As medidas básicas de proteção cibernética na esfera de Subtenentes e Sargentos

2° Sgt Com n° 502 DIOGO LUIZ **PILZ** DOS SANTOS
2° Sgt Com nº 509 CAIO **JEREMIAS** OLIVEIRA BRITTO MARCHENA DE MORAES
2° Sgt Com nº 511 NILSON FABIANO ALVES **FELIX**
2° Sgt Com nº 526 **RUAN CARLOS** SANDY DE DEUS DAS MERCES

Orientador: 1º Sgt Com Dresch

RESUMO

Este ensaio tem como problema central verificar o grau de conhecimento dos militares frente às ameaças cibernéticas e tem como objetivo verificar em que medida os subtenentes e sargentos adotam medidas de proteção cibernética. Inicia-se com uma contextualização do surgimento dos primeiros computadores e da internet, conceituando o espaço cibernético e sua transfronteiricidade como possível ameaça à soberania de Estado. Na sequência, é exposto o emprego da Guerra Cibernética no campo militar, focando o indivíduo como fator preponderante na proteção virtual. Para isso, procurou-se levantar como a segurança das informações no cotidiano reflete também no ambiente corporativo do Exército Brasileiro. Além disso, foi realizada uma pesquisa de campo, envolvendo 151 subtenentes e sargentos, onde foi apontado que os militares estão cada vez mais inseridos no cyberspace, necessitando de mais instruções referente às medidas básicas de proteção cibernética que estão sendo negligenciadas neste universo. Por fim, dado o resultado da pesquisa, concluiu-se que a falta de aplicabilidade de métodos básicos de defesa virtual está atrelado à carência de instruções nas OM, e, sobretudo, nas escolas de formação e de aperfeiçoamento de sargentos.

Palavras-chave: Proteção Cibernética. Segurança da Informação. Ensino e Formação.

1 INTRODUÇÃO

A Guerra Cibernética (G Ciber) é parte integrante do campo de estudos que imbrica as áreas de Segurança da Informação e de Segurança Cibernética. No âmbito das Forças Armadas, a G Ciber se restringe aos níveis operacional e tático em que as tecnologias da informação e comunicações são instrumentos dos diversos tipos de ações cibernéticas. Estas ações visam precarizar adversários e oponentes ou ainda defender seus próprios sistemas de informação (BRASIL, 2017).

Neste contexto, de defesa dos sistemas cibernéticos, o estudo será focado no emprego das medidas de proteção cibernética no meio militar. Para isso, delineou-se o seguinte problema de pesquisa: "Qual o grau de conhecimento militar frente às ameaças cibernéticas?". E para isto este trabalho tem como objetivo verificar em que medida os subtenentes e sargentos do Exército Brasileiro (EB)

adotam hábitos de proteção cibernética no campo militar. Nesse sentido, a metodologia utilizada foi a pesquisa documental e bibliográfica, além de pesquisa qualitativa no universo dos subtenentes e sargentos do Exército Brasileiro.

Na primeira seção foi apresentado o Setor Cibernético, suas origens e conceitos básicos. Na sequência, é apontado o emprego da G Ciber no campo militar, no âmbito da Força Terrestre. Na terceira parte, retrata-se o reflexo da falta de proteção cibernética no ambiente corporativo do EB causado pelos descuidos individuais com dados de toda a ordem que podem vir a revelar brechas e vulnerabilidades virtuais. Em seguida, é apresentado e debatido o resultado da pesquisa aplicada em 151 militares, do círculo de subtenentes e sargentos. Logo após, chega-se à conclusão do ensaio.

2 REFERENCIAL TEÓRICO

2.1 Setor cibernético

O final do século XX ficou marcado pelo início da revolução digital. A impulsão da tecnologia aconteceu nos anos 60, fomentada majoritariamente pelos militares americanos. O primeiro computador industrial foi criado em 1969. E, nos anos 70, a Agência de Pesquisa Avançada do Departamento de Defesa norte-americano implementou e instalou uma rede eletrônica de comunicação, a qual veio a se transformar na internet. A partir desse contexto, os meios e os sistemas de Tecnologia da Informação e Comunicações (TIC) evoluíram a ponto de mudar o modo da sociedade interagir, inserindo o espaço virtual na organização dos Estados, nas relações e no convívio social. É nesse cenário informatizado que estão inseridas as infraestruturas críticas das nações em diversos setores estatais como: o energético, o financeiro, o de transportes, o de telecomunicações, e o de Defesa.

