ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP ENG ATILLA RODRIGO PEREIRA SILVA

O PREPARO DE RECURSOS HUMANOS NO CONTEXTO DA GUERRA CIBERNÉTICA: UMA ANÁLISE DA FORMAÇÃO DO SOLDADO DO EFETIVO VARIÁVEL NO CENÁRIO DA PROTEÇÃO DIGITAL

Rio de Janeiro

2022

CAP ENG ATILLA RODRIGO PEREIRA SILVA

O PREPARO DE RECURSOS HUMANOS NO CONTEXTO DA GUERRA CIBERNÉTICA: UMA ANÁLISE DA FORMAÇÃO DO SOLDADO DO EFETIVO VARIÁVEL NO CENÁRIO DA PROTEÇÃO DIGITAL

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção do grau especialização em Ciências Militares

Orientador: Maj Eng Tomás Martins Pereira Bastos.

Rio de Janeiro

2022

Ficha catalográfica elaborada pelo Bibliotecário Francisco José de Paula Junior
CRB7/6686

S5861

Silva, Atilla Rodrigo Pereira.

O preparo de recursos humanos no contexto da guerra cibernética: uma análise da formação do soldado do efetivo variável no cenário da proteção digital / Atilla Rodrigo Pereira Silva – 2022.

49 f. : il.

Trabalho de Conclusão de Curso – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2022.

Orientação: Maj. Tomás Martins Pereira Bastos.

1. Cibernética. 2. Proteção digital. 3. Programa-padrão I Escola de Aperfeiçoamento de Oficiais. II Título.

CDD: 355

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

DIVISÃO DE ENSINO E PESQUISA/ CURSO DE ENGENHARIA

Ao Cap Eng **ATILLA** RODRIGO PEREIRA **SILVA**

O Presidente da Comissão de Avaliação do TCC, cujo título é O Preparo de Recursos Humanos no Contexto da Guerra Cibernética: uma análise da formação do soldado do efetivo variável no cenário da proteção digital, informa à Vossa Senhoria o seguinte resultado da deliberação: **APROVADO** com o conceito **BOM.**

Rio de Janeiro, 20 de setembro de 2022.

Tomás Martins Pereira Bastos – Maj
Presidente

Douglas Teixeira Araújo– Cap
1º Membro

Lucas Carvalho da Silva – Cap
2º Membro

CIENTE: _____
Atilla Rodrigo Pereira Silva - Cap
Postulante

RESUMO

Nos últimos anos, fruto do desenvolvimento tecnológico, a cibernética tornou-se uma das principais ferramentas de auxílio na elaboração e gerenciamento das atividades desenvolvidas nos quartéis do Exército Brasileiro. Todavia, tal avanço gera preocupações em relação à capacitação atual dos militares para utilizar, de forma segura, esse instrumento. Com a finalidade de analisar a atual preparação dos soldados recém – ingressos na Força Terrestre sobre o assunto, será realizado um estudo sobre o Programa - Padrão de Instrução Individual Básica, buscando identificar se existe a necessidade de atualização do documento, com a inclusão de assuntos sobre a proteção digital. A pesquisa será baseada em referências bibliográficas que abordam o tema, tanto nacionais como de nações amigas.

Palavras-chave: Cibernética. Programa - Padrão.

RESUMEN

En los últimos años, como resultado del desarrollo tecnológico, la cibernética se ha convertido en una de las principales herramientas de ayuda en la elaboración y gestión de las actividades realizadas en los acuartelamientos del Ejército Brasileño. Sin embargo, tal progreso plantea preocupaciones con respecto al entrenamiento actual de los militares para usar este instrumento de manera segura. Con la finalidad de analizar la preparación actual de los soldados que se incorporaron recientemente a la Fuerza Terrestre en el tema, se realizará un estudio sobre el Programa – Patrón Básico de Instrucción Individual, buscando identificar si existe la necesidad de actualizar el documento, con la inclusión de temas sobre protección digital. La investigación se basará en referencias bibliográficas que aborden el tema, tanto nacionales como de naciones amigas.

Palabras clave: Cibernética. Programa – Patrón.

SUMÁRIO

SUMÁRIO

1. INTRODUÇÃO

A utilização da internet, durante os últimos dez anos, tornou-se algo indispensável para o indivíduo. Através da digitalização, processos sociais e profissionais foram simplificados e, cada vez, mais presentes no cotidiano dos seres humanos.

Concomitantemente, o avanço tecnológico também está ocorrendo diariamente nas unidades do Exército Brasileiro, o que está acarretando modificações na doutrina e nas ações administrativas diárias, principalmente em relação à segurança cibernética .

Todavia, a era digital gera preocupações e desafios para a sociedade civil e militar. O ambiente virtual torna-se cada vez mais vulnerável e hostil, sendo notório o aumento, de forma considerável, no número de atores cibernéticos que se apropriam de informações com a finalidade de alcançar benefícios financeiros de uma empresa ou desestabilizar uma entidade ou órgão de Estado.

Dessa maneira, com o objetivo de mitigar essas ameaças, surgiu a necessidade de conscientizar os usuários de medidas necessárias que devem ser praticadas a cada acesso ao ciberespaço. Tais ações são denominadas de proteção digital.

Visando adequar-se para o cenário atual, conforme Abdalla (2021), o Exército Brasileiro criou, no ano de 2010, o Centro de Defesa Cibernética (CDCiber), sendo este responsável por realizar atividades no campo cibernético como também capacitar os recursos humanos para operar de forma segura o espectro digital.

No entanto, na formação do soldado reservista, o Exército Brasileiro utiliza como instrumento de treinamento, o Programa - Padrão de Instrução Individual Básico, documento em que, atualmente, não apresenta orientações ou instruções em relação à proteção digital.

Dessa forma, com o objetivo de propagar a capacitação em assuntos referentes à segurança da informação, surge-se a necessidade de atualização do Programa - Padrão de Instrução Individual Básico, neste caso, fundamental para diminuir a exposição dos quartéis à ataques cibernéticos.

1.1 PROBLEMA

O Exército Brasileiro apresenta, como missão, definida na Estratégia Nacional de Defesa, aprimorar a Segurança da Informação e Cibernética, em todas as instâncias do Estado, com ênfase na proteção das Estruturas Críticas. Conjuntamente com o encargo acima citado, destaca-se a necessidade de contribuir no incremento do nível de segurança dessas áreas, principalmente no nível tecnológico e cibernético.

Considerando tais missões acima citadas, pode-se asseverar que os aquartelamentos castrenses são considerados infraestruturas críticas, onde há a presença de informações sigilosas, consideradas, muitas vezes, estratégicas para o país.

Num contexto de evolução dos meios, a análise da segurança digital deve ser compatível com a expansão das atividades educacionais sobre o assunto cibernética em todos os escalões, a fim de que todos possam auxiliar a Força Terrestre a cumprir as tarefas determinadas e, também, consigam compreender a importância do tema na perspectiva de suas ações diárias que necessitam a utilização da rede mundial de computadores.

1.1.1 Antecedentes do Problema

No Brasil, nos últimos anos, houve um aumento significativo no número de pessoas que possuem acesso à rede digital. De acordo com a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), 82,7% dos domicílios apresentam condições de conectar-se virtualmente. Um aumento de 3,6 pontos percentuais em relação ao ano de 2018. (BRASIL,2021)

Todavia, paralelo ao avanço tecnológico do Brasil, ocorreu, também, um aumento, de forma expressiva, nos números de ataques digitais. No 1º semestre de 2021, de acordo com a empresa SonicWall, o Brasil foi o 5º país do mundo que mais registrou ataques do tipo *ransoware*. Cerca de 9,1 milhões de tentativas. (QUEIROZ, 2021)

Acompanhando a revolução tecnológica atual, o Exército Brasileiro, conjuntamente à sociedade, está digitalizando seus processos operacionais e administrativos, sendo que tal ação, por muitas vezes, é executada por soldados e cabos das Organizações Militares castrenses, que são adestrados por meio do Programa – Padrão de Instrução Individual Básica.

1.1.2 Formulação do Problema

Diante do exposto, o problema que se coloca é o seguinte: O Exército Brasileiro, atualmente, consegue capacitar e expandir os conhecimentos atinentes à Segurança da Informação aos soldados recém-ingressos na Força Terrestre, por meio do Programa – Padrão de Instrução Individual Básica?

1.2 OBJETIVOS

Buscando-se orientar o trabalho para responder ao problema apresentado, foram traçados um objetivo geral e cinco objetivos específicos, que serão a seguir apresentados.

1.2.1 Objetivo Geral

Foi definido como objetivo geral verificar se o Exército Brasileiro consegue, atualmente, capacitar e expandir os conhecimentos atinentes à Segurança da Informação aos soldados recém-ingressos nas fileiras castrenses.

1.2.2 Objetivos Específicos

Os seguintes objetivos específicos foram delineados para se obter uma resposta mais completa ao problema apresentado:

a) Explicar, a partir de seus manuais, as formas de coordenação e execução das atividades relacionadas ao preparo da formação dos combatentes básicos do Exército Brasileiro;

b) Identificar as formas de capacitação de pessoal, no âmbito da Cibernética, existentes no Exército Brasileiro;

c) Descrever, a partir do programa Estratégico do Exército Brasileiro de Defesa Cibernética, os objetivos e formas de implementação e gestão de recursos humanos propostas ao setor cibernético;

d) Identificar se houve a inclusão do assunto Cibernética no Programa – Padrão de Instrução Individual Básica; e

e) Compreender as formas de ensino do assunto cibernética aos soldados pertencentes aos Exércitos de outras nações amigas.

1.3 QUESTÕES DE ESTUDO

Considerando a evolução tecnológica presente nos quartéis do Exército Brasileiro, é observado que a formação básica do soldado do efetivo variável demanda a necessidade de integração à assuntos relacionados com a proteção digital. Diante disso, para o melhor entendimento sobre o estudo, foram realizadas as seguintes questões:

- Qual é a forma de ensino atual do assunto cibernética no Exército Brasileiro?

- O ensino, da forma como está sendo ministrada atualmente, consegue capacitar e expandir os conhecimentos atinentes à segurança da informação aos soldados do efetivo variável?

- Quais assuntos devem estar inseridos na matéria cibernética a fim de ser capaz de capacitar, de maneira eficaz, os reservistas de 2ª Categoria?

1.4 JUSTIFICATIVAS

Ao observar a evolução digital que está ocorrendo diariamente no mundo, percebe-se a migração de procedimentos físicos para o ramo computacional. Concomitantemente à essa mudança, verifica-se o aumento de atividades interligadas à captura de informações particulares, muitas vezes consideradas sigilosas por um determinado órgão ou entidade. Partícipe das transformações que estão ocorrendo, o Exército Brasileiro, busca, de forma progressiva, desenvolver ou utilizar ferramentas que auxiliem seus militares nas suas tarefas administrativas e operacionais, proporcionando, aos seus integrantes, o máximo de efetividade no desenvolvimento das suas atribuições. Não obstante, pode-se afirmar que, com o desenvolvimento tecnológico no ambiente castrense, o Exército Brasileiro pode tornar-se vítima de ciberataques que, conforme ANDRADE (2020), é definido como ações, no espectro digital, com o objetivo de infligir prejuízo à parte opositora, que pode estar no nível pessoal, organizacional e até mesmo estatal, fazendo com que sistemas e infraestruturas de rede não se comportem conforme o planejado.

Exemplificando o imbróglio acima exposto, pode-se citar o ataque hacker, do tipo *ransoware*, sofrido, no mês de dezembro de 2021, pelo Ministério da Saúde, em que os portais “ConecteSUS” e o “Portal Covid”, ferramentas utilizadas no controle do combate à pandemia do COVID-19, ficaram impossibilitados de acesso por 15 dias após o ataque do grupo *hacker Lapsus$ Group* (ANDRADE, 2021).

