ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM ANDRÉ DE JESUS PORTO

SEGURANÇA E PROTEÇÃO CIBERNÉTICA NA FORMAÇÃO DO SARGENTO COMBATENTE DE COMUNICAÇÕES

Rio de Janeiro
2020

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP COM ANDRÉ DE JESUS PORTO

SEGURANÇA E PROTEÇÃO CIBERNÉTICA NA FORMAÇÃO DO SARGENTO COMBATENTE DE COMUNICAÇÕES

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
2020

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 Com ANDRÉ DE JESUS PORTO**

Título: **SEGURANÇA E PROTEÇÃO CIBERNÉTICA NA FORMAÇÃO DO SARGENTO COMBATENTE DE COMUNICAÇÕES.**

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
_____ **DARDANO DO NASCIMENTO MOTA – Ten Cel** Cmt Curso e Presidente da Comissão	
_____ **RAFAEL VILLAR OLIVEIRA - Cap** 1º Membro	
_____ **GLAUCO GONÇALVES DA SILVA - Cap** 2º Membro e Orientador	

_____
ANDRÉ DE JESUS PORTO – Cap
Aluno

SEGURANÇA E PROTEÇÃO CIBERNÉTICA NA FORMAÇÃO DO SARGENTO COMBATENTE DE COMUNICAÇÕES

André de Jesus Porto[*]
Glauco Gonçalves da Silva[**]

RESUMO
A revolução tecnológica trazida pela internet no final do século XX e início do século XXI trouxe um mundo virtual conectado, porém que apresenta muitas ameaças e vulnerabilidades, os ataques cibernéticos. O Brasil, diante deste cenário, através da Estratégia Nacional de Defesa, atribuiu a responsabilidade pela proteção do espaço cibernético ao Exército Brasileiro. O presente artigo científico visa abordar a segurança e proteção cibernética na formação do sargento combatente da Arma de Comunicações, formado pela Escola de Sargentos das Armas (ESA), através da análise do plano de disciplina utilizado atualmente, diante de uma sociedade cada vez mais conectada, na qual o sargento tem um papel fundamental dentro das organizações miliares do Exército.

Palavras-chave: Ataque cibernético. Segurança. Proteção cibernética. Arma de Comunicações. Escola de Sargentos das Armas.

ABSTRACT
A technological revolution brought about by the internet in the late 20th century and the beginning of the 21st century brought a connected virtual world, but one that presents many threats and vulnerabilities, cyber attacks. Brazil, faced with this scenario, through the National Defense Strategy, attributed a responsibility for the protection of cyberspace to the Brazilian Army. The present scientific article aims to address cyber security and protection in the training of the Combatant Sergeant of the Signal Corps, formed by the School of Sergeants of Arms (ESA), through the analysis of the discipline plan currently studied, in the face of an increasingly connected, in which the sergeant has a fundamental role within the military organizations of the Army.

Keywords: Cyber attack. Security. Cyber protection. Signal Corps. School of Sergeants of Arms.

[*] Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2011. Pós-graduando em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) em 2020.
[**] Capitão da Arma de Comunicações. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2009. Pós-graduado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) em 2019.

1 INTRODUÇÃO

Diante da Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, no qual ficam estabelecidas as diretrizes e orientações para a atuação da Marinha, do Exército e da Aeronáutica nos setores estratégicos para o governo federal, coube ao Exército Brasileiro a responsabilidade pelo setor cibernético.

Sendo assim, a Escola de Sargentos das Armas como parte integrante do Exército Brasileiro, deve buscar o ensino voltado para a segurança e proteção cibernética, visando que sejam formados militares com os conhecimentos nessa área e que sejam capazes de difundir essa mentalidade por todo a Força.

Devido ao crescente avanço tecnológico pelo qual o mundo passa, o compartilhamento de informações ocorre de maneira quase que instantânea, levando muitas vezes as pessoas a negligenciarem alguns aspectos de segurança em detrimento do objetivo de se conectar e transmitir uma informação de maneira rápida, porém não segura. Sendo assim, o hacker se aproveita dessa característica atual da sociedade e realiza o ataque, obtendo informações confidenciais desses indivíduos que não se preocupam com a segurança, conforme observado pelos autores Nakamura e Geus (2007, p. 29): “A informática é um instrumento cada vez mais utilizado pelo homem, o qual busca incessantemente realizar seus trabalhos de modo mais fácil, mais rápido, mais eficiente e mais competitivo [...]”.

Em uma sociedade cada vez mais conectada, seja pelo uso de computadores ou pelo uso de *smartphones,* o conceito de rede e a importância de manter-se políticas de segurança vem crescendo muito, seja em ambientes corporativos ou no Exército Brasileiro, principalmente com o histórico de evolução de ataques cibernéticos acontecidos nos últimos anos.

Segundo Mitshashi (2011), o assunto rede refere-se sempre a algum tipo de compartilhamento seja de recursos ou de informações. Com o aumento crescente do acesso à internet, a necessidade de segurança da informação fez-se necessária, principalmente pela grande quantidade de vírus circulando pela rede e, principalmente devido ao crescimento da quantidade de ataques de hackers.

Nesse contexto, as redes sem fio vieram para ajudar ainda mais as pessoas a se conectarem, principalmente pelo fato de o usuário não precisar mais estar conectado em uma rede cabeada para se comunicar. Porém essa facilidade trouxe alguns problemas quanto à segurança das informações que trafegam nesse novo

meio de comunicação tão popular na atualidade, o que fica comprovado pelos autores Nakamura e Geus (2007, p. 169) ao afirmarem: “As redes sem fio representam uma nova forma de acesso aos usuários e trazem grandes benefícios. Porém, elas trazem consigo alguns riscos inerentes às novas tecnologias [...]”.

Diante dessas informações, é desejável que a Escola de Sargentos das Armas, sendo a única Instituição de Ensino formadora do sargento combatente de carreira do Exército Brasileiro, tenha como objetivo de ensino a Segurança e Proteção Cibernética para seus alunos, integrando-se, assim, com os objetivos da Estratégia Nacional de Defesa.

Portanto, apesar de toda a transformação que a utilização da internet trouxe para o mundo, é necessário que medidas de segurança e proteção cibernética sejam tomadas por cada um que navega na grande rede. Sendo assim, o conhecimento dessas medidas torna-se essencial para a proteção dos dados pessoais e da Instituição Exército Brasileiro.

1.1 PROBLEMA

Com o rápido desenvolvimento tecnológico que o mundo passa, é cada vez mais difícil estar protegido de todas as ameaças à que estamos expostos, principalmente quando navega-se na Internet, mas também quando há o compartilhamento de informações, seja por e-mail, mensagens na rede interna ou até mesmo arquivos transmitidos através de dispositivos móveis como, por exemplo, pen drives e hds externos.

Atualmente, observa-se, por grande parte dos militares uma falta de conhecimento de políticas de segurança e proteção cibernética, em particular os praças, diante das ameaças presentes na Internet e que podem prejudicar tanto o militar, quanto a Organização Militar (OM) em que serve, haja vista os subtenentes e sargentos operarem grande parte dos sistemas informatizados do Exército. Existe a necessidade de que eles detenham um maior conhecimento sobre os meios cibernéticos, principalmente no tocante a proteção e segurança cibernética. Essa falta de conhecimento no assunto pode causar danos pessoais e financeiros com a exposição dessas informações no ambiente da Internet.

Neste ambiente, a informação é cada vez mais importante para a sociedade, seja para as instituições públicas ou privadas. Cresce de importância a implementação de políticas de segurança da informação, conforme afirma Freitas.

> [...] as organizações estão cada vez mais dependentes da Tecnologia da Informação. A informação é um ativo não tangível da organização e assim como os ativos tangíveis e financeiros, a organização deve dedicar sua atenção à segurança deste ativo que é a informação que possuem. Falhas e desastres em sistemas de informação podem levar a grandes prejuízos e até à falência de uma empresa (FREITAS, 2009, P. 8).

Dessa forma, após a análise desses fatores citados, foi elaborado o seguinte problema: O ensino de Segurança e Proteção Cibernética na formação do sargento combatente de Comunicações é o suficiente na implementação de medidas de segurança e proteção cibernética em suas futuras Organizações Militares?

1.2 OBJETIVOS

O presente artigo científico tem como objetivo geral avaliar se o sargento, recém egresso das escolas de formação, chega à tropa com os conhecimentos de cibernética necessários para prover a proteção e segurança dos sistemas informatizados do Exército Brasileiro.

Para viabilizar a consecução do objetivo geral de estudo, foram formulados os objetivos específicos, abaixo relacionados, que permitiram o encadeamento lógico do raciocínio descritivo apresentado neste estudo:

a) Apreciar o PLADIS do curso de Comunicações da ESA, verificando se nele, comtemplam instruções de cibernética e ações de proteção e defesa contra os principais ataques cibernéticos; e

b) Propor uma nova abordagem, caso seja necessário, sobre segurança e defesa cibernética no PLADIS.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

Este trabalho justifica-se pela necessidade de o sargento sair da escola de formação com o conhecimento de segurança e proteção cibernética. Os subtenentes e sargentos devem ter este conhecimento pois eles operam a maioria dos sistemas informatizados do EB, sendo assim, eles têm que deter esse conhecimento.

Outro fator que justifica este trabalho, é o crescimento de ataques cibernéticos no Brasil e no mundo, conforme pesquisa realizada pelo Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br), e que está representado no Gráfico 1, no qual observa-se a tendência de aumento no total de incidentes de segurança na internet no Brasil. Dessa forma, cresce de importância que medidas de segurança e proteção cibernética sejam tomadas por cada um dos usuários da internet, visando diminuir a exposição aos

riscos que a existentes na internet.