O espaço virtual, também denominado de espaço cibernético (cyberspace ou ciberespaço), é um aglomerado de dispositivos computacionais individuais que são conectados entre si e ao mundo exterior via algum tipo de rede de comunicações (LIBICKI, 2009, p. 6). O manual EB70-MC-10.232, Guerra Cibernética (BRASIL, 2017), caracteriza o Espaço Cibernético como o espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas.

Ademais, Carneiro (2012, p. 80) apresenta uma teoria em que o Espaço Cibernético é dividido em três camadas, a física, a lógica e a social. A camada física consiste nos computadores, nos roteadores, cabos e conectores de rede, ou seja, os elementos físicos, caracterizando um local de acesso geográfico. Para se conectar a outro dispositivo é necessário o acesso à camada lógica, a qual é responsável pelos diversos protocolos de internet, e todas as conexões com a interface virtual, onde ocorre a interação e trânsito de informação online independente do espaço geográfico que o dispositivo se localiza, qualificando assim a transfronteiricidade do espaço cibernético. Por último, a camada social representa os aspectos humanos e cognitivos interagindo com as camadas anteriores.

É dessa forma que o ciberespaço transcende os limites fronteiriços consagrados entre as Nações, possibilitando atuações cibernéticas (G Ciber), criando espaços para novas perspectivas de segurança e ameaça à Defesa Nacional de um país. Neste ínterim, em 2008, o Brasil publicou a Estratégia Nacional de Defesa (END), que definiu os setores espacial, nuclear e cibernético como estratégicos para a Defesa Nacional, incumbindo ao Exército Brasileiro o desenvolvimento do setor cibernético. Em 2010 foi criado o Centro de Defesa Cibernética (CDCiber). Em 2012, a END foi atualizada, e foi publicada a Política Cibernética de Defesa para orientar, no que tange ao Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de G Ciber, nos níveis operacional e tático. E em 2015, foi criado o Comando de Defesa Cibernética (ComDCiber)

com o propósito de estabelecer estruturas operacionais e táticas relativas ao setor cibernético no âmbito do Exército Brasileiro com o propósito de contribuir com o nível estratégico na defesa do país.

2.2 Emprego da guerra cibernética no campo militar no âmbito do Exército Brasileiro

Adequando-se à END, a doutrina militar passou a considerar o Espaço Cibernético como uma nova dimensão nos assuntos de Defesa. Surgiu assim um novo vetor de combate, com efetividade decisiva, utilizando a Tecnologia da Informação (BRASIL, 2014).

O manual EB70-MC-10.232 define a G Ciber sendo o uso ofensivo e defensivo de informações e sistemas de informação para negar a capacidade de Comando e Controle ao inimigo, explorando, corrompendo, degradando ou destruindo-o. Utilizando de ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas do oponente e defender os próprios (BRASIL, 2017).

A G Ciber atua no emprego militar tático como um multiplicador do poder de combate. Nesse sentido, o conceito operativo do Exército Brasileiro demanda que os comandantes saibam atuar no espaço cibernético, aplicando e empregando a capacidade militar terrestre cibernética nas operações junto com as funções de combate (BRASIL, 2017).

Logo, tendo em vista o seu emprego, a G Ciber pode ser resumida em três atividades: o ataque cibernético, a proteção cibernética e a exploração cibernética, também denominada capacidades operativas (BRASIL, 2017). Tais capacidades estão descritas no Quadro 1, a seguir.

Quadro 1: - Descrição das Capacidades Operativas na G Ciber

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz 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. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: Manual de Guerra Cibernética (BRASIL, 2017).

As capacidades operativas descritas acima podem colaborar e apoiar exponencialmente as funções de combate (movimento e manobra, inteligência, fogos, proteção, comando e controle e logística), principalmente as que já estão informatizadas, potencializando a dinâmica e as vantagens nas operações.

Além disso, a G Ciber dispensa o uso de muita energia cinética no campo de batalha, economizando meios de combate, trocando a ação no espaço-tempo físico pela ação no espaço virtual da rede de computadores. É importante ressaltar que o termo designa uma forma de guerra, a ser disputada no espaço cibernético, no entanto, a rigor uma guerra cibernética entre duas ou mais nações nunca foi travada de maneira declarada e pública.

