ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INF JOSÉ CLÁUDIO DE ARAÚJO SOUSA

PROCEDIMENTO OPERACIONAL PADRÃO PARA PREVENÇÃO QUANTO AO USO DE MÍDIAS REMOVÍVEIS NAS SEÇÕES DAS ORGANIZAÇÕES MILITARES

Rio de Janeiro
2018

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INF JOSÉ CLÁUDIO DE ARAÚJO SOUSA

PROCEDIMENTO OPERACIONAL PADRÃO PARA PREVENÇÃO QUANTO AO USO DE MÍDIAS REMOVÍVEIS NAS SEÇÕES DAS ORGANIZAÇÕES MILITARES

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Operacional.

Rio de Janeiro
2018

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap Inf JOSÉ CLÁUDIO DE ARAÚJO SOUSA**

Título: **PROCEDIMENTO OPERACIONAL PADRÃO PARA PREVENÇÃO QUANTO AO USO DE MÍDIAS REMOVÍVEIS NAS SEÇÕES DAS ORGANIZAÇÕES MILITARES**

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Gestão Operacional, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____ *CONCEITO:* _____

BANCA EXAMINADORA

Membro	Menção Atribuída
_____ **Alexander Ferreira da Silva- Ten Cel** Cmt Curso e Presidente da Comissão	
_____ **Lendro Tavares Luiz- Cap** 1º Membro e Orientador	
_____ **Ubirajá Severiano de Oliveira Filho - Cap** 2º Membro	

_____
JOSÉ CLÁUDIO DE ARAÚJO SOUSA – Cap
Aluno

PROCEDIMENTO OPERACIONAL PADRÃO PARA PREVENÇÃO QUANTO AO USO DE MÍDIAS REMOVÍVEIS NAS SEÇÕES DAS ORGANIZAÇÕES MILITARES

JOSÉ CLÁUDIO DE ARAÚJO SOUSA*
TAVARES**

RESUMO

A Informação nos dias atuais recebe cada vez mais uma importância crescente em todos os setores de uma Organização, quer seja ela pública ou privada. A sua perda ou utilização ilícita pode causar danos irreversíveis a imagem da Instituição. Devido a essa importância, faz-se necessário uma preocupação constante por parte de todos os envolvidos com a proteção das mesmas. O objetivo deste trabalho é demonstrar a relevância do emprego de um procedimento operacional padrão quanto ao uso de mídias removíveis (pen drives, tablets, HD, cartões de memória e celulares) nas seções das Organizações Militares do Exército Brasileiro. Foi realizada revisão da literatura disponível em manuais do Exército Brasileiro, cartilhas e livros de outras Instituições que abordam a temática com o foco voltado para a Proteção da Informação, visando um estudo doutrinário e histórico do assunto. Foram realizadas questionários com a finalidade de se verificar a relevância e o grau de importância que o assunto em voga gera nas diversas Organizações Militares do Exército Brasileiro com a finalidade de mensurar e propor medidas e ações para que seja aprimorada a segurança da Informação no Exército Brasileiro. Ao fim da pesquisa, chegou-se à conclusão de que os Procedimentos Operacionais Padrão ora propostos são efetivos e possuem um custo baixo para implantação, tornando-se assim, viável para sua execução e imediato emprego nas Organizações Militares do Exército Brasileiro.

Palavras-chave: Informação. Procedimento Operacional Padrão. Proteção da Informação. Baixo Custo de Implantação.

ABSTRACT

La información en los días actuales recibe cada vez más una importancia creciente en todos los sectores de una Organización, ya sea pública o privada. Su pérdida o uso ilícito puede causar daños irreversibles a la imagen de la Institución. Debido a esa importancia, se hace necesaria una preocupación constante por parte de todos los involucrados con la protección de las mismas. El objetivo de este trabajo es demostrar la relevancia del empleo de un procedimiento operacional estándar en

cuanto al uso de medios removibles (pen drives, tablets, HD, tarjetas de memoria y celulares) en las secciones de las Organizaciones Militares del Ejército Brasileño. Se realizó una revisión de la literatura disponible en manuales del Ejército Brasileño, cartillas y libros de otras Instituciones que abordan la temática con el foco orientado a la Protección de la Información, visando un estudio doctrinario e histórico del asunto. Se realizaron cuestionarios con la finalidad de verificar la relevancia y el grado de importancia que el tema en boga genera en las diversas Organizaciones Militares del Ejército Brasileño con la finalidad de medir y proponer medidas y acciones para que se mejore la seguridad de la Información en el Ejército Brasileño . Al final de la investigación, se llegó a la conclusión de que los Procedimientos Operacionales Estándar ya propuestos son efectivos y tienen un costo bajo para implantación, haciéndose así, viable para su ejecución e inmediato empleo en las Organizaciones Militares del Ejército Brasileño.

Palabras Clave: Información, Procedimento Operacional Padrón, Protección de La Información, Implantación de Costo Más Bajo.

* Capitão da Arma de Infantaria. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2007.

** Capitão da Arma de Infantaria. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2006. Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2015.

1 INTRODUÇÃO

A informação em sua visão etimológica tem origem do latim *informare* (dar forma) e pode ser conceituada como um conjunto organizado de dados, cujo sua posse, permite ao detentor resolver problemas e tomar decisões, levando em conta que o seu uso é a base do conhecimento (GRAMÁTICA,2016).