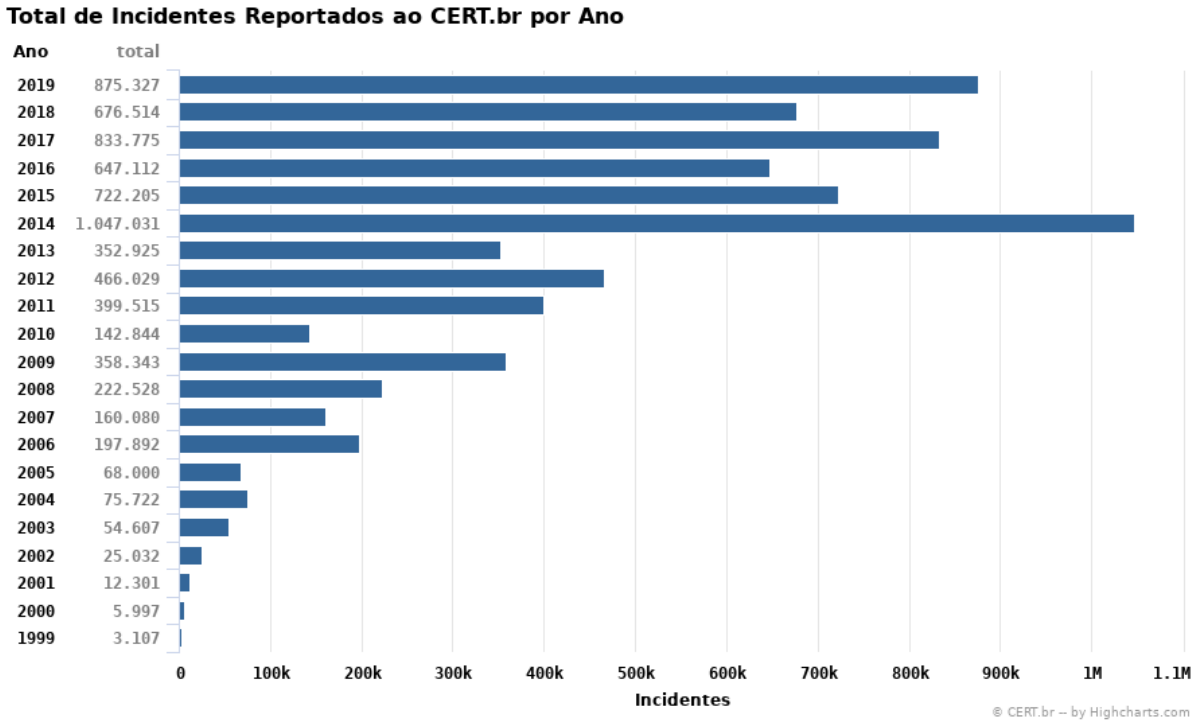


GRÁFICO 1 – Estatísticas dos Incidentes Reportados ao CERT.br
Fonte: CERT.br

Nakamura e Geus (2007, p.173) afirmam que: “A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações.” Dessa maneira, será possível contribuir com o Exército Brasileiro, no sentido da relevância desse assunto para proteção individual do militar, de seus dados pessoais que podem circular pela internet, assim como para a proteção da Instituição, que poderia ter alguma informação sigilosa exposta na rede mundial de computadores.

Ainda sobre o assunto, conforme publicação da Agência Senado de 5 de setembro de 2019, Brasil é 2º no mundo em perdas por ataques cibernéticos:

> O Brasil ocupa a 70º colocação no índice de segurança cibernética da União Internacional de Telecomunicações (ITU, na sigla em inglês), órgão da Organização das Nações Unidas (ONU) que coordena esforços nesta área. Essa situação de fragilidade faz com que o país seja hoje o segundo no mundo que mais tem sofrido perdas econômicas advindas de ataques cibernéticos. Segundo os dados mais recentes da ITU, numa medição de 12 meses entre 2017 e 2018, os prejuízos advindos dos ataques cibernéticos no Brasil ultrapassaram US$ 20 bilhões (mais de R$ 80 bilhões). (Fonte: Agência Senado).

Diante desse cenário, cresce de importância que o sargento seja formado com os conhecimentos de segurança e proteção cibernética, visto que os subtenentes e sargentos operam a maioria dos sistemas informatizados do Exército Brasileiro.

2 METODOLOGIA

A partir do problema apresentado, busca-se colher subsídios que permitam formular uma possível solução para o problema, a necessidade de os alunos saírem da escola de formação com o conhecimento de segurança e proteção cibernética.

Quanto à forma de abordagem, foi utilizado, principalmente, a pesquisa **quantitativa**, pois as referências numéricas obtidas por meio dos questionários foram fundamentais para a uma possível solução do problema apresentado.

Quanto ao objetivo geral, foi empregado a modalidade **exploratória**, tendo em vista o assunto ser recente e pouco explorado, sendo necessário um aprofundamento inicial sobre o tema, através de pesquisas na internet, representadas nas citações presentes neste artigo de diversos autores que já publicaram acerca do assunto, seguida de um levantamento e interrogação direta a um grupo significativo de pessoas que estão envolvidas com o objeto de estudo.

2.1 REVISÃO DE LITERATURA

O delineamento da pesquisa foi iniciado com a definição de termos e conceitos, a fim de viabilizar a uma possível solução do problema de pesquisa, sendo baseada em uma revisão de literatura no período de jan/2007 a ago/2020. Essa delimitação baseou-se nas primeiras publicações sobre o assunto, diante da constante evolução dos ataques cibernéticos, visto que as tecnologias se encontram em constante evolução e o Exército Brasileiro, através da END, iniciou suas atividades nesse setor, demonstrando grande preocupação com o tema.

O limite anterior foi determinado buscando incluir as análises de Nakamura e Geus sobre políticas de segurança da informação, ativo importante de interesse para ataques cibernéticos. Assim como, a publicação no ano seguinte da Estratégia Nacional de Defesa, que foi determinante para o estabelecimento do Setor Cibernético como responsabilidade do Exército Brasileiro.

Foram utilizadas as palavras-chave Ataque cibernético, Segurança, Proteção cibernética, Arma de Comunicações, Escola de Sargentos das Armas, juntamente com seus correlatos em inglês e espanhol, na plataforma de Dados EB Conhecer, em sítios eletrônicos de procura na internet e na biblioteca de monografias da Escola de Aperfeiçoamento de Oficiais (EsAO), sendo selecionados apenas os artigos em português, inglês e espanhol.

a. Critério de inclusão:

- Estudos publicados em português, espanhol ou inglês, relacionados à guerra cibernética, ataques cibernéticos, proteção e segurança cibernética, segurança da informação e segurança de rede;

- Livros, estudos, matérias jornalísticas e portifólio de empresas que retratam inovações tecnológicas com foco na segurança cibernética e segurança de rede; e

- Estudos qualitativos sobre o conhecimento de proteção cibernética pelo militar usuário da internet na rede corporativa.

b. Critério de exclusão:

- Estudos detalhados sobre ataques cibernéticos, como realizar ataques ou sua descrição; e

- Estudos com foco central em vírus e malwares.

2.2 COLETA DE DADOS

Na sequência do aprofundamento teórico a respeito do assunto, o delineamento da pesquisa contemplou a coleta de dados pelos seguintes meios: entrevista exploratória, questionário e grupo focal.

2.2.1 Entrevistas

Com a finalidade de ampliar o conhecimento teórico do assunto e identificar experiências relevantes em cibernética, foram realizadas entrevistas exploratórias com os seguintes especialistas, em ordem cronológica de execução:

Nome	Justificativa
VINICIUS LUIS PALUDETO – Cap EB	Curso de Guerra Cibernética Instrutor do Curso de Guerra Cibernética
HUGO FARIA BRITO FRANCISQUINI – Cap EB	Curso de Guerra Cibernética Instrutor do Curso de Guerra Cibernética

QUADRO 1 – Quadro de Especialistas entrevistados
Fonte: O autor

2.2.2 Questionário

A amplitude do universo foi estimada a partir do efetivo de alunos que estão realizando o segundo ano do Curso de Formação e Graduação de Sargentos. O estudo foi limitado particularmente aos alunos da arma de comunicações, cursando na Escola de Sargentos das Armas, devido à sua formação mais completa e especialização em relação aos militares temporários.

A amostra selecionada para responder aos questionários também foi restrita a militares que são da Arma de Comunicações e que estão na Escola de Sargentos das Armas, excluindo-se os militares que são de Manutenção de Comunicações e que

realizam o curso na Escola de Sargentos de Logística, devido às características do combatente formado na ESA, servir em organizações militares de todas as armas e possuir maior acesso a equipamentos de tecnologia da informação.

Dessa forma, utilizando-se dados de quantidade de alunos informados pelo Curso de Comunicações da ESA, a população a ser estudada foi estimada em 145 militares. A fim de atingir uma maior confiabilidade das induções realizadas, buscou-se atingir uma amostra significativa, utilizando como parâmetros o nível de confiança igual a 95% e erro amostral de 1%. Nesse sentido, a amostra dimensionada como ideal (n_{ideal}) foi de 142.

Sendo assim, foram distribuídos questionários para os 145 alunos do Curso de Comunicações da ESA que serão formados conforme o PLADIS daquela Escola.

A sistemática de distribuição dos questionários ocorreu de forma indireta (formulário do Google) para 145 militares que atendiam os requisitos. Entretanto, devido a diversos fatores, foram obtidas 162 respostas (114,08% de n_{ideal}), havendo a necessidade de invalidar 17 respostas por preenchimento repetido do militar.

A partir do n_{ideal} (142), depreende-se que o tamanho amostral obtido (n=145) foi até superior ao desejado para o tamanho populacional dos integrantes da amostra, no entanto não inviabiliza, haja vista que todos responderam o questionário.