Em tempo de paz, a ameaça de uma G Ciber ou do uso de ações cibernéticas a fim de obter informações relevantes de uma determinada nação, sobretudo nos aspectos governamentais, econômicos e militares, já é uma realidade. O que configura um cenário no qual demanda a necessidade de proteção das informações e dos meios informatizados. O Quadro 1 apresenta claramente a necessidade da atividade de Proteção Cibernética ser de caráter permanente.

O Exército Brasileiro utiliza as redes do Sistema de Comando e Controle do Exército (SC2Ex) para fins operativo e administrativo, cujos operadores, normalmente, são militares graduados de diferentes QMS nas diversas organizações. Diante desse fato, cabe uma reflexão a respeito da responsabilidade (conhecimento) individual na proteção permanente da infraestrutura militar.

2.3 O reflexo da falta de proteção cibernética no ambiente corporativo do Exército Brasileiro

A má utilização dos dispositivos por parte dos militares pode impactar diretamente na segurança dos sistemas nos quais trafegam as informações de interesse da força. À medida que há um aumento do número de crimes praticados por meio da internet, torna-se importante a conscientização coletiva em termos de segurança cibernética. Há uma tendência das pessoas em confiar nos sistemas e aplicativos, supondo que as informações estarão seguras, livres de ação hacker e de ataques cibernéticos. No entanto, existe uma série de medidas básicas de proteção cibernética que podem ser observadas para dirimir a exposição de dados sensíveis tais como a utilização de firewalls; a utilização de senhas fortes que devem ser trocadas regularmente; o gerenciamento do histórico das senhas salvas nos navegadores e sistemas operacionais; a autenticação nos aplicativos em duas ou mais etapas; o gerenciamento de logins nos dispositivos, sejam eles pessoais ou corporativos; o gerenciamento do histórico de páginas acessadas; e a proteção dos cookies pelo usuário.

Para corroborar com as medidas apresentadas, Waschburger (2015), elenca algumas situações as quais podem comprometer a segurança das informações, como: os e-mails falsos utilizados para phishing ou a disseminação de malwares; a falta de utilização de sistemas de detecção de intrusão; a ausência de utilização de normas tais como as preconizadas na ISO 27.001; a engenharia social e a própria falta de conscientização da equipe envolvida.

Dados estão sendo captados a todo o momento em que se navega na internet, de modo que até mesmo o histórico de navegação passa a ser uma fonte de informação, a qual pode ser utilizada por algoritmos com inteligência artificial e por redes neurais. Ademais, existem empresas que utilizam essas tecnologias que servem para identificar perfis de usuário e usar da imitação e da manipulação para alcançar seus objetivos. A importância desse tema é tamanha que recentemente, no Brasil, foi sancionada a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (BRASIL, 2018) que regula as atividades de tratamento de dados pessoais, entretanto esse tema foge ao escopo deste ensaio e fica como sugestão para trabalhos futuros.

No âmbito do Exército, os militares lidam com dados cotidianamente na confecção e na tramitação de documentos. Além disso, são gerenciados sistemas informatizados de dados os quais alimentam a Base de Dados Corporativa de Pessoal do Exército, portanto, há que se dar a devida importância à proteção dessas informações. Na pesquisa que será posteriormente analisada, foi verificado que o público interno tem pouco conhecimento acerca de segurança da informação, o que demonstra uma carência na instrução e nas informações disponibilizadas sobre o tema no âmbito da formação, o que, por sua vez, acarreta uma falta de cultura de defesa cibernética. A falta dessa cultura impacta no cuidado tanto no tratamento pessoal das informações como no tratamento profissional e corporativo.