Com a constante evolução tecnológica, os documentos passaram a ser elaborados e armazenados em computadores. Atualmente, milhões de pessoas usam computadores, elaboram e compartilham documentos contendo informações importantes, através do uso da internet, usam serviços de ensino e pesquisa, acessam redes sociais, dentre outras coisas, abrindo assim uma janela, onde criminosos conhecidos como hackers podem se utilizar dessas para terem acesso as estas informações.

O presente capítulo tem por finalidade realizar a introdução ao tema da pesquisa, apresentando o problema, os objetivos (Geral e Específicos), e as justificativas que tornam o presente tema relevante para a Escola de Aperfeiçoamento de Oficiais e para o Exército Brasileiro contribuindo com medidas que podem se adotadas tendo por finalidade um aumento da segurança da informação nas Organizações Militares.

1.1 PROBLEMA

Vivemos em um mundo globalizado. Tudo o que a sociedade requer e necessita é criado, inventado, produzido, desenvolvido e comercializado com uma velocidade espantosa.

Chegamos ao ponto de nos conectarmos com pessoas de todas as partes do mundo, simultaneamente, através de redes sociais, telefones fixos ou móveis, além de acessar a internet por intermédio de celulares e televisores, ou computadores cada dia menores e mais velozes e com métodos de armazenamento de informações incríveis, como cartões de memória e *pen drives,* ou com conceitos ainda mais arrojados como o de armazenamento na “NUVEM” ou servidores remotos.(EDNO,2016).

As inovações tecnológicas, principalmente nas telecomunicações e na informática, promoveram o processo de globalização. A partir da rede de telecomunicação foi possível a difusão de informações entre as empresas e instituições financeiras, ligando os mercados do mundo.

No início, a computação era um mecanismo que tornava possível automatizar determinadas tarefas em empresas multinacionais e nos meios governamentais. Com o avanço tecnológico, as grandes máquinas começaram a perder espaço para equipamentos cada vez menores e mais poderosos. A evolução das telecomunicações permitiu que, aos poucos, os computadores passassem a se comunicar, mesmo estando em lugares muito distantes geograficamente. Como consequência, tais máquinas deixaram de simplesmente automatizar tarefas e passaram a lidar com a Informação.

A informação deve ser vista como um patrimônio, ela agrega valor à Organização. Não se trata de um monte de *bytes* aglomerados, mas sim de um conjunto de dados classificados e organizados de forma que uma pessoa ou uma empresa possa tirar proveito. A informação é inclusive um fator que pode determinar a sobrevivência ou a descontinuidade das atividades de um negócio. E isso não é difícil de ser entendido. Basta imaginar o que aconteceria se uma instituição financeira perdesse todas as informações de seus clientes (ASSUNÇÃO, 2010).

Em geral, uma combinação entre a ameaça e a vulnerabilidade dos dados é a janela de segurança mais visada. Computadores, *pen drives*, celulares e *tablets* mal configurados e sem as atualizações dos sistemas operacionais contribuem para possíveis falhas de segurança. A ausência de políticas de segurança nas Instituições públicas e privadas e de capacitação para seus funcionários também se somam aos motivos que podem levar a uma segurança frágil de dados.

Esta compilação de fatores é propícia para o surgimento de um **Ataque Cibernético**[1], que pode ser conceituado como um ataque iniciado a partir de um computador contra outro computador ou rede de computadores, através do uso de Ferramentas de Ataque, que tem como objetivo comprometer a integridade, confidencialidade ou disponibilidade do alvo e as informações nele armazenadas (BRASIL, 2017).

O Brasil, quinto país do mundo em extensão territorial e em número de habitantes, contando com a metade dos usuários de Internet da América do Sul, é

[1]**Ataque cibernético:** Ataques cibernéticos são tentativas propositais de alterar, corromper ou destruir sistemas e redes de computadores ou então as informações e programas que eles armazenam ou transmitem. — Conselho Nacional de Pesquisas dos EUA. Fonte: https://wol.jw.org/pt/wol/d/r5/lp-t/102012171#h=6 Acesso em: 05 nov. 2017.

um ator relevante nas discussões da temática cibernética, tanto em nível acadêmico quanto nas relações internacionais, bem como no estabelecimento de políticas e estratégias adequadas à segurança e à defesa nessa nova dimensão.

Em agosto de 2010, embasado na Estratégia Nacional de Defesa, o Brasil definiu que o Exército brasileiro ficaria responsável pelo setor cibernético. O objetivo dessa importante estratégia é reduzir as vulnerabilidades dos sistemas relacionados à defesa nacional contra-ataques cibernéticos. Em 2017, por exemplo, o governo brasileiro, por intermédio do Ministério da Defesa, criou o **Comando de Defesa Cibernética**[2], tendo esse vetor como importante vertente de pesquisa para as Forças Armadas e para o Brasil.

A eficiência da segurança da Informação requer um amplo leque de medidas nos aspectos doutrinários de preparo e emprego da força, a serem tomadas nos diversos escalões de comando, contextualizadas com o tipo de operação que os elementos estiverem sendo empregados (BRASIL, 2011).

Neste contexto, suscita-se a análise das capacidades de ação preventiva contra Ferramentas de Ataque Cibernético nas Seções das Organizações Militares que possuam informações sensíveis, cujo vazamento seria de prejuízos materiais e morais incalculáveis, trazendo como cerne do presente Artigo o seguinte questionamento: Quais medidas podem ser implementadas para aumentar a proteção das Informações digitais?