Foi realizado um pré-teste com 4 capitães-alunos da Escola de Aperfeiçoamento de Oficiais (EsAO), que possuíam o Curso de Guerra Cibernética, com a finalidade de identificar possíveis falhas no instrumento de coleta de dados. Ao final do pré-teste, não foram observados erros que justificassem alterações no questionário e, portanto, o mesmo foi enviado para os alunos da ESA.

2.2.3 Grupo Focal

Devido à natureza exploratória do assunto e finalizando a coleta de dados, foi conduzido um grupo focal, para debater os resultados colhidos nos questionários, com os seguintes especialistas:

Nome	Justificativa
LUIZ PAULO LOPES DOS SANTOS – Cap EB	Curso de Guerra Cibernética Instrutor da Escola de Comunicações
VINICIUS LUIS PALUDETO – Cap EB	Curso de Guerra Cibernética Instrutor do Curso de Guerra Cibernética
HUGO FARIA BRITO FRANCISQUINI – Cap EB	Curso de Guerra Cibernética Instrutor do Curso de Guerra Cibernética
MICHELL MEDEIROS SANTOS – Cap EB	Curso de Guerra Cibernética

QUADRO 2 – Quadro de Especialistas participantes do Grupo Focal
Fonte: O autor

Durante a condução do referido grupo focal, foram levantadas divergências entre o previsto em PLADIS, como Elemento de competência a ser alcançado pelos alunos do C Com da ESA e a percepção da amostra, obtida por intermédio dos questionários, notadamente nos seguintes aspectos:

a) Assuntos previstos para a disciplina cibernética que não condizem com o assunto;

b) Necessidade de melhor distribuir o tema cibernética pelo PLADIS do Curso de Comunicações da ESA;

c) Falta do assunto Proteção Cibernética no PLADIS do C Com da ESA; e

d) Desconhecimento das formas de proteção cibernética por parte dos alunos.

3 RESULTADOS E DISCUSSÃO

3.1 ANÁLISE DO PLADIS

Realizando a análise do PLADIS das Disciplinas Específicas da Arma de Comunicações do 2º Ano do Período de Qualificação do Curso de Formação e Graduação de Sargentos da Escola de Sargentos das Armas, foi possível observar que o assunto cibernética está presente em 3 disciplinas do PLADIS: Fundamentos das Comunicações (Figura 1), Emprego das Comunicações (Figura 2) e na disciplina Cibernética (Figura 3).

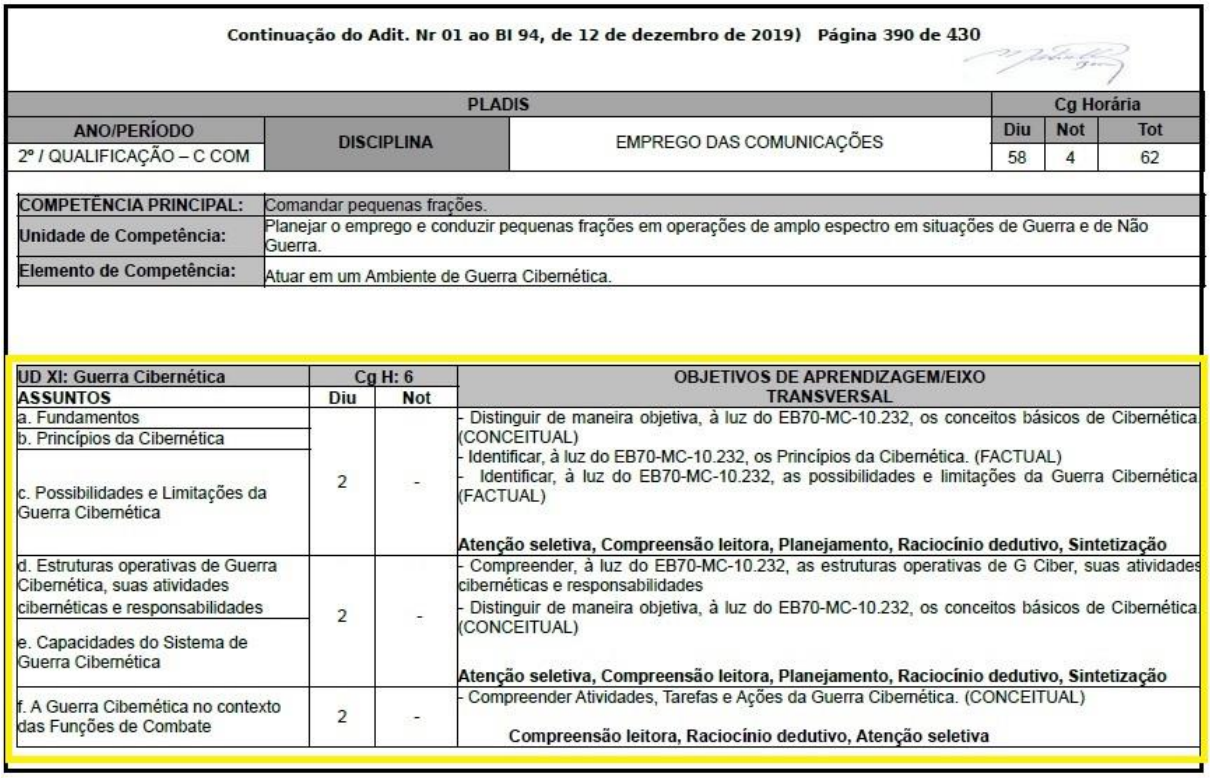
Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 371 de 430

PLADIS			Cg Horária		
ANO/PERÍODO	DISCIPLINA	FUNDAMENTOS DE COMUNICAÇÕES	Diu	Not	Tot
2º / QUALIFICAÇÃO – C COM			116	4	120

COMPETÊNCIA PRINCIPAL:	Comandar pequenas frações em operações no amplo espectro em situações de Guerra e de Não Guerra, integrando às funções de combate.
Unidade de Competência:	Atuar como chefe do grupo de Centro de Controle de Sistema, em uma Seção do Centro de Comunicações.
Elemento de Competência:	Instalar e operar material telefônico.

UD VIII: Sistemas militares de Comunicações	Cg H: 40		OBJETIVOS DE APRENDIZAGEM/EIXO TRANSVERSAL
ASSUNTOS	Diu	Not	
c. Sistema de Guerra Eletrônica do Exército Brasileiro	5	-	- Identificar a estrutura do sistema de GE do EB. (FACTUAL) **Compreensão, Raciocínio dedutivo, Atenção seletiva**
d. Sistema de Defesa Cibernética	5	-	- Identificar a estrutura e a atividade de defesa cibernética do EB. (FACTUAL) **Compreensão, Raciocínio dedutivo, Atenção seletiva**

FIGURA 1 - Pladis de Fundamentos das Comunicações
Fonte: DEFESA, 2019, p. 381



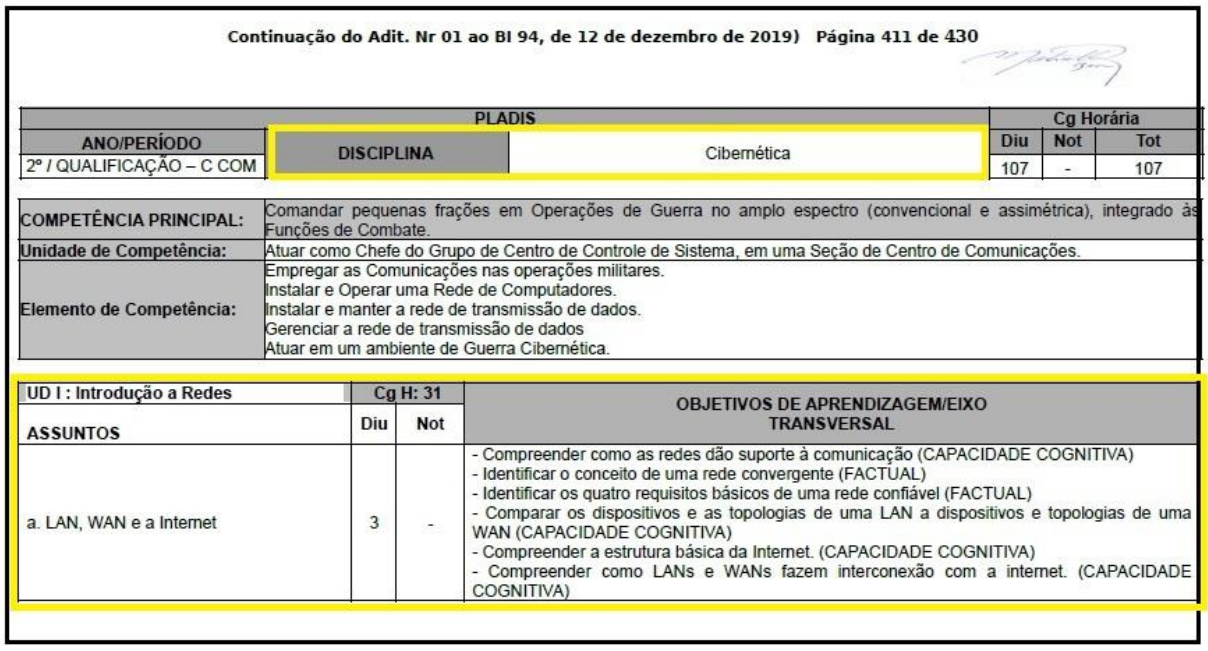
Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 390 de 430

PLADIS			Cg Horária		
ANO/PERÍODO	DISCIPLINA	EMPREGO DAS COMUNICAÇÕES	Diu	Not	Tot
2º / QUALIFICAÇÃO – C COM			58	4	62

COMPETÊNCIA PRINCIPAL:	Comandar pequenas frações.
Unidade de Competência:	Planejar o emprego e conduzir pequenas frações em operações de amplo espectro em situações de Guerra e de Não Guerra.
Elemento de Competência:	Atuar em um Ambiente de Guerra Cibernética.