2.4 Apresentação e discussão dos resultados da pesquisa

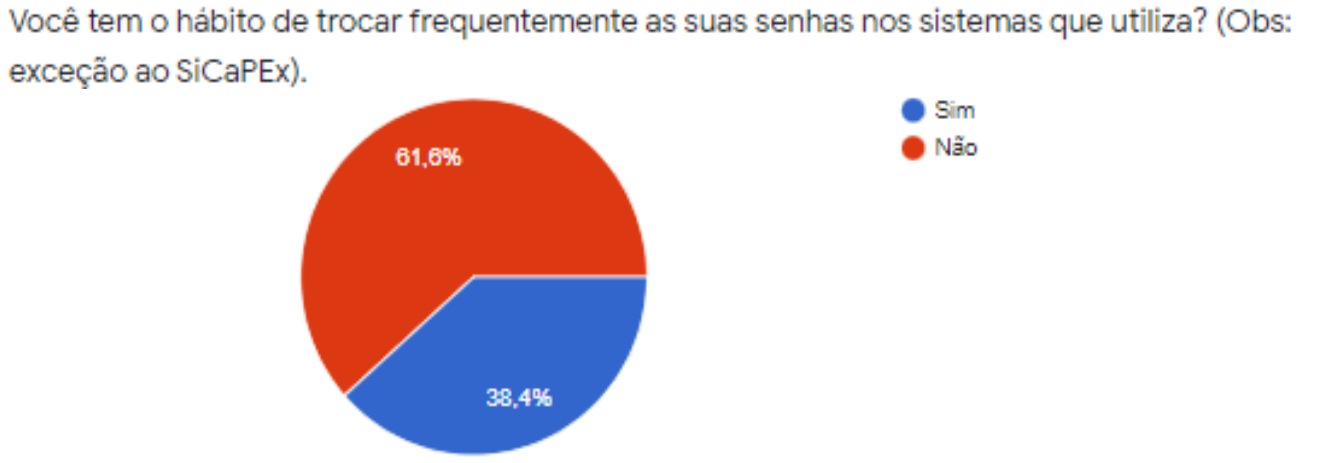
Nesta seção serão apresentados os resultados da pesquisa de campo realizada para este ensaio, composta de oito perguntas. Participaram do questionário um total de 151 subtenentes e sargentos de diversas QMS.

A primeira e a segunda perguntas tiveram a finalidade de verificar o quantitativo de subtenentes e sargentos do Exército, e suas QMS. Visto que o conhecimento sobre a Guerra Cibernética se mostra de vital importância para o EB, uma vez que subtenentes e sargentos são os principais difusores de conhecimento dentro da instituição na medida em que são o elo entre o comando e a tropa.

A terceira questão visa saber quantos entrevistados utilizaram algum equipamento conectado à internet para o cumprimento de alguma missão operacional. Ficou demonstrado que 77,5% da amostra utilizou esse tipo de ferramenta, apontando que o uso de equipamentos cibernéticos por subtenentes e sargentos é uma realidade. Em seguida foi perguntado se as medidas de proteção cibernética são um assunto importante para todas as QMs e graduações, 98% dos participantes responderam que sim, o que demonstra certa preocupação dos militares nesta área do conhecimento no campo militar.

Outrossim, a quinta pergunta: "Você tem o hábito de trocar frequentemente as suas senhas nos sistemas que utiliza?", teve como resposta majoritária "não", com 61,6%, isso evidencia que muitos militares não possuem o costume de realizar procedimentos básicos referentes à proteção de sistemas sensíveis. Apresentou também uma displicência em procedimentos aparentemente simples, os quais podem ocasionar brechas para ataques e explorações virtuais atentando contra a segurança cibernética no campo militar. Pode-se acompanhar o resultado dessa pergunta no Gráfico 1, a seguir.

Gráfico 1: - Militares que tem o hábito de trocar frequentemente as suas senhas nos sistemas que utiliza