[2]**Ministério da Defesa cria o Comando de Defesa Cibernética.** Fonte:https://seginfo.com.br/2014/11/10/ministerio-da-defesa-cria-o-comando-de-defesa-cibernetica-2/ Acesso em 05 nov. 2017.

1.2 OBJETIVOS

A seguir, apresento o Objetivo Geral e os Objetivos Específicos deste projeto de pesquisa.

a. OBJETIVO GERAL

Realizar um estudo sobre a possibilidade do estabelecimento de procedimentos de segurança básicos, de baixo custo e de pequena complexidade aos militares que trabalham em seções cujas informações sejam sensíveis, em que a perda ou captura de dados possam acarretar grandes prejuízos a Instituição Exército Brasileiro.

b. OBJETIVOS ESPECÍFICOS

1) Analisar os riscos à imagem da Instituição, caso seja alvo de um Ataque Cibernético,por intermédio do uso das diversas Ferramentas de Ataque;

2) Caracterizar as peculiaridades de possíveis Ferramentas de Ataque que possam ser utilizadas por Forças Adversas, em um Ataque Cibernético a uma Organização Militar;

3) Identificar, de uma maneira resumida, aspectos relevantes em relação às ameaças existentes no espaço cibernético, que possam comprometer a segurança cibernética;

4) Citar exemplos e locais que sofreram Ataque Cibernético através do uso de Ferramentas de Ataque e suas conseqüências;

5) Enumerar as vulnerabilidades referentes a um possível Ataque Cibernético por meio de Ferramentas de Ataque a que está suscetível uma Organização Militar; e

6) Sugerir procedimentos necessários a todos os militares que trabalham em Seção, de maneira que seja dificultada a violação dos sistemas e a obtenção de informações sensíveis por intermédio de ações criminosas.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

A escolha do tema remete a uma preocupação que vem crescendo a cada dia, a segurança das informações e dados de pessoal e material da Força Terrestre, até aqui não tão bem explorada nos manuais doutrinários do Exército Brasileiro; desta forma, visa a incrementar medidas preventivas de baixo custo

orçamentário e de pouca complexidade para adoção das práticas de proteção contra ferramentas de Ataque Cibernético;

A delimitação do tema remete à busca por uma proteção constante de dados sensíveis cujo sua perda ou roubo, possam acarretar grandes prejuízos a Instituição Exército Brasileiro; tal proposta visa a expandir o conhecimento sobre Ataques Cibernéticos através do uso de Ferramentas de Ataque e quais medidas preventivas podem ser utilizadas de maneira que seja dificultada a violação dos sistemas e a obtenção de dados sensíveis com finalidades criminosas;

A relevância do tema embasa-se no conceito de atuação preventiva de todos os militares, independente de posto ou graduação, que trabalhem em seções por onde tramitam informações e dados de pessoal e material, cuja sua perda ou roubo causem impacto imensurável a Força Terrestre;

Os aspectos positivos da proposta são as diversas medidas preventivas que podem ser implementadas de imediato, não sendo necessária para sua execução nenhum planejamento orçamentário de valor elevado, cuja sua elaboração e aprovação possam causar um lapso temporal, criando assim oportunidades para que ocorram Ataques Cibernéticos através do uso de Ferramentas de Ataque; e

As inovações esperadas são as adaptações necessárias em pessoal e material, com a adoção de novos procedimentos que visem aumentar a segurança dos dados sensíveis nas Organizações Militares, atingindo-se dessa forma o produto desejado da presente pesquisa.

2 METODOLOGIA

A presente pesquisa científica classifica-se quanto à forma de abordagem em pesquisa qualitativa e, quanto ao objetivo geral, em pesquisa exploratória.

O espaço considerado para a pesquisa será o trânsito de informações por intermédio de mídias removíveis, nas Seções de Organizações Militares responsáveis por dados sensíveis, como: Seção de Pagamento de Pessoal; Seção de Operações; Seção de Pessoal; Fiscalização Administrativa; Seção Técnica de Ensino.

Como grupo de pesquisa, tem-se os integrantes dessas seções de alguns Batalhões de Infantaria, Colégios Militares, unidades componentes da Força Terrestre.

As principais fontes de pesquisa para o presente trabalho são os manuais doutrinários e documentações atinentes à Guerra Eletrônica, além das fontes fidedignas oferecidas pela rede mundial de computadores.

Os instrumentos selecionados para a pesquisa são o Questionário e a Ficha de Coleta de Dados, que serão confeccionados visando à coleta de informações para uma futura análise qualitativa das mesmas, o que contribuirá para a solução do problema em questão.

A fim de abordar o problema de forma coerente, foi utilizada a pesquisa mista, haja vista que as referências numéricas obtidas por meio dos questionários foram de primordial valor para que se levantasse as reais necessidades de um aperfeiçoamento da segurança quanto a proteção das informações contidas nos computadores das Organizações Militares.