Por conseguinte, no ramo militar, destaca-se, também, a preocupação estatal com o assunto em questão. No ano de 2018, foi elaborada a Estratégia Nacional de Defesa, documento governamental que define setores estratégicos como essenciais para a defesa do Brasil: O nuclear, a cargo da Marinha do Brasil e o setor Espacial, sob a responsabilidade da Força Aérea Brasileira. Além das áreas já citadas, há o setor Cibernético, a cargo do Exército Brasileiro, onde almeja-se desenvolver o ramo da pesquisa e inovação, com foco nas tecnologias e na execução das atividades Cibernéticas no âmbito do Setor de Defesa, tendo como objetivo principal contribuir para o aprimoramento da Segurança Cibernética, em todas as instâncias do Estado.

Além do exposto, o documento cita a importância da capacitação de pessoal durante o serviço militar obrigatório, destacando a preocupação do Brasil em possuir uma reserva qualificada, pronta para atuar:

> O Serviço Militar Obrigatório deverá ser empregado de acordo com critérios estabelecidos no âmbito das Forças Singulares, em função das

> características e necessidades funcionais e profissionais de cada uma delas. Entretanto, deverá ser observado seu caráter educativo, social e profissionalizante, de modo a entregar à sociedade cidadãos comprometidos com o País e mais bem preparados para o mercado de trabalho, e militares qualificados e motivados para bem servir à Pátria (ESTRATÉGIA NACIONAL DE DEFESA,2008, p.43).

Tendo em vista a progresso do assunto, o Ministério da Defesa, no ano de 2014, desenvolveu a Doutrina Militar de Defesa Cibernética, expressa no Manual MD31-M-07, o qual evidencia, mais uma vez, a preocupação em capacitar o Poder Nacional a responder, de forma oportuna e adequadamente, à novas ameaças que podem surgir na conjuntura globalizada atual.

Trazendo para a realidade atual, faz-se necessária uma análise da formação dos reservistas de 2ª Categoria do Exército Brasileiro, buscando as interseções e necessidades para que os elementos em formação possam ser capacitados no assunto relacionados à cibernética, especialmente na matéria proteção digital.

Destaca-se que o assunto deve estar presente na formação básica combatente pelo motivo de que tais cidadãos empregarão, após a sua formação, nos diversos aquartelamentos do país, a rede de computadores para cumprir as suas tarefas diárias como também utilizarão seus celulares, muitas vezes conectados à internet, numa área militar, sendo que o desconhecimento sobre as peculiaridades cibernéticas numa área bélica poderá causar a exposição de dados, informações ou a criação de vulnerabilidades a serem exploradas por um especialista nesse tipo de atividade.

Trazendo o foco ao modo do ensino profissional do Exército, depreende-se que a formação básica do combatente é feita por meio dos Programas-Padrão, nos quais são definidos a maneira mais eficiente de conduzir as diversas instruções, assegurando a qualidade das mesmas, sem deixar de analisar a conjuntura orçamentária anual.

Voltando vistas para a junção dos elementos já evidenciados, faz-se necessário realizar um estudo sobre a formação básica do efetivo variável e verificar se tal organização educacional atual inclui assuntos relativos à cibernética ou proteção digital.

Ao término deste trabalho, pretende-se chegar à conclusão de se é preciso ou não alterar o Programa-Padrão de Instrução Individual Básica, bem como um correto

entendimento sobre a maneira mais eficiente de lecionar o assunto cibernética ao jovem recém – ingresso às fileiras castrenses.

O trabalho em questão contribui com o Plano Estratégico do Exército 2020-2023, em especial com a Ação Estratégica 4.2.1, que elenca a atividade “4.2.1.4 “Adequar a estrutura de ensino de Defesa e Guerra Cibernética.” (BRASIL, 2019f, p. 20). Dessa maneira, o tema em estudo pode contribuir no desenvolvimento dos e alcance dos objetivos destacados no plano estratégico da Força Terrestre.

2. REVISÃO DA LITERATURA

2.1 O SISTEMA DE INSTRUÇÃO MILITAR DO EXÉRCITO BRASILEIRO

O ensino profissional do Exército Brasileiro é constituído, conforme define o Sistema de Instrução Militar do Exército Brasileiro, por dois sistemas integrados: o Sistema de Ensino Militar e o Sistema de Instrução Militar do Exército Brasileiro (SIMEB). O SIMEB é dirigido para a formação dos quadros temporários que ingressam na vida militar.

O SIMEB é um instrumento utilizado pelo Comando de Operações Terrestres (COTER) para orientar, coordenar e controla o Preparo Operacional da Força Terrestre. Ademais, contém os esclarecimentos e os detalhes julgados necessários à execução das atividades de instrução (BRASIL, 2019).

O Sistema de Instrução Militar do Exército Brasileiro (SIMEB) tem, dentre seus objetivos, o adestramento da Força Terrestre como peça de combate, almejando alcançar a formação das praças temporárias e para a adaptação de técnicos civis à vida militar (BRASIL, 2019).

Destaca-se, ainda, que as instruções militares, reguladas pelo SIMEB, pondera as caracteristicas dos oito Comandos Militares de Área, levando em consideração as características das suas respectivas áreas de atuação e seus respectivos empregos vinculados ao preparo operacional nacional.

Objetivando materializar sua atuação, o COTER utiliza, como produto, os Programas-Padrão de Instrução, nos quais são definidos a maneira mais eficiente de conduzir as diversas instruções, assegurando a qualidade das mesmas, sem deixar de analisar a conjuntura orçamentária daquele ano (BRASIL, 2019).

Torna-se importante ressaltar que os Programas-Padrão de Instrução são documentos que sofrem modificações anualmente, buscando promover a sinergia entre a otimização do custo, o benefício da atividade-fim, a duração dos períodos de instrução, a racionalização da situação orçamentária e a redução do desgaste do material.

Desta forma, frisa-se que a formação dos jovens recém – ingressos ao Exército Brasileiros são reguladas pelo SIMEB, em que, baseados nos Programas – Padrão de Instrução, são transformados em soldados e graduados mobilizáveis, com capacidade de serem integrados na estrutura de emprego, em caso de mobilização.

2.1.1 PROGRAMA – PADRÃO DE INSTRUÇÃO INDIVIDUAL BÁSICA

Para a formação da sua reserva de 2ª categoria, o Exército Brasileiro utiliza o Programa – Padrão de Instrução Individual Básica. Conforme define o próprio documento, a sua finalidade é definir os objetivos que permitem padronizar o treinamento necessário à Preparação Básica do Combatente, independente da arma, quadro ou serviço do quartel onde esteja lotado. (BRASIL, 2019).

No seu escopo, verifica-se a intitulação de objetivos, cuja finalidade é orientar aos instrutores sobre os comportamentos que devem ser desenvolvidos nos jovens durante o período de formação.

Notabiliza-se que, dentre os objetivos parciais elencados, encontra-se a aquisição de conhecimentos básicos indispensáveis aos soldados e o desenvolvimento de habilidades técnicas, propósitos que podem se correlacionar com as matérias de proteção digital.

Dentre outras finalidades já elencadas, destaca-se, também, que o Programa – Padrão destina-se a habilitar o conscrito para o desempenho das funções correspondentes ao cargo que vai ocupar no Quadro de Cargo Previsto (QCP) da

Organização Militar (OM), capacitando-o ser integrado nos grupamentos que constituem o aquartelamento (BRASIL, 2019)

Sobre a metodologia aplicada, o programa de treinamento baseia-se no método de desempenho, visando qualificá-los em assuntos considerados fundamentais para a realização das atividades essenciais para as suas respectivas funções.

As instruções que utilizam o método do desempenho, mobiliza o instruendo, dando-lhe o tempo necessário para aprender. Como decorrência da ênfase dada ao “aprender fazendo”, o instrutor apresenta condições de acompanhar o ensino e, como resultado, tornar o ensino mais eficiente. Dessa forma, verifica-se a necessidade de aguardar pelos resultados e os alunos verificam a sua progressão.

Por conseguinte, no Programa – Padrão, o nucleamento do conhecimento é determinado através de núcleos de integração dos conhecimentos necessários, desdobrando-se em assuntos que, por sua vez, são ordenados em matérias. (BRASIL, 2019)

As instruções com matérias consideradas fundamentais compreendem um conjunto de matérias, um conjunto de assuntos integrantes de cada matéria, um conjunto de sugestões de objetivos intermediários, e um conjunto de objetivos terminais chamados Objetivos Individuais de Instrução (OII), que podem ser relacionados a conhecimentos, a habilidades e a atitudes. (BRASIL, 2019)

Os OII relacionados, respectivamente, às áreas cognitiva e psicomotoras relacionam-se aos comportamentos que o soldado deve exibir como resultado do processo ensino-aprendizagem. Os Objetivos Individuais de Instrução referentes a estas áreas são definidos para cada assunto, expressando um comportamento terminal identificado por três elementos: Atributo, Conjunto de Condições de Observação e Padrão de Evidencia do atributo (BRASIL, 2019).

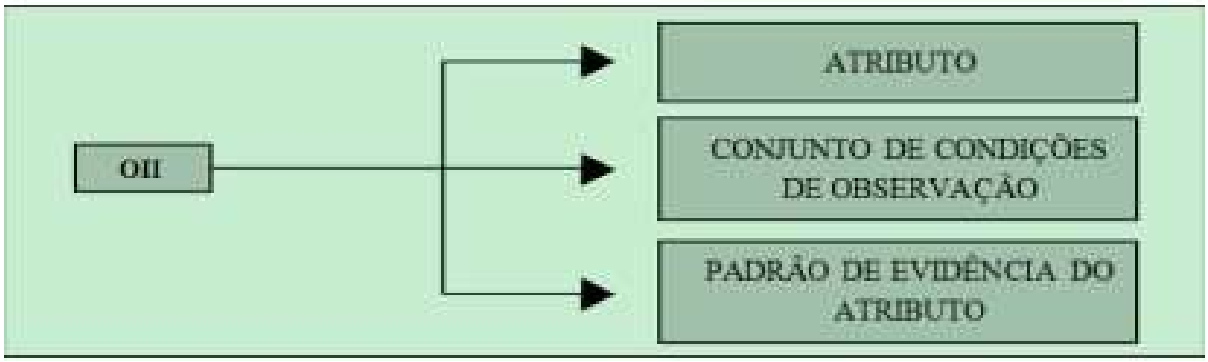


Figura 1 – Exemplo de Instruções previstas no Programa – Padrão de Instrução Individual Básica.
Fonte: SISTEMA DE INSTRUÇÃO MILITAR DO EXÉRCITO BRASILEIRO, 2019, pág 3-3

Em relação ao período de utilização do Programa – Padrão de Instrução Individual Básica na formação do soldado, é imperioso afirmar que o ensino, através dessa ferramenta, limita-se à Fase de Instrução Individual Básica, sendo essa dividida em 2 subfases, conforme elucidado no Programa – Padrão de Instrução Individual Básica:

> 1) Da fase:
> Adquirir conhecimentos básicos que proporcionem a sobrevivência no combate.
> 2) Da 1ª Subfase:
> Capacitar o Soldado a ser empregado na Defesa do Aquartelamento.
> 3) Da 2ª Subfase
> Capacitar o Soldado a ser empregado nas Operações de Garantia da Lei e da Ordem (PROGRAMA PADRÃO DE INSTRUÇÃO INDIVIDUAL BÁSICA, 2019, p.6).

