve também possua mecanismos de proteção em suas instalações. O intuito é impossibilitar o acesso impróprio aos ativos de informação em seus respectivos recintos, como por exemplo, locais onde só é permitida a entrada com sua identificação de usuário, senha e leitura biométrica, que são informações intrasferíveis que cabe a cada um manter-se consigo. Segundo Kevin Mitnick (2003, p.3)

> Como diz o ditado; até mesmo os verdadeiros paranóicos provavelmente têm inimigos. Devemos assumir que cada empresa também tem os seus — os atacantes que visam a infra-estrutura da rede para comprometer os segredos da empresa. Não acabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenar as defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados.

Os militares ou funcionários que utilizam os computadores da OM devem contemplar senhas para que só os mesmos possam ter acesso em suas respectivas máquinas, ou seja, elas devem ser mantidas em sigilo. Cabe, inclusive, à Organização Militar aconselhar os seus subordinados quanto à confecção de suas senhas para que possuam um grande grau de segurança, podendo entrecruzar letras maiúsculas, minúsculas com números e caracteres especiais.

Ainda no que tange à segurança das máquinas da OM, do mesmo modo, deve-se estipular artifícios de limites de tentativas frustradas que levem de imediato ao bloqueio do computador que está operado pela pessoa não autorizada. O batalhão deve orientar o seu efetivo a nunca guardar login, senha e chaves criptografadas de sua aplicação no código primário e sim, buscar empregar serviços de autenticação ou criptografar essas informações para manter o sigilo de seus dados e da organização. De acordo com Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações há outras maneiras de cuidar dos computadores da OM:

1) Utilizar somente software original e licenciado e os constantes no Anexo E ao Plano de Padronização do Ambiente e Migração para Software Livre no Exército Brasileiro publicado na separata ao BE Nr 17 de 30ABR10.

2) Adotar os seguintes tipos de programas de segurança em todos os computadores da OM, utilizando software adquirido ou padronizado pelo Exército:

2.1 Antivírus: para evitar a propagação de vírus de computador;

2.2 Antispyware: para manter a máquina protegida de programas espiões;

2.3 Antispam: para evitar o tráfego de mensagens de correio eletrônico indesejadas; e

2.4 Firewall pessoal: para proteger a máquina de acessos remotos ao seu equipamento e furto de dados.

2.5 Manter permanentemente atualizados e com as mais recentes correções de segurança, todos os programas instalados. Os atos hostis exploram as vulnerabilidades conhecidas que, normalmente, são corrigidas nas versões mais recentes.

3 REFERENCIAL METODOLÓGICO

3.1 TIPO DE PESQUISA

O presente trabalho foi elaborado através de levantamento bibliográfico.

3.2 PROCEDIMENTOS DE PESQUISA

3.3.1 Características de um Batalhão de Infantaria Leve

Pesquisa realizada na instrução IP 7-35, por meio deste foram levantadas as características, possibilidades, limitações e missões em que são empregados o Batalhão de Infantaria Leve.

3.2.2 Segurança da informação aos órgãos da administração pública federal

Os sistemas de segurança da informação nos estabelecimentos foram estudados por meio de publicações encontradas no espaço virtual e pesquisa dos sistemas de outros países.

3.2.3 A gestão da segurança dessas informações por meios defensivos cibernéticos

Essas informações foram abstraídas de manuais do Exército e de outras bibliografias armazenadas em meios eletrônicos e publicações referentes ao tema.

4 CONCLUSÃO

Demonstradas as diversas maneiras sobre a facilidade da perda de informações, o intuito deste trabalho foi expor a necessidade de proteção das informações operacionais e a limitação de acesso a pessoas credenciadas.

É axiomático, portanto, como evidenciado no trabalho, que para obter sucesso na realização das missões, o Batalhão de Infantaria Leve, encarregado de diversas missões em todo território nacional, deve manter o sigilo das informações. Portanto, é de grande valia o estudo de como deve ser tratado o tema e sua inserção na rotina do efetivo do batalhão.

De acordo com o que foi tratado, em relação ao tema softwares maliciosos, temos como o principal vilão o vírus que cresceu conforme a tecnologia avançou. Diante disso, toda máquina que está ligada à WWW está suscetível a esses softwares, tanto os computadores pessoais do efetivo que trabalha na OM quanto as máquinas que acabam sendo infectadas pelos próprios indivíduos, quando por desconhecimento, carregam pendrives infectados ao seu estabelecimento de trabalho. Mediante a isso, foi apresentado o antivírus como um meio de prevenção e destruição dos mesmos.