UD XI: Guerra Cibernética	Cg H: 6		OBJETIVOS DE APRENDIZAGEM/EIXO TRANSVERSAL
ASSUNTOS	Diu	Not	
a. Fundamentos b. Princípios da Cibernética c. Possibilidades e Limitações da Guerra Cibernética	2	-	- Distinguir de maneira objetiva, à luz do EB70-MC-10.232, os conceitos básicos de Cibernética. (CONCEITUAL) - Identificar, à luz do EB70-MC-10.232, os Princípios da Cibernética. (FACTUAL) - Identificar, à luz do EB70-MC-10.232, as possibilidades e limitações da Guerra Cibernética (FACTUAL) **Atenção seletiva, Compreensão leitora, Planejamento, Raciocínio dedutivo, Sintetização**
d. Estruturas operativas de Guerra Cibernética, suas atividades cibernéticas e responsabilidades e. Capacidades do Sistema de Guerra Cibernética	2	-	- Compreender, à luz do EB70-MC-10.232, as estruturas operativas de G Ciber, suas atividades cibernéticas e responsabilidades - Distinguir de maneira objetiva, à luz do EB70-MC-10.232, os conceitos básicos de Cibernética. (CONCEITUAL) **Atenção seletiva, Compreensão leitora, Planejamento, Raciocínio dedutivo, Sintetização**
f. A Guerra Cibernética no contexto das Funções de Combate	2	-	- Compreender Atividades, Tarefas e Ações da Guerra Cibernética. (CONCEITUAL) **Compreensão leitora, Raciocínio dedutivo, Atenção seletiva**

FIGURA 2 - Pladis de Emprego das Comunicações
Fonte: DEFESA, 2019, p. 400 e 401



Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 411 de 430

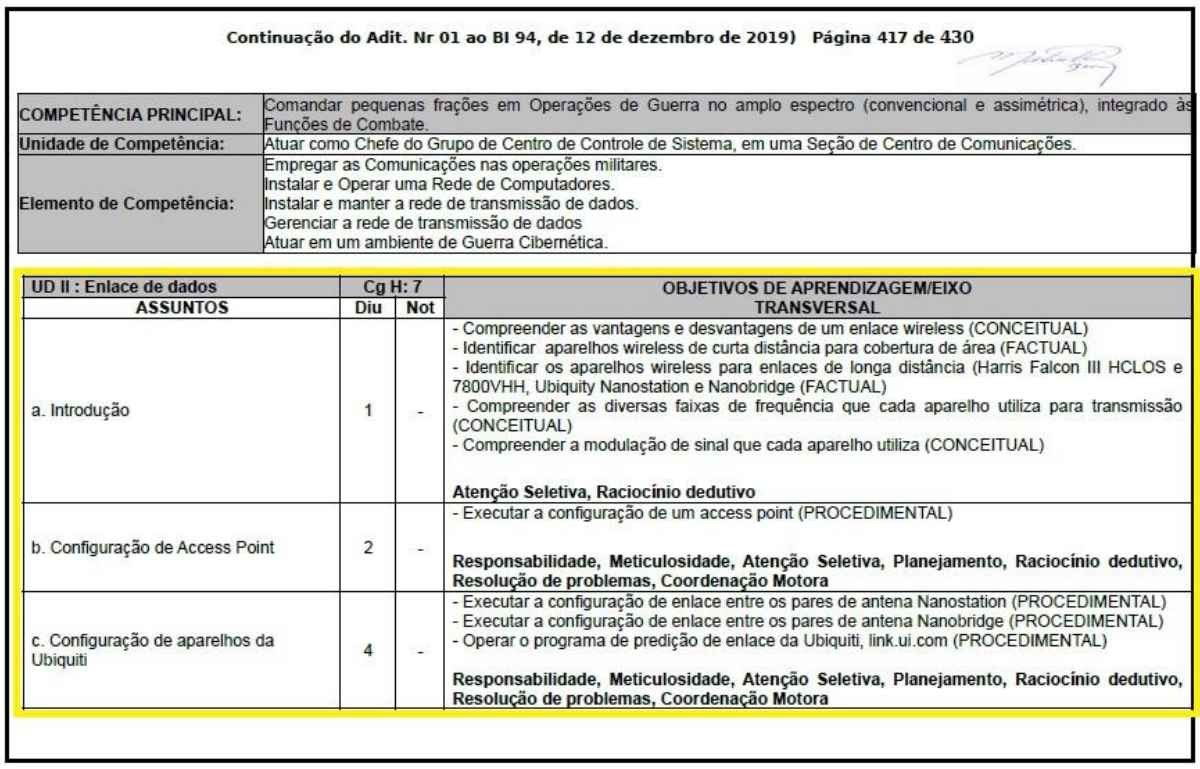
PLADIS			Cg Horária		
ANO/PERÍODO	DISCIPLINA	Cibernética	Diu	Not	Tot
2º / QUALIFICAÇÃO – C COM			107	-	107

COMPETÊNCIA PRINCIPAL:	Comandar pequenas frações em Operações de Guerra no amplo espectro (convencional e assimétrica), integrado às Funções de Combate.
Unidade de Competência:	Atuar como Chefe do Grupo de Centro de Controle de Sistema, em uma Seção de Centro de Comunicações.
Elemento de Competência:	Empregar as Comunicações nas operações militares. Instalar e Operar uma Rede de Computadores. Instalar e manter a rede de transmissão de dados. Gerenciar a rede de transmissão de dados Atuar em um ambiente de Guerra Cibernética.

UD I : Introdução a Redes	Cg H: 31		OBJETIVOS DE APRENDIZAGEM/EIXO TRANSVERSAL
ASSUNTOS	Diu	Not	
a. LAN, WAN e a Internet	3	-	- Compreender como as redes dão suporte à comunicação (CAPACIDADE COGNITIVA) - Identificar o conceito de uma rede convergente (FACTUAL) - Identificar os quatro requisitos básicos de uma rede confiável (FACTUAL) - Comparar os dispositivos e as topologias de uma LAN a dispositivos e topologias de uma WAN (CAPACIDADE COGNITIVA) - Compreender a estrutura básica da Internet. (CAPACIDADE COGNITIVA) - Compreender como LANs e WANs fazem interconexão com a internet. (CAPACIDADE COGNITIVA)

FIGURA 3 - Pladis de Cibernética
Fonte: DEFESA, 2019, p. 411

A partir disso, percebe-se que o assunto cibernética está bem explorado nas disciplinas Fundamentos das Comunicações (Figura 1) e Emprego das Comunicações (Figura 2), com objetivos condizentes com o tema. Porém, o mesmo não ocorre na disciplina Cibernética (Figura 3).



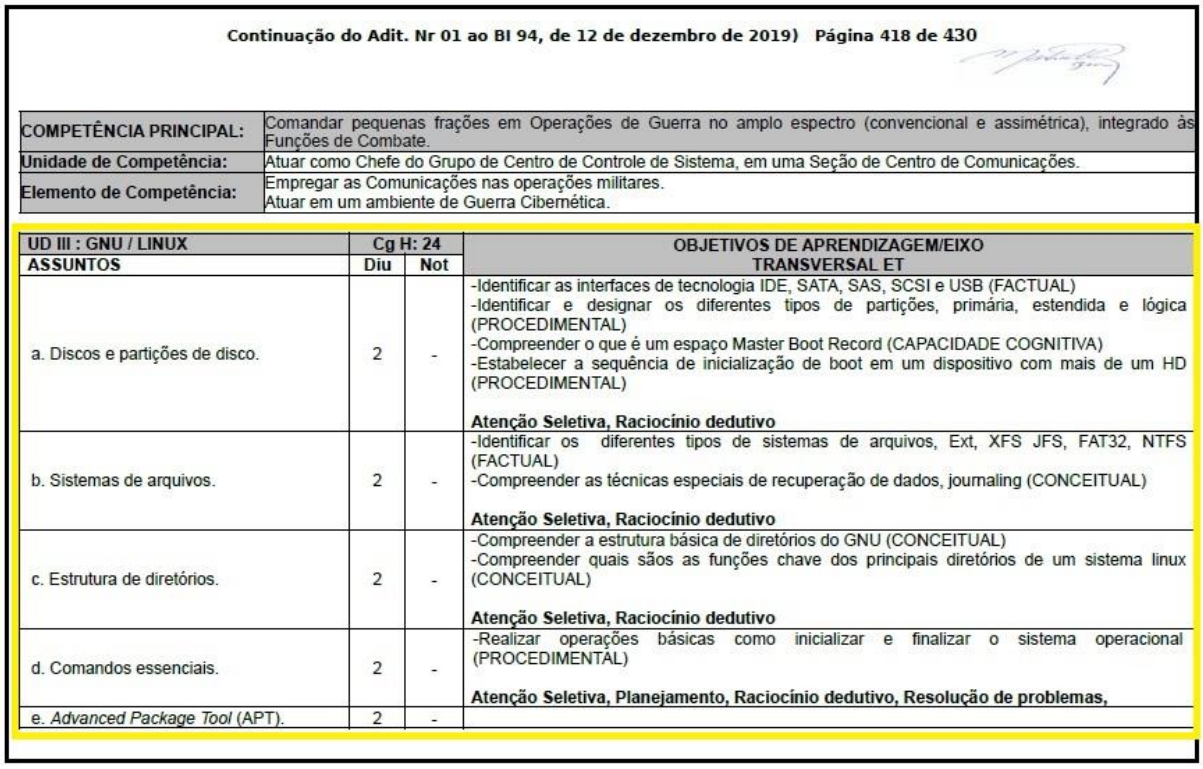
Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 417 de 430

COMPETÊNCIA PRINCIPAL:	Comandar pequenas frações em Operações de Guerra no amplo espectro (convencional e assimétrica), integrado às Funções de Combate.
Unidade de Competência:	Atuar como Chefe do Grupo de Centro de Controle de Sistema, em uma Seção de Centro de Comunicações.
Elemento de Competência:	Empregar as Comunicações nas operações militares. Instalar e Operar uma Rede de Computadores. Instalar e manter a rede de transmissão de dados. Gerenciar a rede de transmissão de dados Atuar em um ambiente de Guerra Cibernética.