Não obstante, a fim de elucidar o Objetivo Geral do presente estudo, foi necessária uma grande exploração do conteúdo, tendo em vista o pouco conhecimento que se tem do assunto e o fato do mesmo estar em constante mudança, obrigando o presente pesquisador a debruçar-se não só sobre o conceito de Guerra Cibernética, mas também fazer um pararelo com as conseqüências de que um uso mal intencionado dela pode acarretar para as Organizações Militares e sobretudo para a imagem da Instituição Exército Brasileiro. Para tanto, foi essencial a realização dos questionários, de forma a tentar dar um valor objetivo e destacar a importância do tema abordado neste presente Artigo.

2.1 REVISÃO DA LITERATURA

A informação é necessidade vital para qualquer ramo da atividade humana, tornando-se indispensável mesmo que a sua procura não seja buscada de forma ordenada ou sistemática, mas sim resultante apenas de decisões casuísticas e/ou intuitivas.

> O Brasil, quinto país do mundo em extensão territorial e em número de habitantes, contando com a metade dos usuários de Internet da América do Sul, é um ator relevante nas discussões da temática cibernética, tanto em nível acadêmico quanto nas relações internacionais, bem como no estabelecimento de políticas e estratégias adequadas à segurança e à defesa nessa nova dimensão (GUIA DE DEFESA CIBERNÉTICA NA AMÉRICA DO SUL, 2017, p. 17).

A inserção das ferramentas de Tecnologia da Informação nos ambientes de trabalho das Instituições e empresas veio acompanhada de uma exigência altamente prioritária, que já existia sobre outras condições em situações convencionais (CARTILHA EMERGENCIAL DE SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES, 2011, p. 2).

Sobre Guerra Cibernética, destaca-se a seguinte definição:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC (GUERRA CIBERNÉTICA, 2017, p. 2-2).

Sobre Ataque Cibernético, destaca-se a seguinte definição:

> É a atividade que tem o objetivo de interromper, negar o uso, degradar, corromper ou destruir sistemas computacionais ou informações armazenadas em dispositivos e redes computacionais e de comunicações de interesse (GUERRA CIBERNÉTICA, 2017, p. 4-1).

A palavra Hacker possui origem inglesa e indica uma pessoa que possui um bom conhecimento no âmbito da área de informática, sendo capaz de fazer modificações em algum sistema da área. *Hack* em sua etimologia é um verbo que significa cortar alguma coisa de forma irregular ou grosseira. Assim, a partir da década de 50 do século XX, a palavra *hack* começou a ser usada para designar uma alteração inteligente em alguma máquina. Mais tarde, este termo passou a ser usado exclusivamente no âmbito da programação informática.

Muitas vezes, o hacker ao deparar-se com sistemas que dificultem o seu acesso, opta pelo elo mais fraco de toda a corrente de segurança de dados e informações: o Ser Humano. Através do uso da técnica conhecida como Engenharia Social.

Sobre Engenharia Social, destaca-se a seguinte definição:

> Técnica que tem por finalidade fazer com que alguém execute algum software malicioso (malware), como keyloggers ou trojans, que nos forneça as informações que precisamos, ou mesmo através de um fake mail, podemos conseguir dados importantes. Às vezes, apenas uma simples conversa é suficiente para o funcionário lhe dizer o que você precisa saber (ARAÚJO, 2014, p. 35).

Com base nas colocações supracitadas, a Tecnologia da Informação exerce um papel de fundamental importância para Instituições Públicas e Privadas. Consequentemente tem crescido a importância da criação e estabelecimento de medidas que visem à proteção das referidas informações e dados quer sejam de pessoal ou material com relação aos riscos e ameaças que se apresentam nessa área (TRIBUNAL DE CONTAS DA UNIÃO, 2014).

A criação, em 2017, do **Comando de Defesa Cibernética**(ComDCiber), demonstra a preocupação do governo brasileiro, em relação ao assunto. Assim é especificado na publicidade da criação:

> O Diário Oficial publicou a portaria Nº 2.777/MD, de 27 de Outubro de 2014, do Ministério da Defesa, criando assim o Comando de Defesa Cibernética (ComDCiber) Brasileiro, uma iniciativa do governo para reforçar a estratégia de defesa cibernética nacional. Segundo a portaria, o Estado-Maior Conjunto das Forças Armadas (EMCFA) fica responsável por supervisionar a implantação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber), subordinados ao Comando do Exército.O ComDCiber e a ENaDCiber contarão com militares das três Forças Armadas, sendo que caberá ao Exército Brasileiro criar o chamado Núcleo do Comando de Defesa Cibernética (NuComDCiber) e o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), subordinados ao Centro de Defesa Cibernética (CDCiber), que serão os embriões do ComDCiber e do ENaDCiber. (...) Aos recém criados ComDCiber e ENaDCiber caberão organizar e executar os projetos governamentais de defesa cibernética, incluindo as medidas para efetiva implantação de uma defesa cibernética, a implantação de um Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, o apoio à pesquisa e ao desenvolvimento de produtos de defesa cibernética, e a criação de um negócio batizado de "Observatório de Defesa Cibernética".[3]

[3]**Ministério da Defesa cria o Comando de Defesa Cibernética.** Fonte:https://seginfo.com.br/2014/11/10/ministerio-da-defesa-cria-o-comando-de-defesa-cibernetica-2/ Acesso em 05 nov. 2017.

2.2 COLETA DE DADOS

De forma a complementar o conhecimento adquirido através das fontes escritas, foi realizada uma coleta de dados por meio de um questionário.