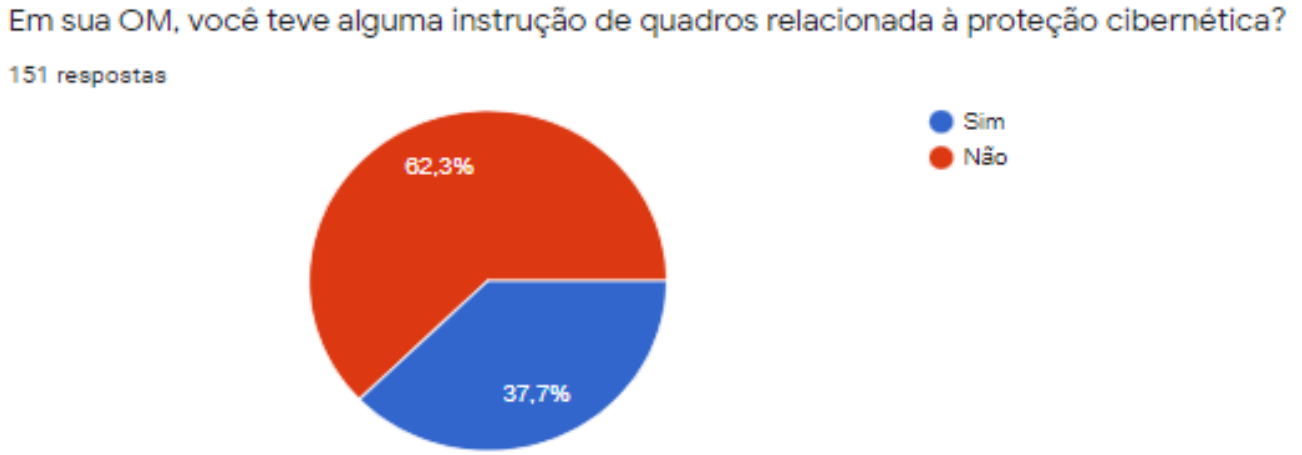


Fonte: apêndice A. Elaborado pelos autores (2021).

Em consonância com a questão anterior, na pergunta: "Você já visualizou algum destes documentos tramitando através de aplicativos de mensagem?", os entrevistados apontaram diversos documentos militares que foram visualizados pelo universo amostral em aplicativos de mensagens. Foram citados desde Documentos Internos do Exército (DIEx), até boletins reservados e relatórios de missões. Estas respostas apontam o desleixo e falta de conhecimento por muitos militares que usam softwares civis para compartilhar dados sensíveis da Força. Finalizando o questionário, foram realizadas as perguntas: "Em sua OM, você teve alguma instrução de quadros relacionada à proteção cibernética?" (Gráfico 2) e "Durante a sua formação você teve alguma instrução abordando as medidas de proteção cibernética?" (Gráfico 3).

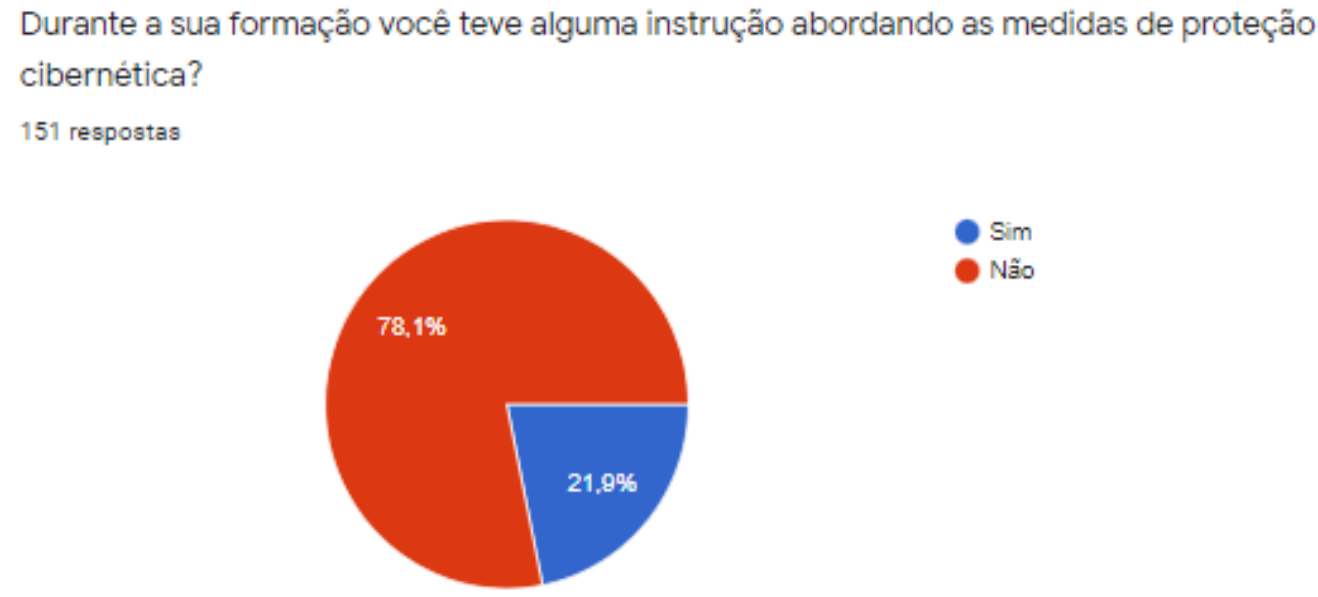
Para esta pergunta 62,3% dos entrevistados responderam que "não" e para aquela pergunta 78,1%, respondeu que "não", as respostas aos questionamentos revelam falhas no processo de proteção cibernética pelos próprios usuários que utilizam os sistemas. Não há instruções relativas as medidas de proteção cibernética na maioria das Organizações Militares, inclusive nas Escolas. Este fato contribui diretamente para a falta de cultura de proteção cibernética no âmbito dos subtenentes e sargentos.