Sobre as matérias consideradas essenciais, verificamos que são dividas conforme as subfases citadas anteriormente, sendo na 1ª subfase ministrado os seguintes assuntos: Armamento, Munição e Tiro, Boas Maneiras e Conduta do Militar Camuflagem, Comunicações, Conhecimentos Diversos, Defesa do Aquartelamento, Educação Moral e Cívica, Fardamento, Hierarquia e Disciplina Militar, Higiene e Primeiros Socorros em Combate, Instrução de Apronto Operacional, Justiça e Disciplina, Lutas, Marchas e Estacionamentos, Ordem Unida, Observação e Orientação, Prevenção e Combate a Incêndio, Serviços Internos e Externos, Técnicas Especiais, Treinamento Físico Militar, e Utilização do Terreno (BRASIL, 2019).

Já em relação à 2ª subfase, tais matérias a constitui: Armamento, Munição e Tiro, Defesa Química, Educação Moral e Cívica, Instrução de Apronto Operacional, Lutas, Marchas e Estacionamentos, Operações de Garantia da Lei e da Ordem, Ordem Unida e Treinamento Físico Militar.

Destaca-se que as subfases se integram, de forma que exista a complementação das matérias mesma em fases distintas, a fim de que a formação básica atinja os padrões mínimos de exigência necessários para um combatente

básico perfaça suas atribuições com eficiências nos pelotões ou seções administrativas que irão ser lotados.

Buscando analisar as matérias presentes na formação atual, verifica-se que não há, em nenhuma matéria das subfases, a difusão de assuntos relacionados à proteção digital, sendo presente a matéria Comunicações, porém com a abordagem de assuntos relacionados ao recebimento e transmissões de mensagens.

4. COMUNICAÇÕES				TEMPO ESTIMADO DIURNO: 6 h NOTURNO:	
	(OII) OBJETIVOS INDIVIDUAIS DE INSTRUÇÃO			ORIENTAÇÃO PARA INTERPRETAÇÃO	
	TAREFA	CONDIÇÕES E VALORES MILITARES	PADRÃO MÍNIMO	SUGESTÕES PARA OBJETIVOS INTERMEDIÁRIOS	ASSUNTOS
B-102 (OP)	Retransmitir a mensagem.	Em um local que permita o escalonamento de 20 a 30 m entre os homens, o instrutor deverá transmitir uma mensagem verbal curta ao primeiro instruendo da coluna. Após ter transmitido a mensagem ao primeiro instruendo, o instrutor deverá ir para o final da coluna para receber a mensagem, depois da sua retransmissão por todos os instruendos da coluna.	A mensagem deve chegar novamente ao instrutor, sem distorções que a façam perder o sentido ou o significado real.	• Descrever a importância do mensageiro. • Citar a missão do mensageiro. • Citar como se classificam os mensageiros. • Descrever como são empregados os mensageiros. • Citar quais são as qualidades inerentes ao bom mensageiro. • Fazer a transmissão de mensagens de maneira rápida e segura. • Descrever as operações e cuidados a serem realizados e observados no recebimento e transmissão de mensagens por mensageiros. • Distinguir mensageiro de escala de especial. • Descrever a diferença de atuar dos diversos tipos de mensageiros.	3. Mensageiro: a. Papel. b. Missão. c. Classificação. d. Emprego. e. Qualidades e seleção. f. Instrução a ser ministrada. g. Princípios a serem observados na transmissão de mensagens. h. Mensageiros duplos, de escala e especiais. 4. Conduta do mensageiro.
B-103 (OP)	Atuar como mensageiro, em situação de combate	Em um terreno que permita deslocamento através do campo, deve ser montado um percurso com diversos incidentes, tais como: • Ferido amigo; • Inimigo morto; • Zonas batidas por fogos;. • Patrulha amiga; • Atirador de emboscada; • Local de entrega da mensagem. Cinco minutos antes de ser liberado, o instruendo deve receber carta ou esboço da região, bússola, indicação do itinerário e a mensagem a ser transmitida (de preferência verbal). Sempre que possível, a instrução deve ser também noturna. • O instrutor deverá relacionar os OII com os atributos: disciplina; iniciativa; responsabilidade; persistência; e coragem.	Durante a execução da tarefa o instruendo deverá: • Ao receber a carta ou esboço, identificar o percurso. • Ao receber a bússola, verificar o seu funcionamento. • Após receber a mensagem, memorizá-la e repeti-la. • Realizar o percurso sem desviar-se de seu objetivo. • Transmitir, ao final do percurso, a mensagem sem deturpação que a faça perder o seu significado e o seu sentido real.		

Quadro 1 - Instruções de Comunicações previstas no Programa – Padrão de Instrução.
Fonte: PROGRAMA – PADRÃO DE INSTRUÇÃO DE INDIVIDUAL BÁSICA, 2019, pág 38.

Ademais, cabe aos instrutores verificar o comportamento do seus instruendos, analisando se a matéria foi compreendida pelos novos militares e apreciando-os em relação às suas capacidades para aplicar os conhecimentos difundidos.

Dessa maneira, dentre os assuntos a serem ministrados aos recrutas, pode-se citar a possibilidade do adestramento para a utilização dos meios digitais da caserna de forma segura e consciente na matéria comunicações assim como, pode-

se, também, explorar a maneira correta e protegida de utilizar os aparelhos eletrônicos com capacidade de conexão à internet numa área considerada militar.

2.2 INSTRUÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO PARA O EXÉRCITO BRASILEIRO - (IG 20-19)

Visando o aperfeiçoamento dos seus quadros de pessoal em relação ao uso seguro dos meios digitais nas Organizações Militares, foi aprovado, pelo Comandante do Exército, Portaria nº 483, de 20 de setembro de 2001, as Instruções Gerais de Segurança da Informação no âmbito do Exército Brasileiro. Sobre o documento, assevera-se que sua finalidade é orientar sobre as atividades que devem ser desenvolvidas no âmbito da segurança digital. (BRASIL, 2001).

Sobre os setes objetivos elencados nas instruções, pode-se destacar a atenção destacada pelo Comandante da Força Terrestre sobre o desenvolvimento de conscientização da segurança cibernética e a preocupação da capacitação dos militares castrenses:

> III - fomentar, ao longo de toda a cadeia hierárquica, a obtenção de atitude favorável no tocante à Segurança da Informação, bem como incrementar a conscientização a respeito da importância do assunto; IV - estimular a eliminação da dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação e de comunicações; V - promover o intercâmbio científico-tecnológico, junto a outros órgãos da Administração Pública Federal e instituições públicas e privadas, sobre as atividades de Segurança da Informação; VI - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em Segurança da Informação; e VII - promover a interoperabilidade e a integração dos sistemas de informação, não só no âmbito do Exército mas, também, junto às demais Forças Armadas e aos demais órgãos da Administração Pública Federal, quando julgado pertinente e respeitadas as regras e normas de segurança em vigor (IG 20-29 INSTRUÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO PARA O EXÉRCITO BRASILEIRO,2001, p.8).

Em relação às regras estabelecidas, observa-se que o presente documento salienta a importância dos militares em trabalharem com a mínima exposição possível, devendo, em todo momento, utilizar medidas de contingência com a finalidade de diminuir os riscos atinentes à utilização da rede mundial de computadores.

No que concerne sobre as medidas a serem realizadas, com a finalidade de alcançar os objetivos estabelecidos, especificamente em relação à capacitação de pessoal, foi determinado, nos artigos 21 e 22, a adoção do tema nas diversas escolas gerenciadas pelo Exército e, também, a realização de campanhas sobre o tema em destaque:

> Art. 21. O tema Segurança da Informação deve ser abordado nas escolas e cursos de formação e aperfeiçoamento militar do Exército Brasileiro, de forma a possibilitar a crescente conscientização e o desenvolvimento de atitudes favoráveis à proteção das informações julgadas relevantes para a Instituição. Art. 22. Em todas as Organizações Militares (OM) devem ser promovidas, periodicamente, campanhas de esclarecimento do público interno, baseadas no teor destas IG e dos demais documentos decorrentes sobre Segurança da Informação que estiverem em vigor (IG 20-29 INSTRUÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO PARA O EXÉRCITO BRASILEIRO,2001, p.11).

Apreciando as responsabilidades delegadas pelo Comandante do Exército, verifica-se que as instruções gerais não esquematizam uma maneira de abordagem do assunto, cabendo aos comandantes, abordarem, em suas respectivas Organizações Militares o tema.

2.2.1 INSTRUÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA O EXÉRCITO BRASILEIRO (EB10-IG-01.014)

Complementando o arcabouço documental do Exército Brasileiro sobre a segurança digital, o Comandante do Exército, através da Portaria nº 803, de 30 de julho de 2014, aprovou as Instruções Gerais de Segurança da Informação e comunicações para o Exército Brasileiro.

Como objetivo, o documento apresenta, orientar as ações relacionadas à segurança da informação e comunicações no âmbito do Exército Brasileiro, com o propósito de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações institucionais (BRASIL, 2014).

No decorrer da diretriz, é reforçado algumas determinações já elencadas na IG 20-19, anteriormente citada, enfatizando a atenção do Comandante do Exército em desenvolver, internamente, a cultura da sensibilização e conscientização dos militares sobre a segurança dos meios eletrônicos.

Sobre a capacitação de pessoal, frisa-se que, mais uma vez, a determinação do assunto ser abordado nas escolas e cursos ministrados pela Força Terrestre, assim como a responsabilidade dos comandantes de unidades em orientar seus subordinados sobre o assunto em questão.

Como novidade, evidencia-se a inclusão do artigo 30, o qual regulamenta o uso de dispositivos móveis para acesso aos recursos computacionais internos, apontando que tal fato deve ser realizado de forma controlada.

Por conseguinte, foi criado a função de Gestor de Segurança da Informação e Comunicações (SIC), cuja função desdobra-se em conduzir os processos digitais de seus quartéis juntamente com a responsabilidade de fomentar e disseminar a cultura da proteção digital.

2.2.2 NORMAS PARA O CONTROLE DA UTILIZAÇÃO DOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO NO EXÉRCITO

Com o objetivo de monitorar o conteúdo de dados armazenados ou divulgados por meio de hardwares de propriedades do Exército Brasileiro, foi desenvolvida as normas para o controle da utilização dos meios de tecnologia da informação no Exército.

Aprofundando o conhecimento sobre as diretrizes abordadas, observa-se que o documento apresenta, como objetivo, controlar o uso, de forma indiscriminada dos meios digitais castrenses e regulamentar a maneira de como devem ser utilizados, a fim de que seja mantido a disciplina militar bem como impedir a exposição negativa da força terrestre.

Sobre a veiculação de dados, observa-se o artigo sétimo, no qual aborda-se a proibição da propagação de conteúdos considerados ilícitos pelo ordenamento jurídico do país juntamente com aqueles contrários à disciplina militar e aos bons costumes:

> Art. 7º É expressamente proibido manter, distribuir ou veicular - utilizando, para isso, dispositivos eletrônicos, ópticos, gráficos ou magnéticos – arquivos contendo matéria considerada ilícita, contrária à disciplina militar, à moral e bons costumes, bem como atentatória à ordem pública, ou que viole qualquer direito de terceiros (NORMAS PARA O CONTROLE DA

> UTILIZAÇÃO DOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO NO EXÉRCITO,2007).

.

Em relação à utilização da internet, sob o domínio do Exército, para acesso aos provedores de e-mails, a norma destaca que pode ser realizada, todavia com com ressalvas, limitando a ação em destaque à somente mensagens de caráter profissional.