2.2.1 **Questionários**

A aplicação dos questionários teve por finalidade elucidar a opinião de militares que já atuaram em seções com relação ao uso de mídias removíveis (pen drives, celulares, hd, laptops e tablets) nos computadores que apresentam informações sensíveis das Organizações Militares, tudo isso sob a ótica de dois grupos distintos, quais sejam:

a. Instruendos do Curso de Infantaria e CEAD;

b. Oficiais e Praças das diversas Organizações Militares.

Com as respostas dos mesmos, foi feita a tabulação dos resultados, de forma a cooperar com o intuito da pesquisa, separando os resultados de acordo com os específicos grupos que tiveram contato com os questionários, haja vista que os mesmos incluem grupos que envolvem oficiais subalternos, intermediários e superiores, bem como com experiências profissionais nos diversos Comandos Militares que integram a Força.

3 RESULTADOS E DISCUSSÃO

A Cartilha Emergencial de Segurança da Tecnologia da Informação e Comunicações do Exército Brasileiro afirma sobre a importância de uma proteção constante às informações:

> A inserção das ferramentas de TI nos ambientes de trabalho das Instituições e Empresas veio acompanhada de uma exigência altamente prioritária, que já existia, sob outras condições, em situações convencionais: **A SEGURANÇA DOS SISTEMAS.** (p. 2, Ed 2011)

Desta forma, entendemos que, para uma OM estar com suas informações protegidas, ela deve constantemente seguir procedimentos de segurança básicos, de baixo custo e complexidade, muitos dos quais já previstos e adotados pelas mesmas.

Neste sentido, foi verificado, por intermédio de um questionário a opinião de militares que já atuaram em seções com relação ao uso de mídias removíveis (pen drives, celulares, hd, laptops e tablets) nos computadores que apresentam informações sensíveis das Organizações Militares, conforme gráficos abaixo:

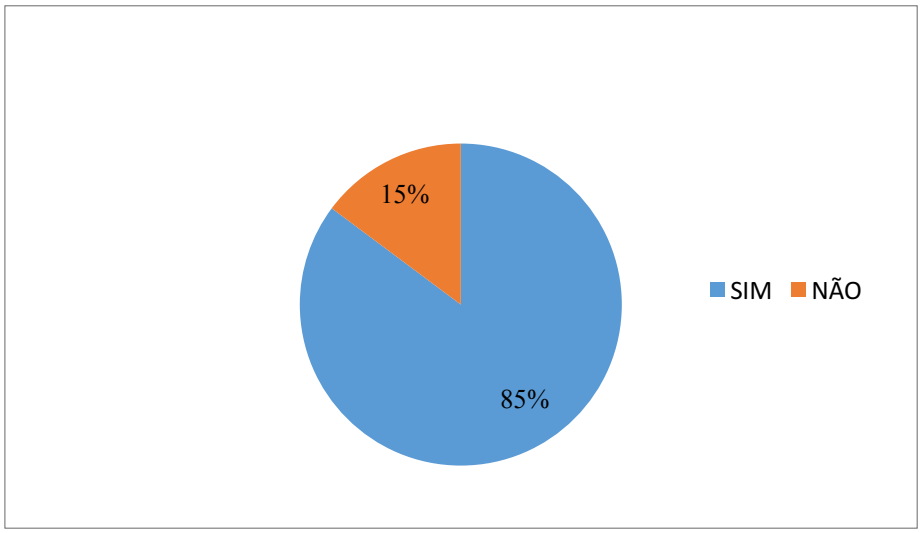

GRÁFICO 1 – Opinião da amostra, em valores percentuais, sobre participação de militares integrantes de Companhias ou de Estado-Maior de Organizações Militares, com o intuito de saber se já foram orientados nas referidas instituições, com instruções referentes à proteção contra crimes cibernéticos.

Fonte: O Autor

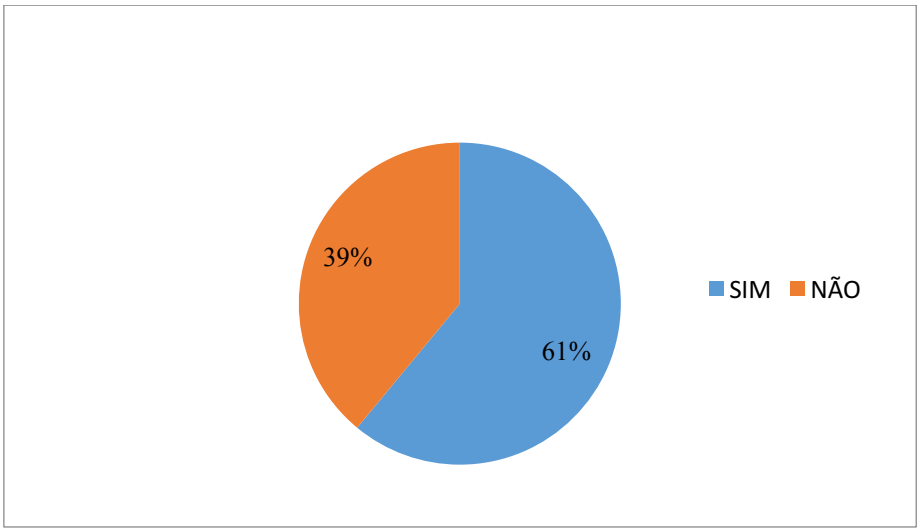

GRÁFICO 2 – Opinião da amostra, em valores percentuais, sobre a conhecimento ou não dos militares,da presença de recomendações nas Organizações Militares como por exemplo avisos proibindo o uso de mídias removíveis particulares nos computadores funcionais da OM.
Fonte: O Autor