UD II : Enlace de dados	**Cg H: 7**		**OBJETIVOS DE APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**Diu**	**Not**	
a. Introdução	1	-	- Compreender as vantagens e desvantagens de um enlace wireless (CONCEITUAL) - Identificar aparelhos wireless de curta distância para cobertura de área (FACTUAL) - Identificar os aparelhos wireless para enlaces de longa distância (Harris Falcon III HCLOS e 7800VHH, Ubiquity Nanostation e Nanobridge (FACTUAL) - Compreender as diversas faixas de frequência que cada aparelho utiliza para transmissão (CONCEITUAL) - Compreender a modulação de sinal que cada aparelho utiliza (CONCEITUAL) **Atenção Seletiva, Raciocínio dedutivo**
b. Configuração de Access Point	2	-	- Executar a configuração de um access point (PROCEDIMENTAL) **Responsabilidade, Meticulosidade, Atenção Seletiva, Planejamento, Raciocínio dedutivo, Resolução de problemas, Coordenação Motora**
c. Configuração de aparelhos da Ubiquiti	4	-	- Executar a configuração de enlace entre os pares de antena Nanostation (PROCEDIMENTAL) - Executar a configuração de enlace entre os pares de antena Nanobridge (PROCEDIMENTAL) - Operar o programa de predição de enlace da Ubiquiti, link.ui.com (PROCEDIMENTAL) **Responsabilidade, Meticulosidade, Atenção Seletiva, Planejamento, Raciocínio dedutivo, Resolução de problemas, Coordenação Motora**

FIGURA 4 - Pladis de Cibernética
Fonte: DEFESA, 2019, p. 417

Ao contrário do que se esperava, a disciplina Cibernética contempla muito sobre os assuntos introdução a redes (Figura 3), enlace de dados (Figura 4), Linux (Figura 5) e Servidores Linux (Figura 6), e nada sobre o assunto cibernética. Inclusive os Elementos de Competência presentes na disciplina Cibernética praticamente não contemplam objetivos desta disciplina. Sendo assim, pode-se concluir que o assunto Cibernética não é bem explorado no PLADIS da disciplina Cibernética.



Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 418 de 430

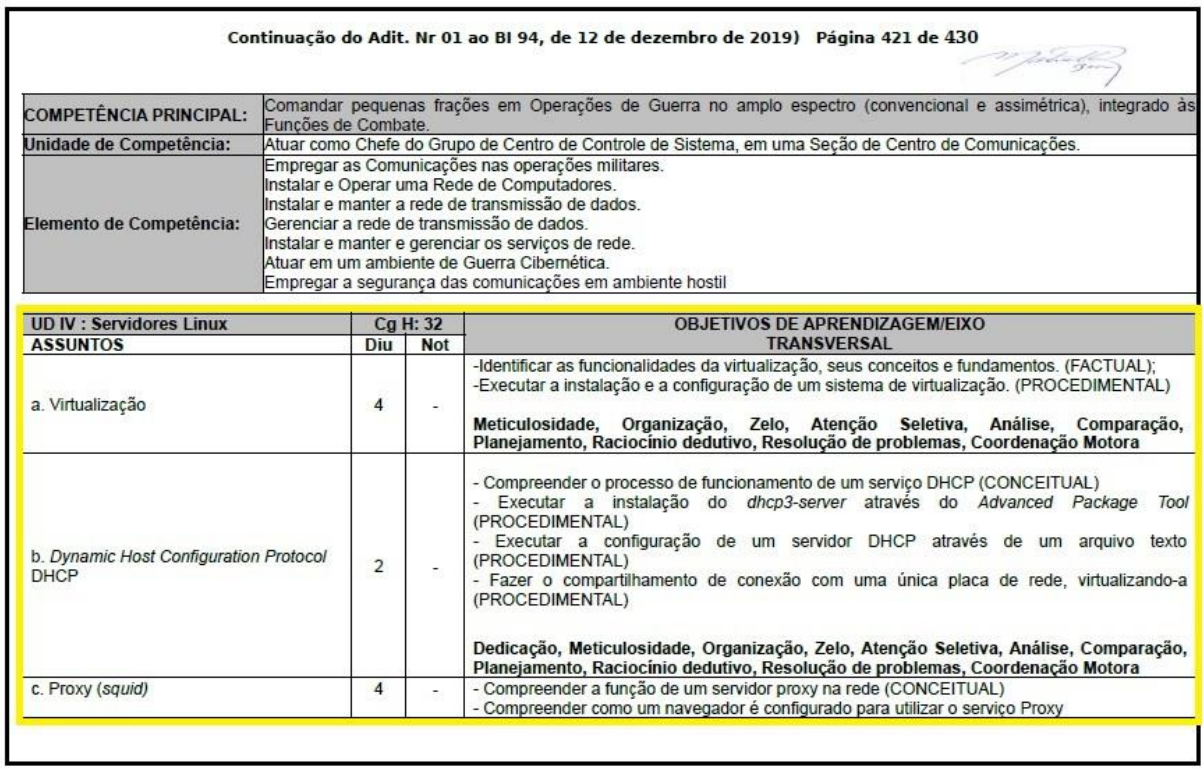
COMPETÊNCIA PRINCIPAL:	Comandar pequenas frações em Operações de Guerra no amplo espectro (convencional e assimétrica), integrado às Funções de Combate.
Unidade de Competência:	Atuar como Chefe do Grupo de Centro de Controle de Sistema, em uma Seção de Centro de Comunicações.
Elemento de Competência:	Empregar as Comunicações nas operações militares. Atuar em um ambiente de Guerra Cibernética.

UD III : GNU / LINUX	**Cg H: 24**		**OBJETIVOS DE APRENDIZAGEM/EIXO TRANSVERSAL ET**
ASSUNTOS	**Diu**	**Not**	
a. Discos e partições de disco.	2	-	-Identificar as interfaces de tecnologia IDE, SATA, SAS, SCSI e USB (FACTUAL) -Identificar e designar os diferentes tipos de partições, primária, estendida e lógica (PROCEDIMENTAL) -Compreender o que é um espaço Master Boot Record (CAPACIDADE COGNITIVA) -Estabelecer a sequência de inicialização de boot em um dispositivo com mais de um HD (PROCEDIMENTAL) **Atenção Seletiva, Raciocínio dedutivo**
b. Sistemas de arquivos.	2	-	-Identificar os diferentes tipos de sistemas de arquivos, Ext, XFS JFS, FAT32, NTFS (FACTUAL) -Compreender as técnicas especiais de recuperação de dados, journaling (CONCEITUAL) **Atenção Seletiva, Raciocínio dedutivo**
c. Estrutura de diretórios.	2	-	-Compreender a estrutura básica de diretórios do GNU (CONCEITUAL) -Compreender quais sãos as funções chave dos principais diretórios de um sistema linux (CONCEITUAL) **Atenção Seletiva, Raciocínio dedutivo**
d. Comandos essenciais.	2	-	-Realizar operações básicas como inicializar e finalizar o sistema operacional (PROCEDIMENTAL) **Atenção Seletiva, Planejamento, Raciocínio dedutivo, Resolução de problemas,**
e. *Advanced Package Tool* (APT).	2	-	

FIGURA 5 - Pladis de Cibernética
Fonte: DEFESA, 2019, p. 418

Como sugestão, decorrente da análise realizada sobre os Planos de Disciplinas do Curso de Comunicações da ESA, poderia ser criada a disciplina Redes, a qual contemplaria o atual conteúdo da disciplina Cibernética. Já a disciplina Cibernética seria composta dos assuntos selecionados nas Figuras 1 (Fundamentos das Comunicações) e Figura 2 (Emprego das Comunicações), acrescentado do assunto Proteção Cibernética, que poderia ser ensinado de forma presencial na ESA.

Atualmente, o assunto Proteção Cibernética está previsto como Atividade de Complementação de Ensino da disciplina Emprego das Comunicações (Figura 7), sendo o conteúdo ministrado pela Escola de Comunicações (EsCom) durante o Pedido de Cooperação de Instrução (PCI) realizado em Brasília-DF.