Gráfico 2: - Entrevistados que tiveram alguma instrução de proteção cibernética em suas OM



Fonte: apêndice A. Elaborado pelos autores (2021).

Gráfico 3: - Entrevistados que tiveram alguma instrução de proteção cibernética durante a sua formação



Fonte: apêndice A. Elaborado pelos autores (2021).

Ao analisar as respostas obtidas no questionário, foi verificado que existe falta de conhecimento em relação à segurança cibernética. Sugere-se com este ensaio que todas as OM, inclusive Escolas como ESA e EASA, planejem instruções presenciais com foco na Guerra Cibernética para os seus efetivos profissionais e corpo de alunos, não só de comunicações, mas sim para todas as QMS. Essas instruções devem se concentrar nas noções básicas de proteção cibernética, tendo em vista que o universo de subtenentes e sargentos que utilizam equipamentos interligados à rede mundial de dados é cada vez maior, tanto em funções administrativas, quanto em funções operacionais afetando diretamente o campo militar. Em relação aos militares da Arma de Comunicações, as Escolas de Formação e Aperfeiçoamento poderiam prepará-los adicionando mais instruções de G Ciber, o que implicaria em mais conhecimento a fim de que estes pudessem desempenhar funções mais sensíveis e pudessem disseminar a importância das medidas de proteção cibernética básicas nas suas organizações militares.

Por fim, a formação cibernética dos sargentos pode basear-se na formação dos cadetes da Academia Militar das Agulhas Negras , conforme aponta Salustriano (2020). A instrução de cibernética é comum desde o primeiro ano e a partir do segundo ano esta disciplina é exclusiva ao curso de comunicações que aprofunda seus conhecimentos na área, e tem a possibilidade de realização de um Estágio de Defesa Cibernética no quarto ano do curso.

3 CONCLUSÃO

Por meio desse ensaio, buscou-se levantar as deficiências do público interno, em relação à falta de cultura cibernética acerca do emprego da segurança e proteção de dados, tópicos que compõem os pilares da G Ciber, no campo militar Ao analisar os resultados da pesquisa, é salientado que sejam tomadas medidas preventivas e corretivas, no âmbito do ensino, da formação e do aperfeiçoamento, dos subtenentes e sargentos do Exército Brasileiro para que a falta de cultura cibernética não se transforme em prejuízo no campo militar. Procurou-se também correlacionar a conscientização individual, através da implementação de medidas básicas de proteção. Tais medidas implicariam em uma gradativa mudança de hábito, impactando o ambiente profissional da força e promovendo uma cultura de proteção cibernética. Hábitos individuais prudentes no tratamento dos dados acarretarão em comportamentos corporativos igualmente prudentes na proteção de dados do Exército.

Este não é um tema que se encerra neste trabalho, a cultura de proteção cibernética no campo militar é um assunto a ser explorado em todos os círculos. Neste ensaio, foi selecionado o universo de subtenentes e sargentos, entretanto essa pesquisa pode ser ampliada para os oficiais, cabos e soldados. Este estudo pode servir de referência ao escalão superior, pois apresenta informações atualizadas sobre a respeito da magnitude da cultura cibernética em um determinado grupo em um determinado período.

Diante do exposto, reforça-se que o ensino, a formação e o aperfeiçoamento devem ser contínuos e devem acompanhar as mudanças tecnológicas de segurança e proteção da informação que são pilares da G Ciber. Essa continuidade, conforme descrito anteriormente, pode se dar por meio de instruções presenciais no começo da carreira dos sargentos, ainda nas escolas de formação e de aperfeiçoamento de modo a proporcionar um aumento significativo na cultura cibernética nos elos de comando da tropa de forma permanente. Pode-se utilizar de informativos no âmbito de cada OM, para aumentar a divulgação através de canais existentes, tais como o "Fique Atento", mensagens da nossa inteligência e, ainda, em instruções de quadros. Desse modo, a conscientização acerca do tema por parte de cada militar vai possibilitá-lo a, tanto no ambiente administrativo como no ambiente operacional, observar e operar as informações repassadas

pelo escalão superior com o devido cuidado para que elas não venham a ser utilizadas por terceiros, fazendo com que comprometam o interesse e a imagem do Exército Brasileiro.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 out. 21.