Com a finalidade de verificar o cumprimento da NORTI, foi estabelecido que os comandantes das organizações militares devem verificar, ou delegar tal ato, os computadores hospedados em propriedade estatal, averiguando se há dados armazenados ou remetidos, anteriormente, que possam ferir o pundonor militar.

Pretendendo impedir a contaminação dos computadores sob responsabilidade da caserna e evitar a criação de portas de acesso para hackers, na rede de internet sob o domínio do Exército, a norma institui a proibição de acesso à sites que permitam downloads, acesso a salas de conversação ou outros conteúdos diferentes ao exigido no cotidiano militar.

Ademais, analisa-se, também, que a preocupação elencada não é somente responsabilidade dos responsáveis pelo comando das unidades militares, mas sim de cada integrante, conforme aborda o artigo dezessete do presente documento, determinando que cada integrante deve acautelar-se de usar os meios eletrônicos de forma indiscriminada, buscando zelar pelas suas atitudes, como usuários, com o objetivo de não cometerem ações consideradas ilícitas à luz do Regulamento Disciplinar do Exército.

Da mesma forma, o artigo dezesseis destaca como essencial a disseminação do documento em análise, com o intuito de que todos tenham total conhecimento da forma correta de utilizar dos artifícios computacionais presentes em área sob responsabilidade do Exército Brasileiro.

2.2.3 INSTRUÇÕES REGULADORAS SOBRE SEGURANÇA DA INFORMAÇÃO NAS REDES DE COMUNICAÇÃO E DE COMPUTADORES DO EXÉRCITO BRASILEIRO

Tendo como objetivo regulamentar as condições de segurança da informação a serem verificadas nas redes de comunicação e de computadores no Exército

Brasileiro, o chefe do Departamento de Ciência e Tecnologia do Exército, DCT, na portaria nº 004-DCT, de 31 de janeiro de 2007, instituiu as Instruções Reguladoras sobre Segurança da Informação nas redes de comunicação e de computadores do Exército Brasileiro, a IR 13-15.

Em seu artigo segundo, verifica-se os objetivos relacionados à finalidade da instrução, destacando-se o estabelecimento de regras para que possa ser estabelecido os mecanismos de defesa contra violações de segurança da rede, a gestão da segurança e a orientação às OM do Exército na composição de suas normas internas de segurança de redes.

Examinando o documento, perscruta-se que foram catalogados alguns procedimentos tecnológicos de segurança, estando, dentre eles a criptografia. Sobre a técnica em questão, pode-se asseverar que o seu uso deve ocorrer quando existir a necessidade de preservação de dados e em compatibilidade com as regras se segurança de salvaguarda de assuntos sigilosos.

Sobre o tema, atenta-se que a criptografia deve ter sido originada ou autorizada pelo DCT e deve ocorrer de forma controlada, com a quantidade de usuários com acesso a esse procedimento, restrita.

Dentre outras técnicas incentivadas ao uso, destacamos o uso do *firewall*. Em relação à sua finalidade, destaca-se a grande proteção proporcionada ao acessar a internet, devendo ocorrer, assim como a criptografia, o uso limitado e cerceado, devendo ser distribuído o acesso conforme a função e especialidade desempenhada por cada militar.

Ademais, outras medidas de proteção são listadas nas instruções reguladoras: utilização de softwares com licença, uso de antivírus, evitar realização de *downloads* de fontes desconhecidas, realizar a abertura do correio eletrônico somente de endereços conhecidos e evitar o emprego de mídias removíveis, como *pendrives,*.

Desdobrando-se sobre a documentação, é determinado, também, que o acesso à rede deve ser feito com controle de acesso. Com essa deliberação, pode-se objetivar a autenticidade de identificação do usuário naquele momento, facilitando, dessa maneira, o reconhecimento do militar que possa estar utilizando a internet do aquartelamento de forma errônea e que, dessa forma, poderia acarretar a exposição de informações e dados internos.

Outra ferramenta de proteção cibernética destacada, que deve ser implementada nas organizações militares terrestres, é a realização de cópias de segurança. Conforme o artigo cinquenta e quatro aborda, toda a rede do Exército deverá efetivar cópias de segurança de seus arquivos, a fim de que seja possível a recuperação de dados supostamente perdidos durante um evento crítico.

Relacionado com a proteção cibernética, pode-se correlacionar a segurança das estruturas físicas locais. Conforme abordado nas diretrizes, a segurança das instalações deve ser realizada de forma minuciosa, sendo realizado, para isso, o controle de pessoas com acesso aos computadores, o horário de utilização dos meios e a gerência dos militares com ingresso permitido no compartimento de servidos da unidade.

2.2.4 CARTILHA EMERGENCIAL DE SEGURANÇA DO DCT

Visando fomentar a projeção da segurança tecnológica no âmbito do Exército Brasileiro, o Departamento de Ciência e Tecnologia (DCT), elaborou a Cartilha Emergencial de Segurança da Tecnologia da Informação e Comunicações.

Frisa-se que, uma das primeiras determinações presente no documento em estudo é a obrigatoriedade de cumprir as medidas estabelecidas, sendo que a não observância poderá implicar a imputação de responsabilidade ao usuário.

Sobre os objetivos da cartilha, salienta-se, mais uma vez, a obrigatoriedade do cumprimento das normas em todas as Organizações Militares do Exército, tendo em vista que a regras ali contidas são de baixo custo e já praticado por muitas unidades militares.

Por conseguinte, os autores ressaltam que as regras formam elaboradas com base na experiência de profissionais do Exército na área de telemática, proporcionando, dessa forma, a adequabilidade das ações de segurança informacional no contexto castrense.

Dentro do escopo das medidas básicas elencadas, há a determinação de que cada comandante de Organização Militar, publique, em Boletim Interno, uma comissão com o objetivo de auditar a atual segurança digital dos computadores da unidade, considerando, como referência, a cartilha desenvolvida:

> 2.1 Cada OM deverá organizar, publicando em Boletim Interno, um Comitê permanente de auditoria interna das medidas de segurança preconizadas na regulamentação vigente, constantes ao final desta Cartilha e parcialmente abordadas no texto, cabendo ao DCT a realização de verificações externas de caráter programado ou inopinado, como autoridade validadora dos níveis de segurança dos sistemas sustentados pela TI do Exército Brasileiro (CARTILHA EMERGENCIAL DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES,2011, p.3).

Expandindo o estudo do documento, percebe-se que o DCT estabelece medidas simples de cibersegurança, que podem ser executadas por qualquer usuário da internet, destacando-se a baixa complexidade das ações a serem executadas, como: controlar o acesso à Internet na OM, proibir a utilização de dispositivos móveis de armazenamento, manter o sigilo das senhas, utilizar somente software original e licenciado entre outras.

Sobreleva-se a determinação de ser estipulado uma rotina de conscientização com os integrantes dos quartéis, com a finalidade de explicar a forma correta e segura de utilizar os meios computacionais:

> 2.3 Estabelecer uma rotina de permanente conscientização dos integrantes da organização quanto ao emprego adequado dos recursos de Tecnologia da Informação e Comunicações (TIC) à disposição da OM (CARTILHA EMERGENCIAL DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES,2011, p.4)

No tocante ao uso da rede, foi estabelecido que, quando o aquartelamento possuir o acesso à internet disponibilizado pelo Centro Integrado de Telemática do Exército ou pelo Centro de Telemática de Área, não deve ocorrer contratações de empresas provedoras. Caso seja considerado algo impreterível, não permitir que tais acessos sejam feitos, também, à EBNet:

> 4.1 Quando a OM possuir acesso à Internet disponibilizado pelo CITEx ou pelo CTA/CT da sua área, não deve haver contratação de outros acessos junto às empresas provedoras do serviço. O DCT está atualizando e ampliando o provimento de serviços necessários às atividades institucionais.
> 4.2 Na imperiosa necessidade de contratação de acesso à Internet, não permitir que as estações conectadas à rede mundial estejam, simultaneamente, conectadas também à EBNet (CARTILHA EMERGENCIAL DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES,2011, p.7).

Juntamente com a medidas já listadas, determina-se que, em caso de meios de tecnologia da informação considerados obsoletos ou que necessitem de

manutenção em regiões externas ao quartel, deve ser retirados os discos rígidos, pois tais periféricos armazenam informações, que, mesmo sendo deletadas, podem ser recuperadas ao serem analisadas por um especialista.

Por fim, em relação à página de internet da Organização Militar, preceitua-se que suas hospedagens sejam feitas nos servidores do Centro Integrado de Telemática do Exército ou do Centro de Telemática de Área, juntamente com a adoção de página simples, com componentes confiáveis e, da mesma forma, atentando aos princípios da contra-inteligência.

2.3 A FORMAÇÃO DO SOLDADO FUZILEIRO NAVAL DA MARINHA DO BRASIL

Buscando perscrutar as medidas adotadas pela Marinha do Brasil em relação ao assunto, delimitou-se o estudo do currículo do curso de Fuzileiros Navais da Marinha do Brasil.

Com relação do propósito do curso, desprende-se o objetivo preparar os aprendizes para exercerem a função atinente ao Soldado Fuzileiro Naval dentro dos parâmetros exigidos e necessários à Marinha do Brasil.

Sobre o currículo, analisa-se que são ministradas, durante a formação, oito disciplinas, instrução militar naval, ordem unida, treinamento físico militar, instrução básica de combate, operações de fuzileiros navais, armamento e tiro, ética profissional militar e inglês, sendo cada uma constituída de uma determinada carga horária.

Particularizando o estudo sobre as disciplinas, aprecia-se que cada unidade de estudo apresenta objetivos secundários, denominado lista de unidade de ensino, na qual são estabelecidos novos assuntos correlacionados, de forma pormenorizada, com a disciplina.

MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA

CENTRO DE INSTRUÇÃO ALMIRANTE MILCÍADES PORTELA ALVES **CENTRO DE INSTRUÇÃO E ADESTRAMENTO DE BRASÍLIA**
CURSO DE FORMAÇÃO DE SOLDADOS FUZILEIROS NAVAIS
CÓDIGO: FSD-FN-I **CARGA HORÁRIA: 24 HORAS** **DISCIPLINA: INSTRUÇÃO MILITAR NAVAL** **ATUALIZADO EM 2022**
SUMÁRIO

1) OBJETIVO DA DISCIPLINA
Identificar as características básicas da vida militar.

2) LISTA DE UNIDADES DE ENSINO
1 - UNIFORME DA MARINHA DO BRASIL..... 3 HORAS
1.1 - Finalidade, princípios básicos e regras gerais dos uniformes da Marinha do Brasil (MB);
1.2 - Classificação, composição e situação de uso dos uniformes básicos da MB; e
1.3 - Insígnias e distintivos.

2 - NORMAS DE CORTESIA, RESPEITO E CERIMONIAL..... 4 HORAS
2.1 - Conceitos fundamentais sobre sinais de respeito e elementos essenciais da continência individual;
2.2 - Procedimentos em outras situações, continência em veículos, continência à tropa e situações diversas; e
2.3 - Regras gerais de honras, procedimentos com o Hino e a Bandeira Nacional.

Quadro 2 – Disciplina Instrução Militar Naval do Curso de Formação de soldados Fuzileiros Navais da Marinha e sua lista de unidades de ensino.
Fonte: CURRÍCULO DE FORMAÇÃO DE SOLDADOS FUZILEIROS NAVAIS, 2022,pág 11

Deslindando o documento educacional, percebe-se que o assunto segurança digital ou cibersegurança não é abordado ou constitui-se como integrante da formação do fuzileiro naval do país.