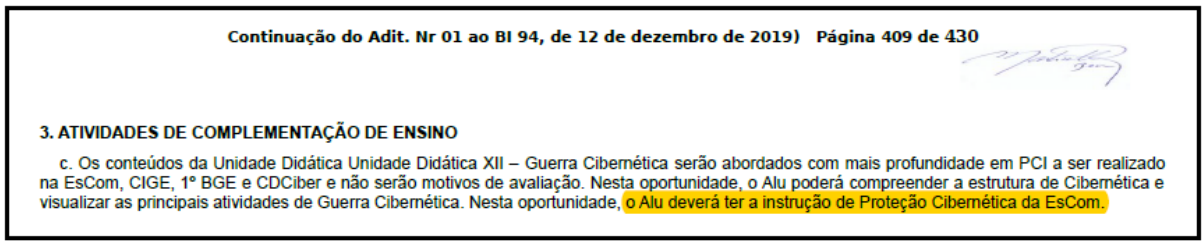
Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 421 de 430

COMPETÊNCIA PRINCIPAL:	Comandar pequenas frações em Operações de Guerra no amplo espectro (convencional e assimétrica), integrado às Funções de Combate.
Unidade de Competência:	Atuar como Chefe do Grupo de Centro de Controle de Sistema, em uma Seção de Centro de Comunicações.
Elemento de Competência:	Empregar as Comunicações nas operações militares. Instalar e Operar uma Rede de Computadores. Instalar e manter a rede de transmissão de dados. Gerenciar a rede de transmissão de dados. Instalar e manter e gerenciar os serviços de rede. Atuar em um ambiente de Guerra Cibernética. Empregar a segurança das comunicações em ambiente hostil

UD IV : Servidores Linux	Cg H: 32		OBJETIVOS DE APRENDIZAGEM/EIXO TRANSVERSAL
ASSUNTOS	**Diu**	**Not**	
a. Virtualização	4	-	-Identificar as funcionalidades da virtualização, seus conceitos e fundamentos. (FACTUAL); -Executar a instalação e a configuração de um sistema de virtualização. (PROCEDIMENTAL) **Meticulosidade, Organização, Zelo, Atenção Seletiva, Análise, Comparação, Planejamento, Raciocínio dedutivo, Resolução de problemas, Coordenação Motora**
b. *Dynamic Host Configuration Protocol* DHCP	2	-	- Compreender o processo de funcionamento de um serviço DHCP (CONCEITUAL) - Executar a instalação do *dhcp3-server* através do *Advanced Package Tool* (PROCEDIMENTAL) - Executar a configuração de um servidor DHCP através de um arquivo texto (PROCEDIMENTAL) - Fazer o compartilhamento de conexão com uma única placa de rede, virtualizando-a (PROCEDIMENTAL) **Dedicação, Meticulosidade, Organização, Zelo, Atenção Seletiva, Análise, Comparação, Planejamento, Raciocínio dedutivo, Resolução de problemas, Coordenação Motora**
c. Proxy (*squid)*	4	-	- Compreender a função de um servidor proxy na rede (CONCEITUAL) - Compreender como um navegador é configurado para utilizar o serviço Proxy

FIGURA 6 - Pladis de Cibernética
Fonte: DEFESA, 2019, p. 421

Ainda sobre o assunto Proteção Cibernética, ele também está previsto como Atividade de Complementação de Ensino da disciplina Cibernética (Figura 8), porém como matéria optativa no Estágio de Proteção Cibernética, também ministrado pela Escola de Comunicações (EsCom).

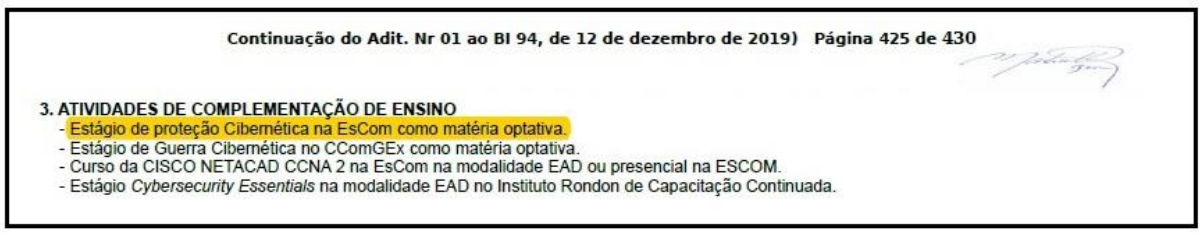


Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 409 de 430

3. ATIVIDADES DE COMPLEMENTAÇÃO DE ENSINO

c. Os conteúdos da Unidade Didática Unidade Didática XII – Guerra Cibernética serão abordados com mais profundidade em PCI a ser realizado na EsCom, CIGE, 1º BGE e CDCiber e não serão motivos de avaliação. Nesta oportunidade, o Alu poderá compreender a estrutura de Cibernética e visualizar as principais atividades de Guerra Cibernética. Nesta oportunidade, o Alu deverá ter a instrução de Proteção Cibernética da EsCom.

FIGURA 7 - Pladis de Emprego das Comunicações
Fonte: DEFESA, 2019, p. 409



Continuação do Adit. Nr 01 ao BI 94, de 12 de dezembro de 2019) Página 425 de 430

3. ATIVIDADES DE COMPLEMENTAÇÃO DE ENSINO

- Estágio de proteção Cibernética na EsCom como matéria optativa.
- Estágio de Guerra Cibernética no CComGEx como matéria optativa.
- Curso da CISCO NETACAD CCNA 2 na EsCom na modalidade EAD ou presencial na ESCOM.
- Estágio *Cybersecurity Essentials* na modalidade EAD no Instituto Rondon de Capacitação Continuada.

FIGURA 8 - Pladis de Cibernética
Fonte: DEFESA, 2019, p. 425

3.2 RESULTADOS OBTIDOS E DISCUSSÃO

Após a análise do PLADIS das Disciplinas Específicas da Arma de Comunicações, foi realizado um questionário com os 145 alunos do 2º ano do CFGS de Comunicações. Na pergunta inicial, foi perguntado se o militar tinha conhecimento de algum ataque cibernético ocorrido, como demonstrado no gráfico 2.

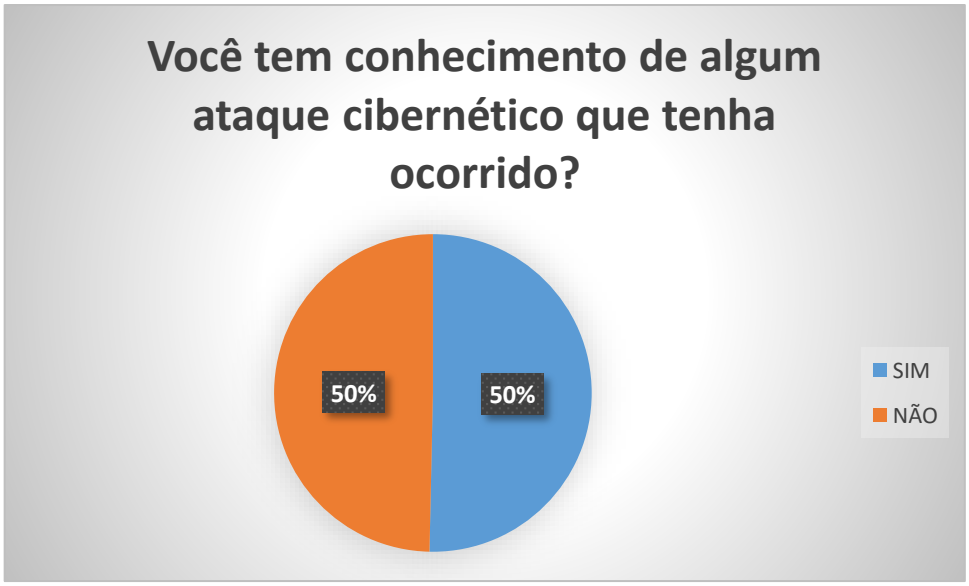


GRÁFICO 2 – Conhecimento de ataques cibernéticos
Fonte: O autor

A partir dos resultados obtidos, percebe-se que o assunto cibernética possui conhecimento parcial por parte dos alunos do curso de comunicações. Já na pergunta seguinte, foi questionado sobre o dispositivo usado para acesso à internet, conforme observado no gráfico 3.

GRÁFICO 3 – Dispositivo usado para acesso à internet
Fonte: O autor

No gráfico 3, observa-se que a grande maioria dos alunos (70%) acessa à internet através de dispositivos como celular e computador. Na pergunta seguinte, foi questionado aos alunos sobre qual o tipo de conexão para realizar o acesso à internet, conforme o gráfico 4.

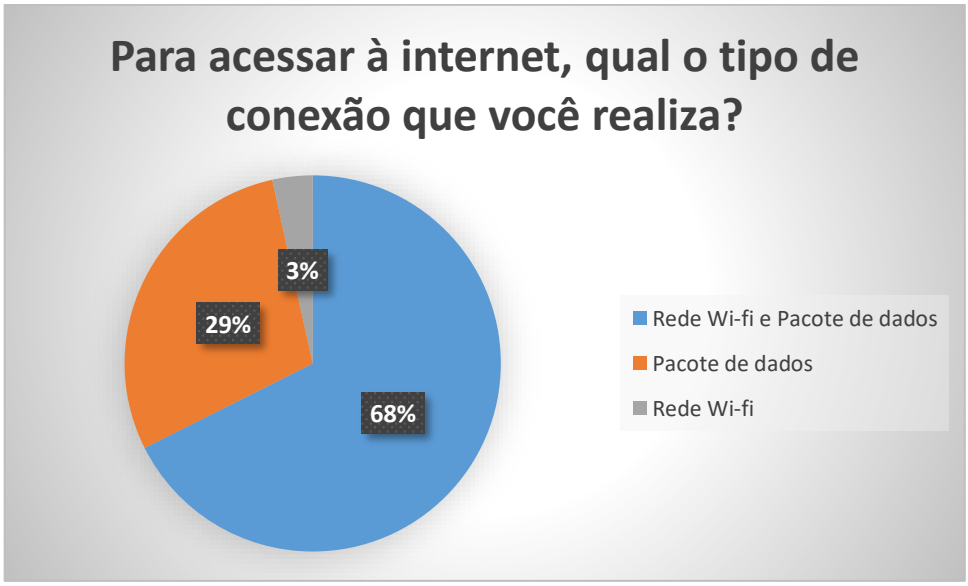


GRÁFICO 4 – Tipos de conexão
Fonte: O autor

Neste questionamento, observa-se que grande parte dos alunos (68%) utiliza a rede wi-fi da ESA e o pacote de dados do celular para acesso à internet. O restante dos alunos utiliza somente o pacote de dados (29%) ou somente a rede wi-fi (3%). Já o próximo questionamento foi sobre o recebimento de fake News, conforme demonstrado no gráfico 5.