As redes sociais, meio atualmente indispensável para as comunicações, trouxeram benefícios, como a possibilidade de contato instantâneo mesmo em grandes distâncias. Não obstante, o uso indevido propaga notícias rápidas para a sociedade, superando, inclusive, os sistemas televisivos. As redes sociais devem ser utilizadas de forma correta ou até mesmo proibidas, caso necessário, no ambiente de trabalho, para não comprometer a segurança de informações sobre o que acontece naquele estabelecimento ou dados sigilosos a respeito de operações futuras e que não devem ser retransmitidas para a sociedade e forças adversas.

Indubitável, portanto, que é de grande valia que sejam elaboradas medidas, como cartilhas, pelos batalhões, visando aumentar a segurança da informação que circula dentro de suas unidades, com intuito de ensinar ao indivíduo, de baixa patente até ao nível mais alto hierárquico, os procedimentos que devem ser tomados no que diz respeito à segurança da informação que se inicia, desde a criação de senhas fortes que dificultam ao acesso de pessoas não autorizadas e utilização de dispositivos de armazenamentos móveis que são disponibilizados pela própria seção para evitar a contaminação dos computadores do ambiente de trabalho.

REFERÊNCIAS

ABNT NBR ISO/IEC 17799. **Tecnologia da Informação – Técnicas de Segurança Código de prática para a gestão de segurança da informação.** Rio de Janeiro, 2005

About The Open Web Application Security Project. Disponível em:<https://www.owasp.org/index.php/Top_10_2010-Main>>. Acesso em: 9 abr. 2019.

ASHOUR et al. **System and method for protecting user logoff from web business transactions.** Disponível em: <https://patents.google.com/patent/US7024394B1/en>. Acesso em 20 abr. 2019.

AZEVEDO, Hugo Alves de. **Segurança em Rede.** 2007. 11 f. Monografia (Especialização) - Curso de Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2007.

BRASIL. Exército. Estado-Maior. **IP 7-35**: O Batalhão de Infantaria Leve, 1. ed, 1996

Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/>. Acesso em: 20 abr. 2019.

Cartilha Emergencial de Segurança, Tecnologia da Informação e Comunicações. Disponível em: <http://www.2icfex.eb.mil.br/images/conteudo/area_das_secoes/01_satt/01_secao_informatica/cartilha_seguranca.pdf> Acesso em: 28 ago. 2018

Conselho da Justiça Federal. Disponível em:<https://www.cjf.jus.br/aj/help/Efetuar_Login.htm>. Acesso em: 10 abr. 2019.

COSTAS, M.et al. **A política de segurança da informação:Uma analise da rca 025/2009 S icoob Credip** Disponível em: <http://www.infobrasil.inf.br/userfiles/28-05-S2-2-68453 A%20Politica%20de%20Seguranca.pdf >. Acesso em: 11 abr.2019.

DE OLIVEIRA, Lucas Vinícius ; DE BEM, Ricardo Orige. **Proteção na rede: Uma análise informativa do atual cenário da segurança da informação**, Araranguá, 2015.

Departamento de **Segurança da Informação e Comunicações**, Gabinete de Segurança Institucional da Presidência da República. Disponível em: <http://dsic.planalto.gov.br/assuntos/publicacoes> Acesso em: 28 ago. 2018

Fake News que geraram guerras e conflitos ao redor do mundo. Disponível em: <https://www.bbc.com/portuguese/geral-43895609> Acesso em: 28 ago. 2018

MARCIANO, João Luiz Pereira Marciano. **Segurança da Informação**: uma abordagem social. Brasília, 2016. Trabalho de Conclusão de Curso () - UNIVERSIDADE DE BRASÍLIA.

MARTINS, Daniel Mourão. **Uma estratégia para sistemas de detecção e prevenção de intrusão baseada em software livre.** 2012. 100 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Departamento de Computação, Universidade Federal do Ceará, Fortaleza, 2012. Disponível em: <http://mdcc.ufc.br/teses/doc_download/197->. Acesso em: 9 abr. 2019.

MEDEIROS, Carlos Diego Russo. **Segurança da Informação: Implantação de Medidas e ferramentas de Segurança da Informação**. Monografia (Bacharelado em informática) – Universidade da Região de Joinville "Univille Departamento de Informática", Joinville, 2001.

MITNICK, Kevin ; SIMON, William. **A arte de enganar**. São Paulo: Gisélia Costa, 2003.

Requisitos Mínimos de Segurança da Informação aos Órgãos da Administração Pública Federal. Brasília, DF, 2017.

Segurança nas redes sociais. Disponível em:<http://www.11rm.eb.mil.br/publicar/SEGURANCA_NAS_REDES_SOCIAIS.pdf>. Acesso em: 10 abr. 2019.

SÊMOLA, Marcos. **Gestão da Segurança da Informação - Uma Visão Executiva**. Rio de Janeiro: Elsevier, 2014.

SÊMOLA, M. **Gestão da Segurança da Informação Uma Visão Executiva**. 7. ed. [S.l.]:Elsevier, 2003.