Dos dados levantados nos gráficos 1 e 2 principalmente, pode-se concluir que uma considerável parte de militares, em torno de 15%, ainda não possuem uma cultura preventiva em relação a cuidados com a proteção das Informações, sendo que particularmente na análise do gráfico 2 podemos inferir que muitas Organizações Militares não tem dado prioridade ao quesito Segurança da Informação, pois cerca de 39% do público alvo da pesquisa alegou não haver a presença de recomendações como por exemplo a proibição do uso de mídias removíveis particulares nos computadores funcionais de suas referidas Organizações.

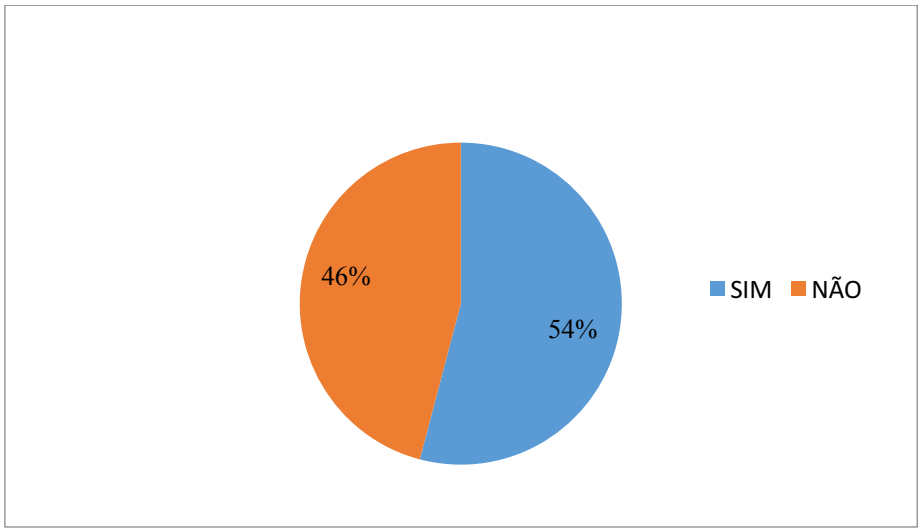

GRÁFICO 3 – Opinião da amostra, em valores percentuais, se havia por parte da 2ª Seção uma fiscalização e orientação com relação à restrição do uso de mídias removíveis particulares no ambiente de trabalho.

Fonte: O Autor

Neste caso, dentre os que apontaram uma resposta negativa, 46% do público alvo alegou não haver uma fiscalização e orientação por parte da 2ª seção das Organizações Militares.

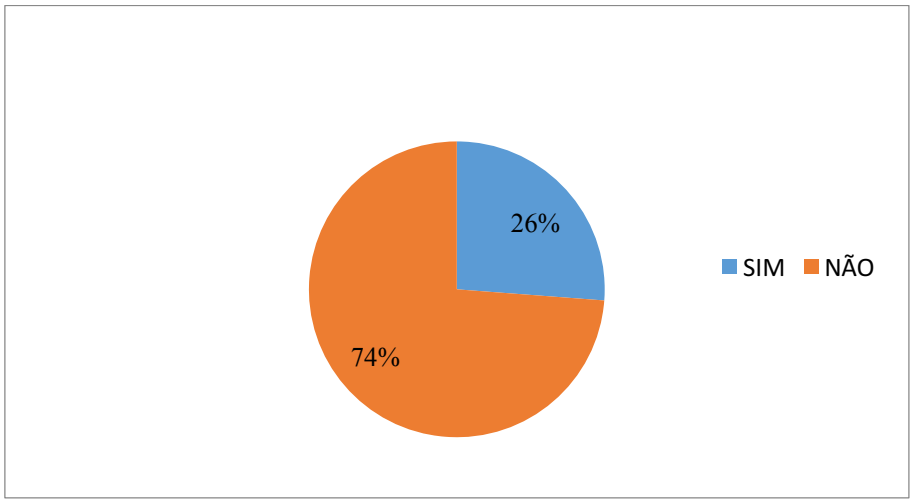

GRÁFICO 4 – Opinião da amostra, em valores percentuais, se os militares que responderam ao questionário teriam conhecimento de que na suas Organizações Militares haveriam disponibilidades por parte da mesmas de dispositivos móveis funcionais (pen drives, hd, laptops)?

Fonte: O Autor

De posse dos índices, é possível deduzir, que ainda há por grande parte das OM um “negligenciamento” no tocante a preocupação de usar dispositivos móveis funcionais nas seções, arquivos e sargenteações das mesmas, levando-nos a conclusão de que é necessário que os militares que estejam em função de Comando, em todos os níveis, devem corrigir o quanto antes a conduta dos demais

militares que trabalham com computadores e não atentam para essa prevenção, prevista na Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações do Exército Brasileiro, que orienta o uso de dispositivos móveis funcionais, de maneira que não sejam manipulados dispositivos particulares, aumentando assim a segurança da Informação preservada no local de destino.