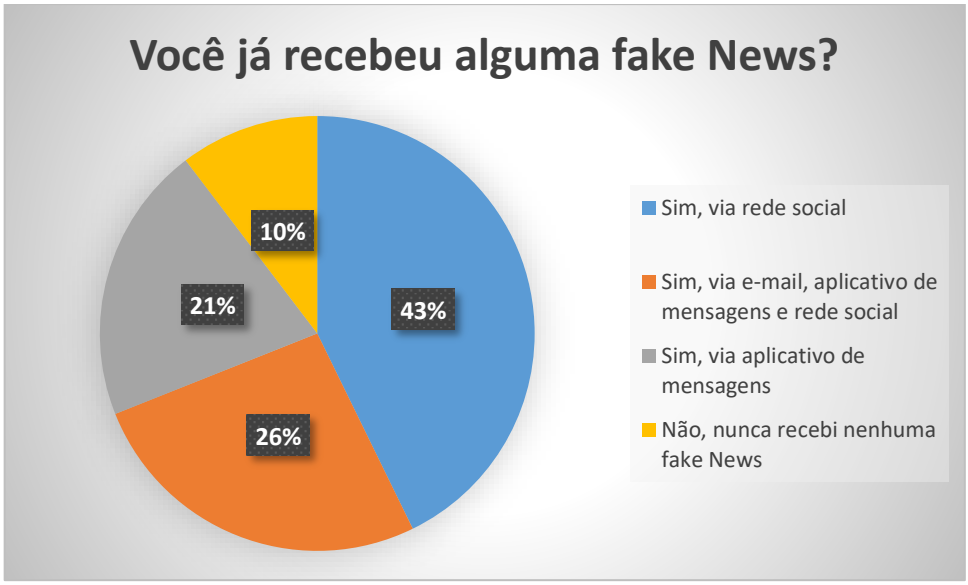


GRÁFICO 5 – Recebimento de fake News
Fonte: O autor

Nesta pergunta, observa-se que 90% dos alunos já recebeu algum tipo de fake News, seja via rede social, e-mail ou aplicativo de mensagens. Apenas 10% nunca se depararam com essa situação. Na pergunta seguinte, foi questionado sobre o tipo de senha que cada aluno utiliza para cadastro em sites, conforme gráfico 6.

GRÁFICO 6 – Senha cadastrada
Fonte: O autor

Nesse caso, obteve-se como resposta que a grande maioria dos alunos (66%) utiliza senhas diferentes para cadastro em diferentes sites. O restante dos alunos utiliza a mesma senha em todos os sites. Na próxima pergunta realizada, foi questionado sobre o tipo de senha normalmente utilizado para cadastro, conforme apresentado no gráfico 7.

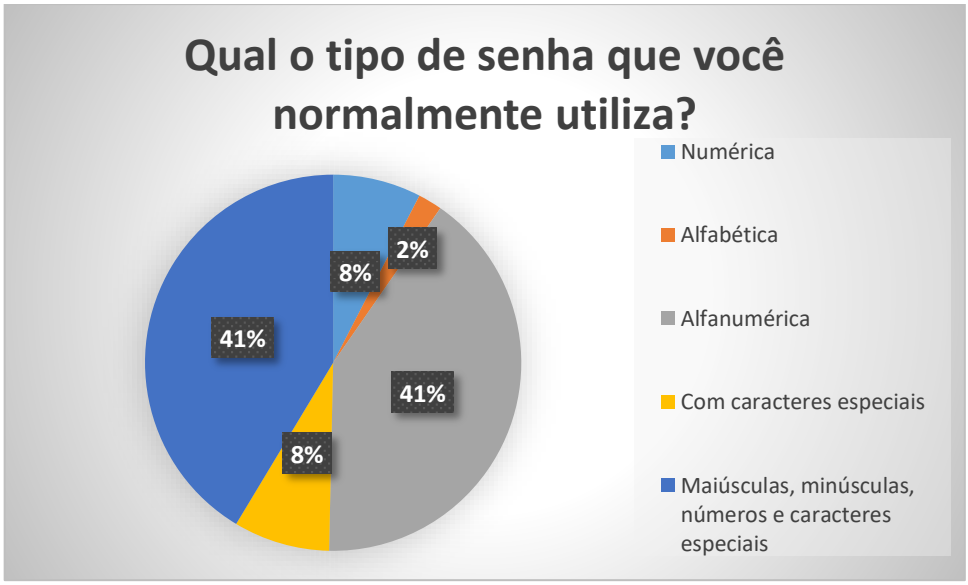


GRÁFICO 7 – Tipo de senha
Fonte: O autor

Já neste questionamento, 82% dos alunos utilizam senhas alfanuméricas ou com maiúsculas, minúsculas, números e caracteres especiais. Os demais alunos utilizam senhas numéricas, alfabéticas ou com caracteres especiais. Na pergunta seguinte os alunos foram questionados se costumam realizar backup de seus dados pessoais, conforme o gráfico 8.

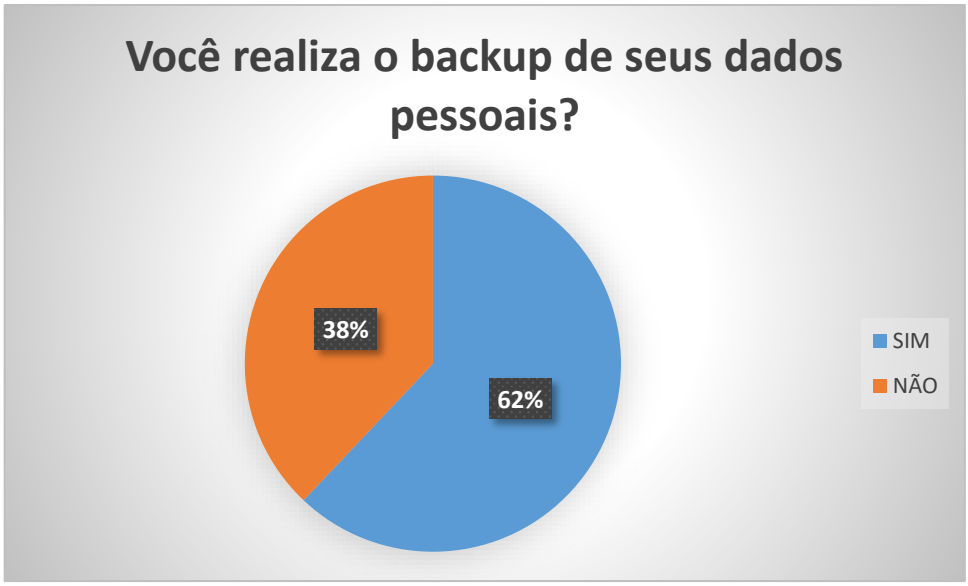


GRÁFICO 8 – Backup de dados pessoais
Fonte: O autor

Em relação ao backup de seus dados pessoais, 62% possuem essa prática regular, os demais alunos não. Na pergunta seguinte, os alunos foram questionados sobre a necessidade de mais tempo abordando o assunto Segurança e Proteção Cibernética, conforme demonstrado no gráfico 9.

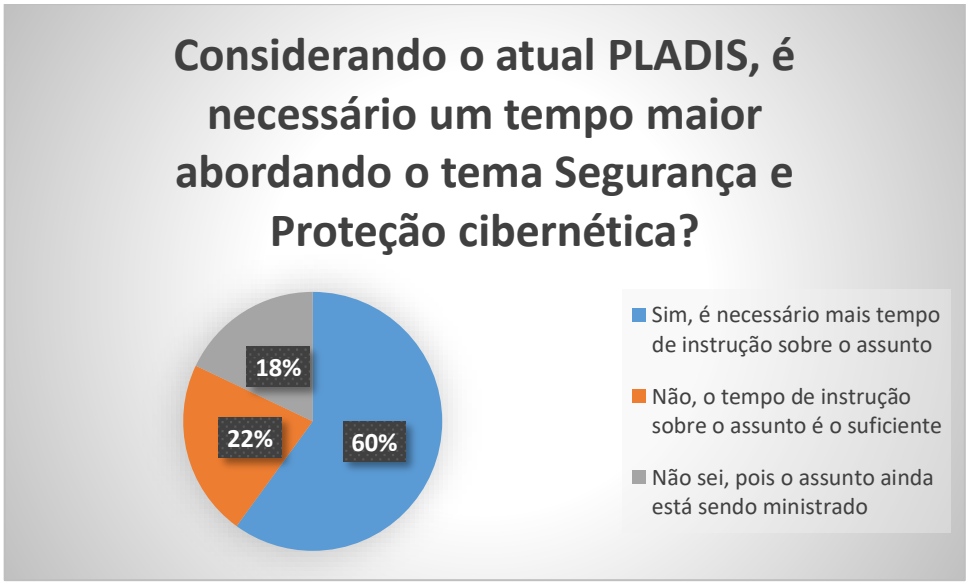


GRÁFICO 9 – Necessidade de mais tempo para Segurança e Proteção cibernética
Fonte: O autor

Quanto ao questionamento do Pladis e a necessidade de maior tempo abordando o assunto Segurança e Proteção cibernética, 60% consideram que é necessário mais tempo de instrução sobre o assunto, 22% acham que o tempo de instrução é o suficiente e os outros 18% acreditam que o conteúdo ainda está sendo ministrado.

Por fim, foi disponibilizado um espaço para considerações sobre a pesquisa, no qual surgiram vários comentários, dos quais ressaltam-se os seguintes:

a) “Maior tempo para instrução de cibernética.”;

b) “O conhecimento sobre segurança da informação é importante na vida do terceiro sargento comunicante do Exército Brasileiro.”;

c) “Na parte nas instruções, seria bom se tivesse instruções práticas em consonância com as teóricas.”;

d) “O cenário cibernético no mundo inteiro vem crescendo, é de vital importância que o sargento de comunicações tenha conhecimento dos assuntos mais abordados nesse contexto cibernético.”; e

e) “Acredito na importância do foco em cibernética para os próximos anos.”.

Diante do questionário realizado, observa-se que os alunos já possuem um conhecimento adquirido referente ao assunto cibernética, conforme pode ser visto nos gráficos 6, 7 e 8, nos quais a maioria dos alunos demonstram utilizar de boas práticas de Segurança e proteção cibernética.