2.3.1 LA FORMACIÓN DE EGRESO DEL NÚCLEO DE INSTRUCCIÓN BÁSICO DEL EJÉRCITO ARGENTINO

Divergindo da formação dos soldados do Exército Brasileiro, a formação dos soldados recém – incorporados ao Exército Argentino não ocorre em diversos

quartéis do território platino, mas sim em unidades especializadas, cujo objetivo é formar, preparar e adestrar os novos integrantes de sua força terrestre.

Com o objetivo de regulamentar a formação em seus núcleos, é elaborada a *directiva del comandante para la preparación y ejecución de los Núcleos de Instrucción Básica correspondientes a la Incorporación,* no qual é observado as instruções que devem ser ministradas juntamente com o quadro horário destinados àquela matéria específica.

Dentre as matérias definidas encontra-se as matérias *orden cerrado, tiro, adiestramiento fisico, combate, teoría general, educación etico espiritual e formación social militar.*

Ademais, na *directiva,* são estabelecidas exigências que devem ser alcançadas pelos soldados em relação à matéria, em companhia com o quadro horário correspondente e o manual que deve ser utilizado.

Em relação ao assunto proteção digital, não foi encontrada, no estudo das matérias de formação dos recrutas argentinos, a abordagem do tema, todavia, foram elaboradas sugestões de instruções sobre cibersegurança, com o objetivo de conscientizar sobre os riscos digitais e ensinar aos militares sobre as ferramentas disponíveis para a proteção dos seus dados e de suas unidades (MOYANO, 2020).

Nro	Lineas de concientización	Objetivos generales de concientización	
1	General	1.1	Dar a conocer los riesgos del ciberespacio.
		1.2	Informar que las FFAA son objetivo de ciberataques, aumentando esta circunstancias el nivel de amenaza al que está sometido su personal.
2	Identificación y Credenciales de acceso	2.1	Concientizar de la importacia de una gestión adecuada de las contraseñas y de otras credencia-les de acceso en la protección de la información.
3	Navegación de Internet	3.1	Promocionar el uso responsable de Internet.
		3.2	Difundir hábitos y buenas prácticas de navegación por Internet.
		3.3	Enseñar cómo identificar enlaces potencialmente peligrosos.
		3.4	Recomendaciones especificas para el uso de servicios electrónicos homebanking y pagos on-line
4	Correo electrónico	4.1	Advertir que el correo electrónico es uno de los medios más frecuentes de ciberataque, puesto que no es un método totalmente seguro para intercambiar información fuera del ámbito de las FFAA.
		4.2	Enseñar cómo identificar mensajes potencialmente peligrosos ("pishing" y fraudes on-line)
5	Servicios en la red	5.1	Difundir recomendaciones de uso seguro de servicios de internet, conciliando la productividad con la seguridad.
		5.2	Recomendaciones especificas para proteger la información personal en Internet.
6	Actividad en redes sociales	6.1	Explicar a los usuarios cómo pueden ser victimas de ataques de "ingeniería social", especial-mente en las redes sociales.
		6.2	Promover la prudencia en el uso de las redes sociales, especialemente a la hora de publicar información.
		6.3	Prevenir situaciones de riesgo para las FFAA o terceras personas que tienen relación con los usuarios.
7	USB y soportes de información	7.1	Avisar de los riesgos asociados al uso de soportes y dispositivos de almacenamiento USB (infec-ción, pérdida de información y posible infracción de la normativa)
8	Protección del entorno personal	8.1	Explicar a los usuarios cómo pueden proteger su PC personal.
		8.2	Enseñar cómo es posible trasladar esta protección a los dispositivos y redes personales en el ámbito personal.
9	Fuera de la oficina: Movilidad	9.1	Informar a los usuarios de su especial vulnerabilidad en situación de movilidad fuera de su puesto de trabajo.
		9.2	Explicar a los usuarios cómo pueden proteger los dispositivos móviles y portátiles tanto en el ámbito profesional como el personal.
10	Prevención y reacción ante los incidentes	10.1	Poner de manifiesto la importancia de la participación de los usuarios en la detección temprana y respuesta a incidentes de ciberseguridad.
		10.2	Fomentar que el usuario acuda a informarse sobre los riesgos y alertas de seguridad a través de los portales falsos.
		10.3	Enseñar a identificar incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
		10.4	Difundir el procedimiento para comunicar incidencias de seguridad, sean reales o falsas alar-mar a las unidades encargadas de gestionarlas.

Quadro 3 – Ejemplos de de líneas de concientización y objetivos perseguidos del plan de concientización em ciberdefensa.

Fonte: LA REPÚBLICA ARGENTINA Y SUS ESFUERZOS EN CIBERDEFENSA. EL COMPROMISO CON LAS BUENAS PRÁCTICAS COMO PARTE DE SU IDEARIO, 2020, pág 59.

A elaboração dos documentos sobre ciberdefesa, na República da Argentina, é de responsabilidade do *Comando Conjunto de Ciberdefensa,* CCCD, o qual, tem, como missão, elaborar a doutrina necessária para o adequado emprego dos meios de cibersegurança:

> Nesta esfera de interesse, a promulgação da legislação respectiva por parte das distintas carteira ministeriais, como também as necessidades que surgem para incorporar a ciberdefesa ao planejamento e execução das operações que realiza o instrumento militar proporcionam o *input* para que o CCCD se dedique à elaboração da doutrina necessária par ol adequado emprego dos meios de ciberdefesa à disposição.(MOYANO, 2020, p. 56, tradução nossa)

Conjuntamente com a missão citada, assevera-se que o CCCD possui a atribuição de capacitar, criar competências e sensibilizar os militares, buscando desenvolver uma estratégia de proteção cibernética eficaz para as Forças Armadas daquele país.

2.3.2 NATIONAL CYBER SECURITY FRAMEWORK MANUAL

Com a finalidade de acompanhar o panorama atual de ameaças digitais e manter a defesa cibernética, a Organização do Tratado do Atlântico Norte, OTAN, adotou políticas que visam desenvolver as capacidades de defesa digital e cooperação entre os seus países aliados.

Como ferramenta para o apriromanento da sua proteção, foram realizados diversos encontros entre as nações, onde foram estabelecidos compromissos, acordos e a comuta de boas práticas para a amplificação da resiliência cibernética da Organização.

Dirigindo-se para estabelecer padrões educacionais sobre o assunto, a OTAN criou centros educacionais de segurança informacional, onde são realizados os cursos, estágios, compartilhamentos de dados e incrementação de ações coordenadas.

Dentre os centros de ensino já destacados, ressalta-se o e *NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE.* Localizado na Estônia, o centro é responsável pela pesquisa e treinamento de defesa cibernética da Organização do Tratado do Atlântico Norte, tendo como objetivo de capacitar os integrantes dos países membros e nivelar o conhecimento a serem aplicados nas nações integrantes.

Ademais, como fruto das pesquisas realizadas, foi desenvolvido o *NATIONAL CYBER SECURITY FRAMEWORK MANUAL.* Sobre os objetivos destacados do documento, destaca-se a exposição de facetas que devem estar presentes na elaboração de políticas de proteção informacional bem como medidas a serem adotadas diantes das principais ameaças cibernéticas atuais.

No estudo do documento, observou-se o levantamento de boas práticas implementadas pelos países membros, cuja finalidade é a análise e a possível efetização em outras nações, considerando a peculiaridade de cada uma.

Por conseguinte, é explorado a atividade de proteção digital em ambientes militares. Sobre o assunto, o manual salienta que as medidas não devem estar restritas àquelas elaboradas pela OTAN, mas que, cada país, considerando suas singularidades, incluindo as diferentes formações dos seus militares, deve promovar a conscientização e propagação de atitudes que objetivam à proteção dos seus meios informatizados, devendo atentar, antes da execução, para as normas e procedimentos padronizados na Organização.

Em relação ao desenvolvimento educacional, o manual explora que, tipicamente, são adotadas medidas de prevenção, o que ocasiona uma escassez de conhecimento em relação à ações de resposta e recuperação de informações após um ataque, defendendo que se deve almejar a compreensão e entendimento nos casos citados.

Como complementação à ideia, é acentuada a importância da realização dos cursos disponibilizados para fins de preparação de pessoal,em todos os escalões, incluindo os soldados recrutas, com a finalidade de que esses discentes possam propagar as informações aprendidas em todos os meios frequentados.

IT Systems Attack and Defence Course (ITSADC)

Location: Tallinn or online

Date: 19-23 September, 2022

Registration starts: 28 June 2022

Registration deadline: 2 August 2022

Course fee: 500 € (1 free slot per Sponsoring Nations, Contributing Participants and NATO bodies)

Administration fee: 130 € (if the course will be held in Tallinn, for the online course there is no Administration fee)

Course Aim

IT Systems Attack and Defence is a practical 5-day course, intended for system administrators, developers and other technical personnel. The course introduces tools and methods used by attackers to gain access to IT systems and discusses potential countermeasures and ways of detection. A large part of the course is based on hands-on exercises. Practical tasks focus mainly on the offensive side of IT security, the participants can try out for themselves how various real-world attacks can be conducted. In addition, participants can take part in a Capture the Flag competition, where points are awarded for successfully completing the hands-on tasks, with bonus points awarded for the fastest students.

Students will be provided with virtual machines based on Kali Linux. The majority of the tools used in the class are free or open-source. The vulnerable web applications are built using mostly PHP and MySQL. The course does not focus on specific technologies, but rather uses them as an example for certain classes of attacks.

Quadro 4 – Exemplo de curso ministrado pelo *NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE.*
Fonte: NATO CCDCOE TRAINING CATALOGUE, 2022, pág 22.

3. METODOLOGIA

3.1 OBJETO FORMAL DE ESTUDO

A pesquisa buscou identificar as lacunas existentes no Programa - Padrão de Instrução Individual Básica sobre a matéria cibernética, visando analisar a situação documental atual em relação ao respectivo assunto, destacando o quesito segurança digital, utilizando, para isso, as determinações e diretrizes nacionais

sobre o tema cibernética e manuais militares e legislações de outras nações que já desenvolveram suas políticas de defesa sobre proteção cibernética.

Para auxiliar o estudo, foram levantadas questões com o objetivo de compreender os seguintes panoramas relacionados ao ensino sobre a proteção digital ao soldado reservista:

Como é realizado o ensino da matéria cibernética no Exército Brasileiro, buscando identificar os assuntos abordados e os militares que, atualmente, possuem acesso aos conteúdos abordados.

Conjuntamente, identificou-se se o conteúdo relacionado à proteção digital consegue ser expandido aos soldados do efetivo variável ou se tais matérias fazem parte dos seus currículos de formação educacional militar.

Realizou-se uma análise sobre quais temáticas devem estar presentes na formação do recruta do Exército Brasileiro, a fim de mitigar possíveis acidentes digitais com computadores das diversas Organizações Militares castrenses.

Com essas informações e compilações de dados, foi possível alcançar os resultados para as questões enumeradas.

3.2 DELINEAMENTO DA PESQUISA

A pesquisa foi do tipo qualitativa com método bibliográfico em obras relacionadas à cibernética, tanto civis como militares.

.

3.3 AMOSTRA

Foram estudados manuais doutrinários, leis nacionais e internacionais vigentes, artigos científicos e publicações periódicas que abordam o assunto cibernética e segurança digital no contexto da defesa e soberania nacional.

3.4 PROCEDIMENTOS PARA REVISÃO DA LITERATURA

A revisão ocorreu dentro de um universo de legislações relativas ao tema, obtidos de forma física e, principalmente, com consulta na internet, utilizando plataformas governamentais que abordem o assunto, o Google Acadêmico e a Biblioteca do Exército.