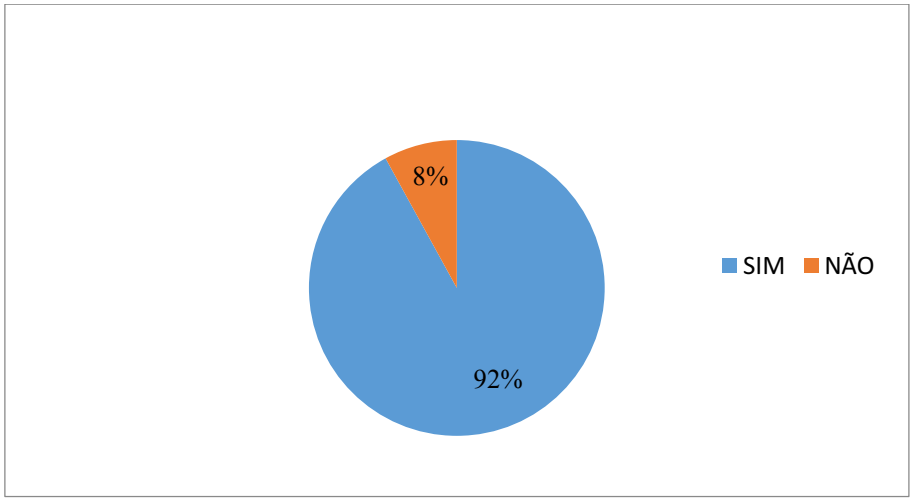

GRÁFICO 5 – Opinião da amostra, em valores percentuais, questionando os militares que responderam ao questionário, se existe Seção de Informática nas Organizações Militares pelos quais os mesmos passaram.
Fonte: O Autor

Neste caso, é possível deduzir que a quase totalidade das Organizações Militares, cerca de 92%, possuem Seções de Informáticas, que tem por finalidade prestarem apoio na área de informática da organização Militar, trazendo consigo também uma janela de vulnerabilidade para possíveis tentativas ilícitas de busca de informações sensíveis nas OM. Cresce de importância a preocupação com a prevenção e segurança das informações presentes nas mídias digitais.

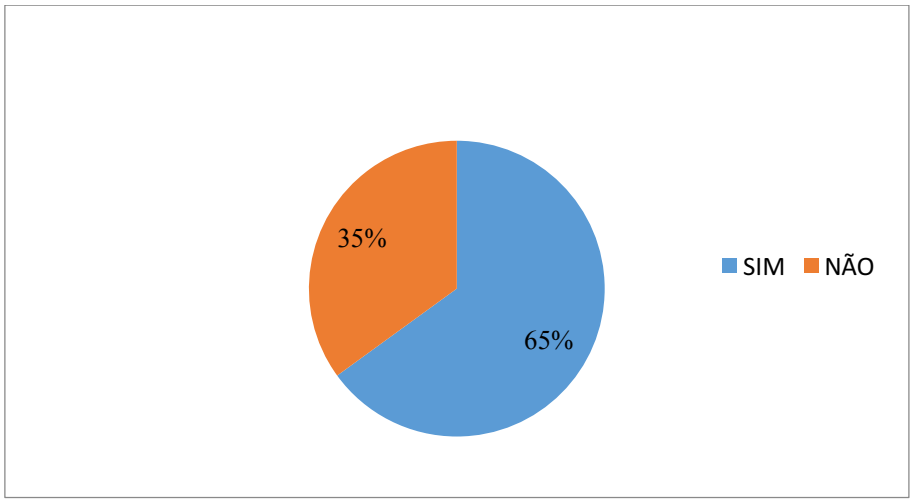

GRÁFICO 6 – Opinião da amostra, em valores percentuais, questionando os militares se haviam nos computadores funcionais das Seções pelas quais passaram, softwares licenciados que proporcionassem uma segurança ao acessar a intranet e/ou internet?
Fonte: O Autor

Após a análise deste gráfico, pode-se perceber que uma parcela considerável das Organizações Militares não possui softwares licenciados. Os prejuízos causados pelo uso de softwares “piratas” vão muito além do que imaginamos. Por exemplo, softwares “piratas” normalmente contêm vírus ou malwares, que são instalados e ocultados nos sistemas. A gama de problemas que essas contaminações trazem varia de propagandas incessantes, até o roubo de dados privados. Outro risco do software “pirata” está no uso dos chamados “cracks”. Incluir essas aplicações na instalação do software não implica instabilidade somente no programa, mas também no sistema. A performance do sistema é comprovadamente reduzida devido ao uso de software não licenciado.

Do exposto neste último item do questionário, além das questões já verificadas anteriormente, faz-se necessária uma maior atenção no que tange a proteção das informações.

4 CONSIDERAÇÕES FINAIS

Ao analisarmos então as questões de estudo e os objetivos propostos no início deste artigo, pode-se concluir que a investigação atendeu ao pretendido, ampliando a compreensão sobre a importância da proteção às informações, que deve ser considerada uma das prioridades em todas as Organizações Militares, através da implantação, desde já, de procedimentos de segurança básicos, de baixo custo e complexidade, muitos dos quais já previstos e adotados pelas OM, que devem ser padronizados mediante ampla divulgação e instruções para todos os militares que trabalham em repartições militares, bem como “ligar” o sinal de alerta aos Capitães Alunos que logo estarão de volta à tropa, seja na perspectiva de exercer a função de Cmt Cia, seja na de Oficial do EM de sua OM, e propagarão essa constante preocupação que são as formas de proteger as informações de uma Organização militar.