Porém, conforme observado no gráfico 9 e nas considerações dos alunos sobre a pesquisa, ainda é necessário mais tempo em Pladis voltado para a Cibernética, principalmente quanto à Segurança e Proteção Cibernética, com preferência para instruções práticas abordando o tema.

4 CONSIDERAÇÕES FINAIS

Em relação aos objetivos propostos no início deste trabalho, conclui-se que a presente pesquisa atendeu ao pretendido, inclusive trazendo a opinião dos alunos do Curso de Formação e Graduação de Sargentos 2019/2020 acerca da temática de Segurança e Proteção Cibernética na formação do sargento combatente de Comunicações.

Este artigo científico identificou que o sargento de Comunicações formado pela ESA apresenta relativo conhecimento sobre segurança e proteção cibernética, visto que parte dos alunos já realizam algumas boas práticas nessa área, conforme

observado no questionário aplicado, representado através dos gráficos.

Porém, esse conhecimento de segurança e proteção cibernética poderia ser maior, caso o Pladis estivesse melhor estruturado. No item 3 (Resultados e Discussões), foi apresentado o Pladis do Curso de Comunicações e os locais nos quais o assunto cibernética era abordado, sendo identificado oportunidades de melhoria na estruturação do assunto, resultando em uma sugestão de alteração no Pladis do curso.

Ainda sobre o Pladis do C Com, foi observado também, que o assunto segurança e proteção cibernética seria ministrado apenas no PCI em Brasília, através de instruções teóricas e práticas realizadas na EsCom. Entretanto, devido à grande relevância do assunto para a carreira do praça, e consequentemente para o EB, seria interessante que o assunto fosse ministrado na própria ESA, haja vista que, caso o PCI não seja realizado (como ocorreu este ano por conta do COVI-19) o aluno não tenha sua formação prejudicada pela falta do conhecimento nessa área.

Sendo assim, após realizada a análise do Pladis, foi apresentado o resultado do questionário aplicado aos alunos do CFGS 2019/2020, ferramenta esta que auxiliou na busca do objetivo geral deste artigo científico, pois o sargento é aquele que opera grande parte dos meios informatizados do EB, ou seja, é essencial que ele detenha os conhecimentos de segurança e proteção cibernética desde a escola de formação.

A revisão de literatura possibilitou concluir que a segurança e proteção cibernética é importante não apenas para o Exército Brasileiro, mas também é essencial para as demais instituições, visto que um ataque cibernético pode trazer muitos prejuízos financeiros para as empresas.

Dessa forma, conclui-se que o Plano de disciplina, utilizado pelo curso de Comunicações da ESA, tem sido muito útil na formação do sargento, haja vista os resultados apresentados no questionário, nos quais foi apresentado um considerável conhecimento na área de segurança e proteção cibernética. Porém, na incessante busca pela excelência na formação dos recursos humanos do EB, é recomendável algumas alterações no Pladis, conforme apresentado neste artigo científico. Dessa maneira, as organizações militares receberão sargentos com os conhecimentos mais atuais na área de cibernética.

REFERÊNCIAS

BRASIL. Ministério da Defesa. **MD31-M-07 – Doutrina Militar de Defesa Cibernética**. Brasília, 2014.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2008.

CERT.Br. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 5 ago 2020.

CONCEIÇÃO, Marcelo Eduardo de Souza. **Ataques cibernéticos perpetrados na atualidade e os possíveis impactos para as OM do Exército Brasileiro**. Escola de Aperfeiçoamento de Oficiais, EsAO, Rio de Janeiro, 2017.

DAMIAO, André Kohler. **Guerra cibernética: proteção cibernética monitoramento de redes e sistemas e levantamentos de vulnerabilidades**. Escola de Aperfeiçoamento de Oficiais, EsAO, Rio de Janeiro, 2018.

FREITAS, Eduardo Antônio Mello. **Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação**. 2009. 71 p. Monografia, Curso de Pós-graduação “Lato Sensu” em Gestão Estratégica e Qualidade, Universidade Cândido Mendes, Brasília, DF, 2009. Disponível em: <https://bd.camara.leg.br/bd/bitstream/handle/bdcamara/3564/gestao_riscos_freitas.pdf?sequence=2&isAllowed=y>. Acesso em: 21 abr. 2020.

MITSHASHI, Roberto Akio. **Segurança de Redes**. 2011. 54 f. Trabalho de Conclusão de Curso (Tecnólogo em Processamento de Dados) - Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes:** em ambientes cooperativos. São Paulo: Novatec, 2007. 488 p.

PEREIRA, Guilherme da Silva. **Firewall GNU/LINUX e iptables: um estudo de implementação de ensino no plano de disciplina da formação do oficial de carreira de comunicações**. Academia Militar das Agulhas Negras, AMAN, Resende, 2019.

SENADO, Agência. **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>. Acesso em: 24 abr 2020.

SILVA, Endrew Irineu Santos. **Segurança e defesa cibernética: levantar aspectos de política e segurança aplicáveis ao contexto de um batalhão de infantaria**. Academia Militar das Agulhas Negras, AMAN, Resende, 2019.

	ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS **SEÇÃO DE PÓS-GRADUAÇÃO**

QUESTIONÁRIO

O presente instrumento é parte integrante da especialização em Ciências Militares do Cap Com André de Jesus Porto, cujo tema é **Segurança e Proteção cibernética na formação do sargento combatente de Comunicações**. Pretende-se, através da compilação dos dados coletados, demonstrar a importância do assunto cibernética ministrado na formação do sargento de Comunicações para a segurança cibernética do Exército Brasileiro (EB).

A fim de conhecer as necessidades no ensino dos militares, o senhor foi selecionado, dentro de um amplo universo, para responder as perguntas deste questionário. Solicito-vos a gentileza de respondê-lo o mais completamente possível.

Dessa forma, esse questionário auxiliará na resolução do seguinte problema: O ensino de Segurança e Proteção Cibernética na formação do sargento combatente de Comunicações é o suficiente para que possam atuar em suas Organizações Militares na implementação de medidas de segurança e proteção cibernética, durante as atividades diárias nas respectivas OM?

A experiência profissional do senhor irá contribuir sobremaneira para a pesquisa, colaborando nos estudos referentes à mentalidade de segurança e proteção cibernética que deverá ser utilizada nas organizações militares do EB. Será muito importante, ainda, que o senhor complemente, quando assim o desejar, suas opiniões a respeito do tema e do problema.

Desde já agradeço a colaboração e coloco-me à disposição para esclarecimentos através dos seguintes contatos:

André de Jesus Porto (Capitão de Comunicações – AMAN 2011)

Celular: (55) 99629-0629

E-mail: andrejporto@hotmail.com

IDENTIFICAÇÃO

1. Qual é seu nome de guerra?

_____

ASPECTOS DE CIBERNÉTICA

2. Com o crescimento do avanço tecnológico, tem crescido também os ataques cibernéticos. Você tem conhecimento de algum ataque cibernético que tenha ocorrido?

( ) Sim

( ) Não

3. A crescente quantidade de dispositivos interconectados, como celulares, câmeras de segurança, computadores e carros, resultou em um aumento da quantidade de pontos de entrada para atacantes cibernéticos. Qual o dispositivo que você usa para acessar à internet?

( ) Celular

( ) Computador

( ) Celular e computador

( ) Outros

( ) Não tenho acesso à internet

4. Para acessar à internet, qual o tipo de conexão que você realiza?

( ) Rede Wi-fi disponibilizada pela ESA

( ) Pacote de dados

( ) Rede Wi-fi e Pacote de dados

( ) Não tenho acesso à internet

5. O Covid-19 transformou a vida das pessoas ao redor do mundo. Além dos cuidados relacionados à saúde, é importante ter cuidado com os golpes cibernéticos. Com a crescente quantidade de notícias sobre o assunto, os fraudadores digitais se aproveitam da situação utilizando-se de fake News para roubar informações pessoais. Você já recebeu alguma fake News?

( ) Sim, via e-mail

( ) Sim, via aplicativo de mensagens

( ) Sim, via rede social

( ) Sim, via e-mail, aplicativo de mensagens e rede social

( ) Não, nunca recebi nenhuma fake News

6. Durante a navegação na internet, muitos sites solicitam um cadastro para acesso a algum conteúdo específico ou para que alguma compra seja realizada. Sobre a senha cadastrada em sites diversos, você utiliza:
( ) A mesma senha em todos os sites
( ) Todas as senhas diferentes, uma para cada site

7. Para navegar com segurança na internet e evitar que sua conta seja invadida, é importante escolher uma boa senha. Qual o tipo de senha que você normalmente utiliza?
( ) Numérica
( ) Alfabética
( ) Alfanumérica
( ) Com caracteres especiais
( ) Maiúsculas, minúsculas, números e caracteres especiais

8. Em sua busca para obter informações pessoais dos usuários, hackers usam estratégias de engenharia social para fazer os usuários caírem em armadilhas, sendo assim é importante manter backup regular. Você realiza o backup de seus dados pessoais?

   ( ) Sim

   ( ) Não

ANÁLISE DO PLADIS

9. Considerando o atual Plano de Disciplina (PLADIS) e os assuntos ministrados durante o ano de instrução no Curso de Comunicações, é necessário um tempo maior abordando o tema Segurança e Proteção cibernética?

   ( ) Sim, é necessário mais tempo de instrução sobre o assunto

   ( ) Não, o tempo de instrução sobre o assunto é o suficiente
   ( ) Não sei, pois o assunto ainda está sendo ministrado
   ( ) Não sei, pois o assunto ainda não foi ministrado

FECHAMENTO

10. Você gostaria de acrescentar alguma consideração sobre a presente pesquisa?

_____

_____

_____

Obrigado pela participação.