3.5 INSTRUMENTOS

O trabalho contou com o auxílio da coleta documental e a análise de conteúdo de países com vasta experiência no campo da defesa cibernética, juntamente com as suas legislações atinentes ao tema. Agregando à pesquisa, utilizar-se-á, também, as legislações nacionais e manuais militares nacionais para verificar a diretrizes e determinações nacionais sobre o tema.

3.6 ANÁLISE DE DADOS

Os dados alcançados foram estruturados de forma a analisar os conceitos disponíveis nos manuais sobre o assunto, extraindo informações julgadas importantes para o estudo.

Após esta análise, buscou-se o confronto dos dados obtidos com as necessidades demandadas no arcabouço jurídico brasileiro, visando analisar os tópicos considerados importantes e que não estejam de acordo com as necessidades determinadas.

A tabulação dos dados obtidos foi utilizada para verificar a necessidade de atualização do documento vigente, tendo como procedimento demandado a comparação direta do documento atual com os manuais dos exércitos de outras nações sobre o assunto cibernética.

4. RESULTADOS

Almejando alcançar uma solução para os problemas evidenciados, foram realizadas pesquisas bibliográficas sobre a forma de adestramenro cibernético dos soldados em manuais militares do Exército Brasileiro, da Marinha do Brasil, da Organização do Atlântico Norte e do Exército da República Argentina. Conjuntamente, foram analisados estudos desenvolvidos sobre o tema em estabelecimentos militares, nacionais e internacionais, assim como em estabelecimentos civis, em que buscou-se dados referentes ao desenvolvimento e prepararo das nações à possíveis ataques cibernéticos.

Em relação ao ensino do assunto cibernética no Exército Brasileiro, pode-se asseverar que tal matéria, atualmente, é disponibilizada através de cursos e estágios, que são ministrados no Centro de Instrução de Guerra Eletrônica, na Escola de Comunicações do Exército e na Escola de Inteligência Militar do Exército.

Sobre o universo de seleção para a realização das capacitações, verifica-se que a solicitação para a realização pode ser feita por oficiais, subtenentes e sargentos, respeitando-se a normatização e finalidade de cada formação.

30.5 - CURSO DE INTELIGÊNCIA CIBERNÉTICA PARA OFICIAIS

Área de Atuação: Inteligência

Duração: 22 semanas

FINALIDADE	Habilitar Majores e Capitães aperfeiçoados de carreira, das linhas de ensino militar-bélico, científico-tecnológica (QEM Computação) e complementar (QCO Informática), à ocupação de cargos e ao desempenho de funções que exijam o emprego de técnicas especializadas de Inteligência Cibernética para obtenção de dados bem como a produção de conhecimentos em agências e órgãos de Inteligência do Sistema de Inteligência do Exército (SIEx).
NORMATIZAÇÃO	• Portaria nº 479 - EME, de 28 de novembro de 2017 – Estabelece as condições de funcionamento do Curso de Inteligência Cibernética para Oficiais; e • Portaria nº 041 - EME, de 29 de fevereiro de 2016 – Cria o Curso de Inteligência Cibernética para Oficiais.
MODALIDADE	Pós-graduação *lato sensu*.
UNIVERSO DE SELEÇÃO	Capitães, os primeiros-tenentes, e em caráter excepcional a critério do EME, os majores, das Armas, do Quadro de Material Bélico, do Serviço de Intendência, do Quadro de Engenheiros Militares (especialidade Computação) e do Quadro Complementar de Oficiais (especialidade Informática) não possuidores de um dos seguintes cursos: Curso de Altos Estudos Militares (CAEM/ECEME), Curso de Direção para Engenheiros Militares (CDEM/ECEME), Curso Intermediário de Inteligência para Oficiais, Curso de Inteligência de Sinais para Oficiais, Curso de Inteligência de Imagens para Oficiais e Curso de Geointeligência para Oficiais, da EsIMEx
ÓRGÃO GESTOR	Centro de Inteligência do Exército.
DURAÇÃO	01 (um) curso a cada ano ímpar, com até 22 (vinte e duas) semanas (até 10 EAD e até 12 presenciais).
COMPETÊNCIAS PROFISSIONAIS	a. Realizar a produção continuada de conhecimento; b. Planejar e executar ações de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA); c. Apoiar a obtenção de consciência situacional; d. Apoiar a obtenção da superioridade de informações; e e. Apoiar a busca de ameaças.

Quadro 5 – Curso de Guerra Cibernética para Oficiais ministrado pelo Centro de Instrução de Guerra Eletrônica do Exército Brasileiro.
Fonte: CATÁLOGO DE CURSOS DO DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO, 2019, pág 257.

30.6 - CURSO DE INTELIGÊNCIA CIBERNÉTICA PARA SUBTENENTES E SARGENTOS

Área de Atuação: Inteligência — Duração: 20 semanas

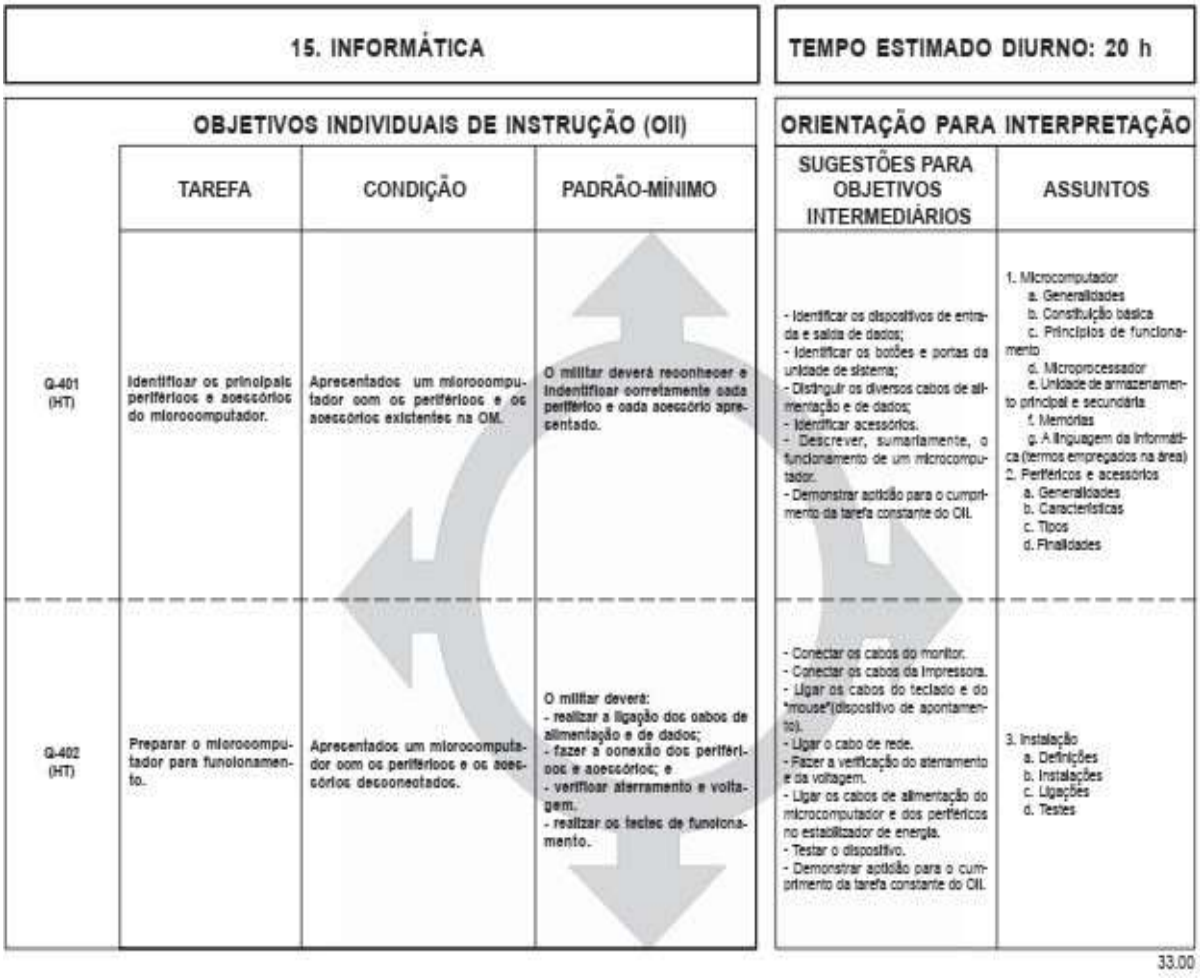
FINALIDADE	Habilitar Subtenentes e Sargentos de carreira, da linha de ensino militar-bélico, à ocupação de cargos e ao desempenho de funções que exijam o emprego de técnicas especializadas de Inteligência Cibernética para obtenção de dados bem como a produção de conhecimentos em agências e órgãos de Inteligência do Sistema de Inteligência do Exército (SIEx).
NORMATIZAÇÃO	• Portaria nº 488 - EME, de 28 de novembro de 2017 – Estabelece as condições de funcionamento do Curso de Inteligência Cibernética para Subtenentes e Sargentos; e • Portaria nº 043-EME, de 29 de fevereiro de 2016 – Cria o Curso de Inteligência Cibernética para Subtenentes e Sargentos
MODALIDADE	Especialização.
UNIVERSO DE SELEÇÃO	Subtenentes, os primeiros-sargentos e os segundos-sargentos aperfeiçoados, das Qualificações Militares de Subtenentes e Sargentos (QMS) Combatentes ou Logísticas, e que não possuam o Curso Avançado de Inteligência para Subtenentes e Sargentos realizado na EsIMEx.
ÓRGÃO GESTOR	Centro de Inteligência do Exército.
DURAÇÃO	01 (um) curso a cada ano ímpar, com até 20 (vinte) semanas (até 8 EAD e até 12 presenciais).
COMPETÊNCIAS PROFISSIONAIS	a. Realizar a produção continuada de conhecimento; b. Executar ações de Inteligência, Reconhecimento, Vigilância e Aquisição de Alvos (IRVA); c. Apoiar a obtenção de consciência situacional; d. Apoiar a obtenção da superioridade de informações; e e. Apoiar a busca de ameaças.

Quadro 6 – Curso de Inteligência Cibernética para Subtenentes e Sargentos ministrado pela Escola de Inteligência Militar do Exército Brasileiro.
Fonte: CATÁLOGO DE CURSOS DO DEPARTAMENTO DE EDUCAÇÃO E CULTURA DO EXÉRCITO, 2019, pág 257.

Em relação à qualificação ministrada aos soldados do efetivo variável, no âmbito do Exército Brasileiro, nenhum assunto ou dado foi encontrado interligado à Cibernética durante à formação básica.

Notabiliza-se, de forma a contribuir com o estudo, que, na fase de qualificação do soldados e cabos da arma de Comunicações, a proteção digital também não é abordada no Programa-Padrão de Instrução de Qualificação, havendo somente

menção ao estudo sobre informática, em que objetiva-se o conhecimento de componentes de um computador e instalações de periféricos.