BRASIL. Ministério da Defesa (MD). Doutrina Militar de Defesa Cibernética. MD31-M-07. Brasília, DF: Ministério da Defesa. 18 de novembro de 2014. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/136. Acesso em: 28 out. 2021.

BRASIL. Ministério da Defesa (MD). Manual de Campanha Guerra Cibernética. EB70-MC 10.232. Brasília, DF: Ministério da Defesa. 8 de junho de 2017.

CARNEIRO, J. M. E. A Guerra Cibernética: uma proposta de elementos para a formulação doutrinária no Exército Brasileiro. Tese de Doutorado - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Brasil, 2012.

CASTELLS, M. A Era da Informação: Economia, Sociedade e Cultura, Vol. I, A Sociedade em Rede. Fundação Calouste Gulbenkian. Lisboa, 2002.

LIBICKI, Martin C. Cyberspace Is Not a Warfighting Domain. I/S Journal of Law and Policy for the Information Society, v.8, n.2, 2012. Disponível em: https://kb.osu.edu/handle/1811/73111. Acesso em: 28 out. 2021.

SALUSTRIANO, Wagner de Matos. Capacitação de Cadetes da Academia Militar das Agulhas Negras (AMAN) em Cibernética: a descoberta de novos talentos para o setor. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/8736/1/MO%206329%20-%20WAGNER.pdf. Acesso em: 28 out. 21.

SILVA, Júlio Cezar Barreto Leite da. Guerra Cibernética: A Guerra no quinto domínio, conceituação e princípios. Artigo Científico - R. Esc Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193 – 211, jan./jun. 2014.

TEIXEIRA, A.; LOPES, G. V.; FREITAS, M. T. D. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. Revista Carta Internacional, Belo Horizonte, v. 12, n. 3, 2017, p. 30-53.

WASCHBURGER, L. R. Segurança da Informação - Conhecimentos Necessários para as empresas atuais. Trabalho de Conclusão de Curso (Especialização em Redes de Computadores) - Universidade Tecnológica Federal do Paraná. Pato Branco, 2015. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/7131/1/PB_ESPRC_II_2015_16.pdf. Acesso em: 28 out. 21.

Apêndice A: - QUESTIONÁRIO ACERCA DE MEDIDAS BÁSICAS DE PROTEÇÃO CIBERNÉTICA COM RESPOSTAS

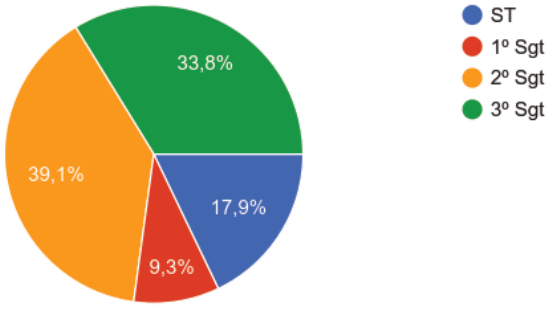
Questionário acerca de medidas básicas de proteção cibernética.

151 respostas

Publicar análise

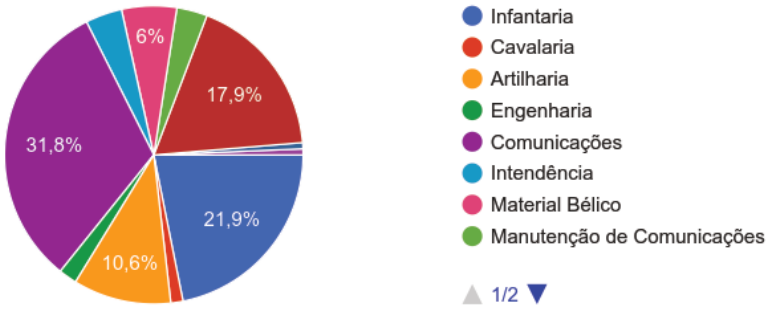
Qual é a sua graduação?