A revisão de literatura possibilitou concluir que com a constante evolução pela qual passamos, as informações deixaram de ser armazenadas apenas em papéis, onde a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das instituições modernas, já que sem computadores e redes de comunicação, a prestação de serviços de informação poderá se tornar inviável (TRIBUNAL DE CONTAS DA UNIÃO, 2012).

Diante disso, faz-se necessária a tomada de medidas de segurança que contribuam para resguardar a imagem da instituição, tais como:

a)Restringir o acesso aos Recursos Informacionais das OM:

- O fato de um usuário ter sido identificado e autenticado não quer dizer que ele poderá acessar qualquer informação ou aplicativo sem qualquer restrição. Deve-se implementar um controle específico restringindo o acesso dos usuários apenas às aplicações, arquivos e utilitários imprescindíveis para desempenhar suas funções na instituição. Esse controle poderá ser feito por menus, funções ou arquivos. (TRIBUNAL DE CONTAS DA UNIÃO, 2012). Esta

medida pode ser desempenhada pela Seção de Informática de uma Organização Militar.

b) Prevenir o Acesso de Pessoas não autorizadas as Sessões cujas informações sejam sensíveis e sua manipulação por pessoas mal intencionadas sejam prejudiciais para a imagem da Força, vindo assim a impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da OM. Devem ser fornecidas diretrizes para áreas seguras, incluindo perímetro de segurança física, controles de entrada física (Ex: portas, janelas), segurança em escritórios, salas e instalações, proteção contra ameaças externas e do meio ambiente e acesso do público, áreas de entrega e carregamento.Para a segurança de equipamentos, são dadas recomendações para instalação e proteção do material, inclusive contra falta de energia elétrica e outras interrupções provocadas por falhas das utilidades, segurança do cabeamento e manutenção de equipamentos (TRIBUNAL DE CONTAS DA UNIÃO, 2012);

c) Controle Efetivo, por parte da Seção de Informática da OM, do acesso à Rede Mundial de Computadores (Internet), sendo permitido o acesso apenas às estações de trabalho que efetivamente necessitarem do mesmo. Ainda assim, deverão ser bloqueados os sítios que reduzam a produtividade, ou que sejam incompatíveis com o trabalho desenvolvido na seção da OM (BRASIL, 2011);

d) Utilização de contas de usuários únicas, pessoais e não compartilhadas de forma que possibilitem a identificação dos autores de atividades realizadas com privilégios administrativos no sistema operacional e no banco de dados. Esse controle deverá ser verificado pela Sessão de Informática da OM e supervisionado por cada Chefe de Seção que possuam informações relevantes nos Computadores Funcionais da OM (TRIBUNAL DE CONTAS DA UNIÃO, 2012);

e) **Proibir** a utilização de dispositivos móveis de armazenamento como: P*endrives*, celulares, 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 (BRASIL, 2011). Para uma perfeita aplicação desse procedimento, deverão ser fornecidos pelas OM dispositivos móveis funcionais e escaninhos para que sejam guardados os equipamentos pessoais.

f) 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 (BRASIL, 2011). Essa medida deve ser constantemente reforçada em reuniões dos Chefes de Seções e sempre que possível ser destinada uma instrução de quadros para todo o efetivo da Organização Militar.

A compilação dos dados colhidos nos questionários permitiu ainda identificar, que um percentual considerável do público alvo, não possui uma mentalidade de proteção à Informação, sendo necessário um engajamento por parte do Comando para que sejam difundidos em todos os níveis essas medidas e providências.

Recomenda-se, assim, que uma carga maior de instruções e verificações por parte da seção de Informática com a supervisão do Comando da OM sejam de imediato aplicadas, tendo por objetivo a proteção das Informações e consequetemente da Imagem da Força Terrestre.

REFERÊNCIAS

ASSUNÇÃO, M. F. A. **Segredos do Hacker Ético**. Florianópolis: Visual Books, 2010.

BRASIL. Exército. C 34-21: **Emprego da Guerra Eletrônica**. 2. ed. Brasília, DF, 2009.

BRASIL. Exército. Estado-Maior. **Glossário de Termos e Expressões para uso no Exército**. C 20-1. Brasília, DF: Estado-Maior do Exército, 2009.

_____._____. **Manual de Campanha Abreviaturas, Símbolos e Convenções Cartográficas**. C 21-30. Brasília, DF: Estado-Maior do Exército, 2002.

BRASIL. Exército. Comando de Operações Terrestres. **EB70-MF-10.232: Guerra Cibernética**. 1. ed. Brasília, DF: Comando de Operações Terrestres, 2017.

BRASIL. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação**. 4. Ed. Brasília, DF, 2012.

BRASIL. Exército. Estado-Maior. **Cartilha Emergencial de Segurança Tecnologia da Informação e Comunicações**. Brasília, DF: Estado-Maior do Exército, 2011.

_____._____. **Instruções Reguladoras para utilização da rede mundial de computadores (internet) por Organizações Militares e militares do Exército**. Brasília, DF: Estado-Maior do Exército, 2001.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário da língua portuguesa**, Rio de Janeiro: Nova Fronteira, 1975.