15. INFORMÁTICA				TEMPO ESTIMADO DIURNO: 20 h	
	OBJETIVOS INDIVIDUAIS DE INSTRUÇÃO (OII)			ORIENTAÇÃO PARA INTERPRETAÇÃO	
	TAREFA	CONDIÇÃO	PADRÃO-MÍNIMO	SUGESTÕES PARA OBJETIVOS INTERMEDIÁRIOS	ASSUNTOS
Q-401 (HT)	Identificar os principais periféricos e acessórios do microcomputador.	Apresentados um microcomputador com os periféricos e os acessórios existentes na OM.	O militar deverá reconhecer e identificar corretamente cada periférico e cada acessório apresentado.	- Identificar os dispositivos de entrada e saída de dados; - Identificar os botões e portas da unidade de sistema; - Distinguir os diversos cabos de alimentação e de dados; - Identificar acessórios. - Descrever, sumariamente, o funcionamento de um microcomputador. - Demonstrar aptidão para o cumprimento da tarefa constante do OII.	1. Microcomputador a. Generalidades b. Constituição básica c. Princípios de funcionamento d. Microprocessador e. Unidade de armazenamento principal e secundária f. Memórias g. A linguagem da informática (termos empregados na área) 2. Periféricos e acessórios a. Generalidades b. Características c. Tipos d. Finalidades
Q-402 (HT)	Preparar o microcomputador para funcionamento.	Apresentados um microcomputador com os periféricos e os acessórios desconectados.	O militar deverá: - realizar a ligação dos cabos de alimentação e de dados; - fazer a conexão dos periféricos e acessórios; e - verificar aterramento e voltagem. - realizar os testes de funcionamento.	- Conectar os cabos do monitor. - Conectar os cabos da impressora. - Ligar os cabos do teclado e do "mouse"(dispositivo de apontamento). - Ligar o cabo de rede. - Fazer a verificação do aterramento e da voltagem. - Ligar os cabos de alimentação do microcomputador e dos periféricos no estabilizador de energia. - Testar o dispositivo. - Demonstrar aptidão para o cumprimento da tarefa constante do OII.	3. Instalação a. Definições b. Instalações c. Ligações d. Testes

33.00

Quadro 7 – Assuntos da matéria informática presentes na formação dos cabos e soldados de Comunicações do Exército Brasileiro .
Fonte: PROGRAMA-PADRÃO DE QUALIFICAÇÃO DO SOLDADO E CABO DE COMUNICAÇÕES DO EXÉRCITO BRASILEIRO, 2020, pág 33.

No que diz respeito à formação dos soldados da Marinha do Brasil, observa-se que não há dados que autentiquem o ensino da Cibernética aos soldados recrutas. Todavia, como no Exército Brasileiro, a Diretoria de Comunicações e Tecnologia da Informação da Marinha ministra cursos de defesa cibernética para seu efetivo concursado lotado nos Centros Locais de Tecnologia da Informação, bem como os que atuam em Defesa Cibernética Naval (ASSIS, 2019).

Em relação à Organização do Atlântico Norte, a formação, na área cibernética, como já citada anteriormente, é realizada pelo *NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE,* com cursos ministrados na capital da Estônia, Tallin ou de forma online.

Nota-se que os estágios e cursos lecionados aos representantes dos países membros da Organização não são delimitados aos postos ou graduações, podendo ser realizados por qualquer membro das Forças Armadas pertencentes aos países integrantes da OTAN, inclusive recrutas.

Como forma de destacar tal fato, abaixo segue a grade curricular de um curso ministrado pelo *NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE* sobre a conscientização de defesa cibernétca, em que o público alvo é qualquer usuário das redes relacionadas às Forças Armadas pertencentes à OTAN.

Cyber Defence Awareness e-Course (ADL 076)

Date: On demand.

Course fee: free.

Course Aim

To complement the courses offering, the Centre provides an online web-based course on cyber defence awareness, the last update of the course was published in June, 2019.

This course is open to all individuals from Sponsoring Nations, Contributing Participants and NATO; and it can be accessed through the NATO e-Learning Joint Advanced Distributed Learning Portal.

The Cyber Defence Awareness e-Learning course aims to enhance the general user's awareness of cyber security risks and measures to mitigate those risks.

Learning Objectives

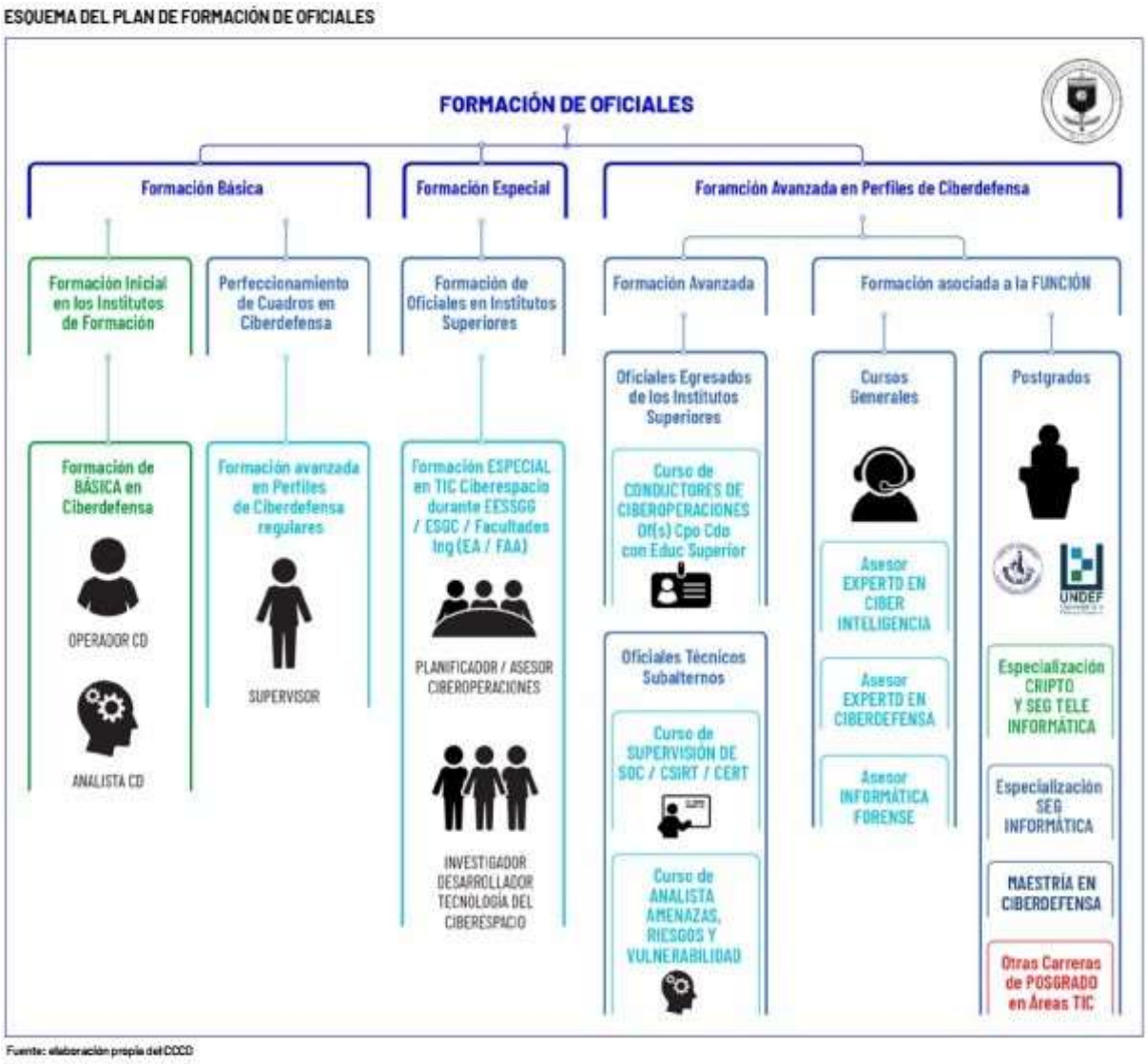
This course provides an introduction to general cyber security in order to aid familiarisation with attacks, terminology and defensive techniques. It gives an overview of the recent threat landscape.

Target Audience

The Cyber Defence Awareness e-course was developed with the goal of raising the awareness of the average user within the NATO community, covering the most relevant topics in the area. The training audience includes all users of NATO networks.

Quadro 8 – Público – alvo definido em curso ministrado pelo *NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE.*
Fonte: NATO CCDCOE TRAINING CATALOGUE, 2022, pág 47.

No Exército da Repúbica Argentina, foi verificado, em relação ao assunto em estudo, que, da mesma forma que no Exército Brasileiro, não há instruções previstas sobre cibernética aos soldados recrutas. Sobre a formação de militares argentinos no âmbito digital, atualmente, existe um estudo, desenvolvido pelo *Comando Conjunto de Ciberdefensa,* para o desenvolvimento de uma carreira técnica de *oficiales y suboficiales* na área digital, focada no emprego de ações militares. (MOYANO, 2020).



Quadro 9 – Estudo do plano de formação de oficiais argentinos especializados em cibernética elaborado pelo *Comando Conjunto de Ciberdefensa de la Argentina.*
Fonte: *La república argentina y sus esfuerzos en ciberdefensa el compromiso con las buenas prácticas como parte de su ideario*, 2020, pág 57.

De posse dos dados apresentados, é possível concluir que o Exército Brasileiro, assim como exige a sua legislação, realiza instruções sobre a objeto em

questão. No entanto, a matéria é explorada em cursos específicos, sendo que tais só permitem a matrícula de sargentos, subtenentes ou oficiais.

Por conseguinte, analisando outras Forças Armadas estrangeiras, verifica-se que a Força Terrestre da Argentina não possui, na formação do soldado recruta, instruções sobre proteção digital, somente a OTAN, que ministra cursos na área, através de seu centro de ciberdefesa, para todos os militares, não havendo restrição em relação ao posto ou graduação nas capacitações sobre o assunto em estudo.

5. DISCUSSÃO DOS RESULTADOS

Nesse momento, após realização do estudo dos conceitos atinentes aos objetivos delimitados previamente e ter-se realizada a coleta de dados por meio de pesquisas bibliográficas, será demonstrado quais foram os resultados obtidos e sua influência no problema manifesto.

5.1 O ENSINO DA CIBERNÉTICA NO EXÉRCITO BRASILEIRO

Após a coleta dos dados, verificou-se que, no âmbito castrense, existe, atualmente, cursos e estágios com a finalidade de explorar o assunto cibernética. Tal fato destaca a busca pelo aperfeiçoamento e o preparo da Força Terrestre do Brasil em relação aos novo atores presentes na globalização.

Contextualizando tais informações apresentadas, observou-se dois centros dedicados ao estudo da defesa digital, o Centro de Instrução de Guerra Eletrônica e a Escola de Inteligência do Exército, os quais apresentam cursos de aperfeiçoamento na área da proteção digital, a fim de preparar militares para atuar, no espectro cibernético.

Assistindo o tema, cita-se que a criação, numa estrutura física do Exército Brasileiro, da Escola Nacional de Defesa Cibernética em 2017, que, atualmente, disponibiliza alguns cursos, de livre acesso, na modalidade ensino a distância, na área da proteção digital, buscando disseminar, entre militares e civis, a importância da segurança cibernética.

Como verificado acima, o assunto cibernética é explorado na escolas especializadas do Exército Brasileiro, possuindo Centros destinados à proteção digital, com capacidade de fomentar e especializar os integrantes da caserna no quesito em estudo.

5.2 O ENSINO DA SEGURANÇA DIGITAL AOS SOLDADOS DO EFETIVO VARIÁVEL

Analisando os cursos dos órgãos destinados à instrução cibernética, pode-se verificar que tais somente podem ser realizados por oficiais, subtenentes e sargentos. Nota-se, também, que o objetivo da formação de tais preleções é a utilização do discente num aquartelamento vocacionado à área digital.

Dessa forma, verifica-se que tal fato restringe a expansão do conhecimento aos soldados do efetivo variável, pois os militares possuidores do conhecimento não participam novamente das rotinas dos aquartelamentos que não são especializados em segurança digital.

Conjuntamente com as análises já citadas, observa-se que a capacitação dos soldados do efetivo variável em proteção digital, torna-se deficitária, tendo em vista que os oficiais e praças detentores do conhecimento exercem suas especializações em Organizações Militares distintas.