151 respostas



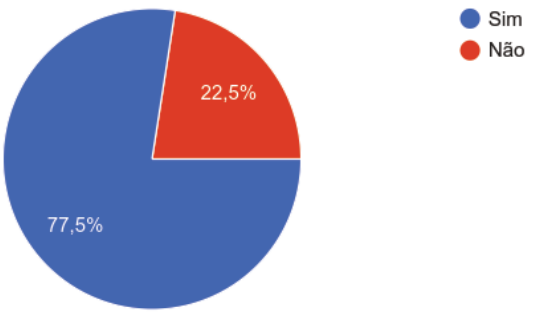
Qual sua QMS?

151 respostas



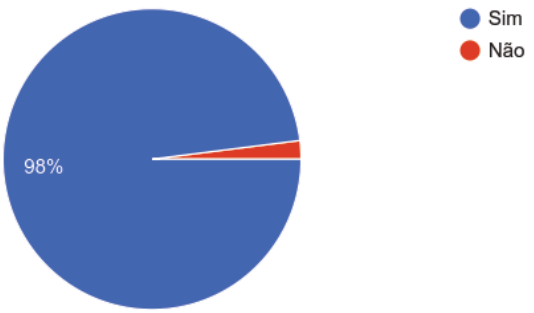
Você já utilizou algum equipamento conectado à rede mundial de computadores (internet) para o cumprimento de alguma missão operacional?

151 respostas



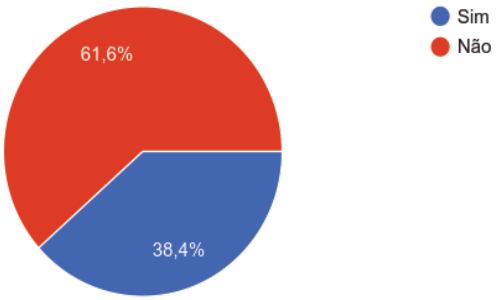
Você acredita que as medidas de proteção cibernética é um tema que deve ser de conhecimento em todas as QMS, postos e graduações?

151 respostas



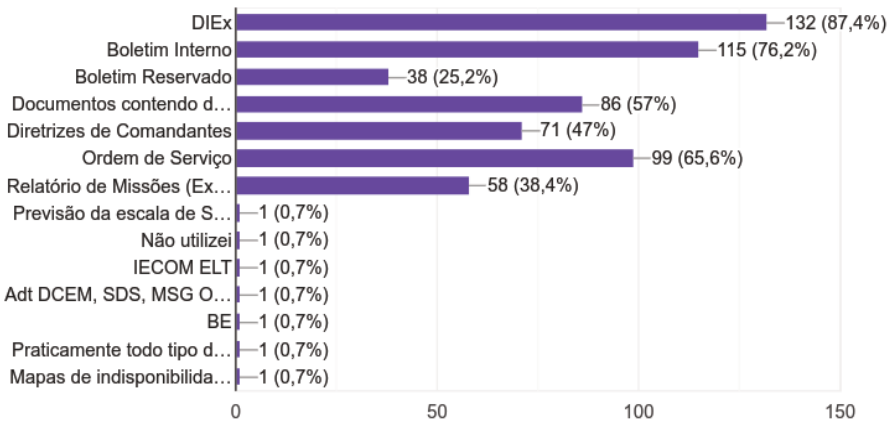
Você tem o hábito de trocar frequentemente as suas senhas nos sistemas que utiliza? (Obs: exceção ao SiCaPEx).

151 respostas



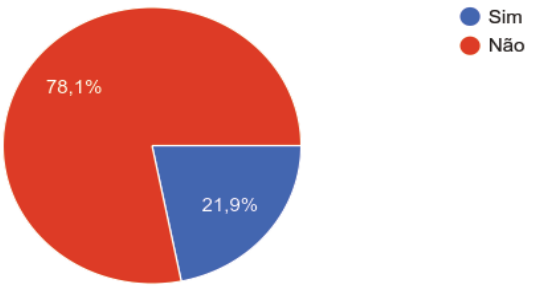
Você já visualizou algum destes documentos tramitando através de aplicativos de mensagem?

151 respostas



Durante a sua formação você teve alguma instrução abordando as medidas de proteção cibernética?

151 respostas



Em sua OM, você teve alguma instrução de quadros relacionada à proteção cibernética?

151 respostas