Sobre o programa de formação do soldado do efetivo variável, percebe-se que não há menção ou exploração do assunto no seu arcabouço literário, o que dificulta, ainda mais, a exploração da matéria ou assunto correlacionado ao tema.

Por fim, assevera-se que o ensino do assunto cibernética é algo essencial na formação do soldado do efetivo variável, pois devido à utilização de forma de cotidiana dos meios digitais nos quartéis castrenses, o ensino da utilização de forma segura e eficientes dos meios digitais deve ser algo explorado, conforme já determinado nas Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército.

5.3 A CIBERNÉTICA NA FORMAÇÃO DOS SOLDADOS DO EFETIVO VARIÁVEL

Ao realizar o estudo sobre o ensino do assunto cibernética na educação militar do soldado recruta, percebe-se que existe oportunidades de aperfeiçoamento nas instruções ministradas atualmente. Tendo em vista os arcabouços legislativos existentes no Exército Brasileiro determinando a exploração do assunto segurança digital nos aquartelamentos castrenses, como a IG 20-19 e a NORTI, e a grande quantidade de ataques cibernéticos sofridos pelo Brasil, torna-se necessário o

aprimoramento da educação digital dos novos militares, para o uso adequado e seguro dos meios eletrônicos com conexão à internet, no ambiente bélico.

Conforme já investigado, percebe-se que tal assunto não é explorado, ainda, no meio naval brasileiro como no Exército Argentino, todavia, entre os países pertencentes à Organização do Tratado do Atlântico Norte, a matéria em estudo é de suma importância, sendo criado o Centro de Excelência em Cyberdefesa, com o objetivo de aprimorar e capacitar os militares em cibernética.

Explorando o Centro de Excelência em Cyberdefesa da OTAN, destaca-se que os treinamentos existentes preparam os recrutas, com medidas básicas de segurança digital, como os militares que trabalham na área de exploração do campo cibernético, demonstrando, assim, o amplo alcance educacional da escola.

Considerando que na Força Terrestre Brasileira os cursos cibernéticos são ministrados somente para praças e oficiais selecionados, que trabalharão no estudo do espaço digital, percebe-se que existe a necessidade de expansão de tal conhecimento a outros graus hierárquicos.

Como forma de expansão e enriquecimento educacional, existe a possibilidade do assunto ser adotado no Programa – Padrão de Individual Básica, pois a formação ali presente é destinada aos soldados do efetivo variável recém incorporados do meio civil e que, ainda, não participam das atividades rotineiras dos quartéis.

Cita-se, também, que o estudo presente no desenvolvimento militar do recruta proporcionará uma forma de fomento do assunto, já que tais militares poderão permanecer naquela organização castrense até oito anos após o seu alistamento.

Em relação aos assuntos a serem explorados e utilizados no Programa – Padrão de Individual Básica, sobre cibernética, pode-se utilizar como fundamento ou parâmetro, a cartilha já disponibilizada pelo Departamento de Ciência e Tecnologia do Exército, onde são abordadas medidas de forma objetivas e claras que diminuem, de forma substancial, a exposição de ativos tecnológicos da unidade militar à internet.

8.3.2 Desconsiderar **todos os *e-mails*** de supostas instituições bancárias ou governamentais, solicitando atualização de cadastro ou instalação de programas;

8.3.3 Ficar atento a *e-mails* ou telefonemas solicitando dados pessoais (números de cartão, senhas, etc.) ou dados sobre a tecnologia que está sendo utilizada (sistema operacional, antivírus, etc.).

Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

2.6 Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. Os cadastros de usuários que acessam os sistemas devem ser **mantidos atualizados e supervisionados pela contra-inteligência da OM.**

2.7 Estabelecer uma política clara e supervisionada relativa ao **descredenciamento** de usuários que tenham sido transferidos de OM ou de função.

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

3 COMPUTADORES DA OM

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

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

Quadro 10 – Medidas de Segurança da Informação presentes na Cartilha Emergencial de Segurança do Departamento de Ciência e Tecnologia.

Fonte: Cartilha Emergencial de Segurança de Tecnologia da Informação do Departamento de Ciência e Teconolgia, 2011, pág 12.

6. CONCLUSÃO

A Guerra Cibernética é, atualmente, um dos principais modais utilizados para a obtenção e captura de informações. Dentro desse contexto, o Brasil é um dos países que mais sofrem ataques digitais, podendo ser observado diversos ataques que ocasionam vazamentos de informações privadas ou indisponibilizam algum serviço. Não obstante, com o avanço da virtualização, é importante que o Exército Brasileiro esteja em condições de salvaguardar suas informações e dados de forma segura. Diante do enriquecimento tecnológico, o Exército Brasileiro, também, desenvolveu-se. Salienta-se que tal fato não ocorreu somente na gestão de informações, mas também no arcabouço legal, de maneira que fosse estabelecido normas e instruções de como devem ser realizadas as ações digitais num ambiente castrense e os cuidados que devem ser tomados ao manusear materiais da Força Terrestre no ciberespaço.

Todavia, para que haja a instauração dessas medidas, é necessário os militares do Exército Brasileiro tenham conhecimento e sejam instruídos, por meio dos planos de instrução básica ou de qualificação, sobre as diversas medidas estabelecidas.

Dentro de tal universo, sobrepuja-se os soldados recrutas, os quais apresentam pouco conhecimento sobre segurança digital e, durante as atividades cotidianas da caserna, utilizam computadores ou operam, de forma particular, seus meios digitais, numa área militar.

Pela conjuntura apresentada, foi formulado o seguinte problema: O Exército Brasileiro, atualmente, consegue capacitar e expandir os conhecimentos atinentes à Segurança da Informação aos soldados recém-ingressos na Força Terrestre, por meio do Programa – Padrão de Instrução Individual Básica?

Com o objetivo de ser alcançado uma possível solução para o problema, foi necessário coletar dados em manuais doutrinários, leis nacionais e internacionais vigentes, artigos científicos e publicações periódicas que abordam o assunto cibernética e segurança digital no contexto da defesa e soberania nacional.

Após a tabulação dos dados coletados e suas análises, foi observado a ausência de instruções atinentes à proteção digital no Programa – Padrão de Instrução Individual Básica e será apresentada as implicações decorrentes da ausência da matéria proteção digital na formação do soldado recruta do Exército Brasileiro:

Exposição de dados sensíveis da Organização Militar na internet, tendo em vista que as informações podem ser expostas com a negligência de simples ações, como o acesso a um determinado *e-mail* de origem desconhecida.

Inutilização de sistemas, pois o acesso indevido ou a utilização de mídias removíveis constituídos por códigos maliciosos podem danificar os dados de um *software*, acarretando, dessa forma, a paralização de um determinado programa.

Desgaste na imagem do Exército Brasileiro, visto que, ao sofrer um ataque cibernético que gere inutilização de sistemas, vazamentos de dados ou outros efeitos, a Força Terrestre tem a sua reputação de proteger-se digitalmente afetada, gerando desconfiança na população civil sobre a sua capacidade atual de defender-se num possível conflito.

Diante disso, foi levantada as possíveis formas de ensino sobre proteção digital presentes, atualmente, no Exército Brasileiro, na Marinha do Brasil e em outras nações, chegando à conclusão que, na Força Terrestre, é ministrado o assunto em cursos para sargentos, subtenentes e oficiais, não contemplando, assim, os soldados recrutas.

Foi observado, também, que na Marinha do Brasil e no Exército Argentino, não há instruções sobre o assunto aos recrutas, somente, há cartilhas de orientação com medidas a serem tomadas a fim mitigar possíveis ataques cibernéticos.

Em relação aos países que compõe a Organização do Tratado do Atlântico Norte, existe instruções, inclusive para recrutas sobre cibersegurança, a fim de todos possam usufruir de uma capacitação na área e reduzam as chances de possíveis contratempos.

Portanto, foi possível identificar que não há, atualmente, instruções sobre cibersegurança previstas ao soldado recruta como também existe a necessidade de que seja atualizado o Programa – Padrão de Instrução Individual Básica, com a possível inclusão de matérias sobre proteção digital, tendo, como sugestão de

assuntos, a cartilha emergencial de segurança de tecnologia da informação e comunicações, elaborada pelo Departamento de Ciência e Tecnologia do Exército, em que são elencadas medidas de proteção digital a serem realizadas numa Organização Militar pertencente ao Exército Brasileiro.

: _____
Atilla Rodrigo Pereira Silva - Cap

REFERÊNCIAS

ABDALLA Jofre Ferreira. **A Atuação do Exército Brasileiro para o domínio do espaço cibernético.** Revista do Exército Brasileiro,2021.

ANDRADE Henrique. **Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar**. 10 dez. 2021. Disponível em: <https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/>. Acesso em: 10 mar.2022.

ANDRADE Luiz Claudio Oliveira. **O uso do Big Data na prevenção de ataques cibernéticos**. 2020. 46 f. Dissertação (Especialista em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.

ASSIS, Ana. **A Questão da Proteção Cibernética na Marinha: Organização Institucional e Normas.** Revista Brasileira de Estudos de Defesa,2019

BRASIL. Exército. Comando de Operações Terrestres. **EB70-PP-11.011 – INSTRUÇÃO INDIVIDUAL BÁSICA.** Brasília, DF, 2019.

BRASIL. Exército. Comando de Operações Terrestres. **EB70-PP-11.024 – Instrução de qualificação do cabo e do soldado de comunicações.** Brasília, DF, 2020.

BRASIL. Exército. Comando de Operações Terrestres. **SISTEMA DE INSTRUÇÃO MILITAR DO EXÉRCITO BRASILEIRO.** Brasília, DF, 2019.

BRASIL. Exército. Departamento de Educação e Cultura do Exército. **Catálogo de Cursos do Departamento de Educação e Cultura do Exército.** Rio de Janeiro, RJ, 2019.

BRASIL. Exército. **Plano estratégico do Exército 2020-2023**. Brasília, DF, p.20, dez. 2019.

BRASIL. Exército. PORTARIA Nº 483, DE 20 DE SETEMBRO DE 2001. IG 20-19 - Instruções Gerais de Segurança da Informação para o Exército Brasileiro. **Boletim do Exército**, Brasília, DF, 2001.

BRASIL. Exército. PORTARIA Nº 720, DE 21 DE NOVEMBRO DE 2011. CARTILHA EMERGENCIAL DE SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES. **Boletim do Exército**, Brasília, DF, 2011.

BRASIL. Exército. PORTARIA Nº 803, DE 30 DE JULHO DE 2014. EB10-IG-01.014- Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro. **Boletim do Exército**, Brasília, DF, 2014.

BRASIL. Marinha. Diretoria de Ensino da Marinha. **Currículo Curso de Formação de Soldados Fuzileiros Navais**, Rio de Janeiro, RJ, 2022.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. 2. ed.: Brasília, DF, 2008.

ESTÔNIA. *NATO*. ***NATIONAL CYBER SECURITY FRAMEWORK MANUAL*****.** 2012.

ESTÔNIA. *NATO*. ***NATO CCDCOE TRAINING CATALOGUE*****.** 2021.

MOYANO Tomás Ramón. **La República Argentina y sus esfuerzos en ciberdefensa. El compromisso con las buenas prácticas como parte de su ideario.** Revista Visión Conjunta,2020.

Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à Internet. **Ministério das Comunicações**, DF, 14 abr. 2021. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet>. Acesso em: 10 mar.2022.

QUEIROZ Vitória. **Brasil é o 5° país mais afetado com ataques cibernéticos em 2021**. 30 jul. 2021. Disponível em: <https://www.poder360.com.br/brasil-e-o-5-pais-mais-afetado-com-ataques-ciberneticos-em-2021/>. Acesso em: 10 mar.2022.