ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

Guilherme da Silva Pereira

FIREWALL GNU/LINUX E IPTABLES : UM ESTUDO DE IMPLEMENTAÇÃO DE ENSINO NO PLANO DE DISCIPLINA DA FORMAÇÃO DO OFICIAL DE CARREIRA DE COMUNICAÇÕES

Resende
2019

Guilherme da Silva Pereira

FIREWALL GNU/LINUX E IPTABLES : UM ESTUDO DE IMPLEMENTAÇÃO DE ENSINO NO PLANO DE DISCIPLINA DA FORMAÇÃO DO OFICIAL DE CARREIRA DE COMUNICAÇÕES

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

Orientador(a): Ten **Gustavo Henrique** Bastos da Mota

Resende
2019

Guilherme da Silva Pereira

FIREWALL GNU/LINUX E IPTABLES: UM ESTUDO DE IMPLEMENTAÇÃO DE ENSINO NO PLANO DE DISCIPLINA DA FORMAÇÃO DO OFICIAL DE CARREIRA DE COMUNICAÇÕES

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

Aprovado em ____ de _____ de 2019.

Banca examinadora:

Gustavo Henrique Bastos da Mota – Ten
Orientador

Allanderson Rodrigues Teixeira – Maj
Avaliador

Fernando Pazzinato – Cap
Avaliador

Resende
2019

A meus familiares, amigos e mentores que me apoiaram e acreditaram em meu potencial desde o princípio.

AGRADECIMENTOS

Nenhuma grande meta ou sonho é realizado por um indivíduo isolado. Nestes cinco anos de formação e mais os que antecederam durante minha preparação, tenho a agradecer a todos que contribuíram para que chegasse onde estou.

Meus pais José Carlos Pereira e Keili Cristina da Silva Pereira, que sempre foram os melhores pais que poderia pedir e fizeram o possível e o impossível para que eu e meu irmão sempre tivéssemos as melhores condições e nunca carregássemos nossos fardos sozinhos e foram, sem dúvidas, os pilares centrais para meu desenvolvimento e crescimento pessoal, meu irmão de sangue Carlos Henrique da Silva Pereira, figura que sempre me espelhei pelo seu exemplo de caráter e serenidade para lidar com as mais difíceis situações.

Aos amigos distantes, que a intensa vida viajando pelo país trouxe, em especial aos oito que estiveram comigo desde o ensino médio e hoje são presenças constantes em minha vida, tanto para os momentos de alegria e festejo, quanto para os momentos de tristeza ou trabalho árduo. O que veio de uma união por nosso gostos em comum ocasionou em laços tão fortes que hoje posso chamá-los de irmãos e considerá-los como parte de minha família, o suporte e compreensão de todos vocês certamente foi essencial durante esse período intenso de formação.

Também aos irmãos de farda que, juntamente comigo, suportaram as piores dificuldades e os mais intensos desafios em todos os cinco anos partilhando do mesmo ambiente e sempre motivando-nos uns aos outros, a convivência da caserna jamais será esquecida e a camaradagem e companheirismo serão levados para toda minha vida.

Todos meus professores, instrutores e mentores já que cada um em sua área e da sua maneira proveram os conhecimentos, valores e ferramentas para que pudesse transformar meus sonhos e aspirações em realidade. Além disso aos familiares por todo o Brasil, que nas rápidas visitas e encontros sempre me proveram apoio e incentivo.

E por fim a todos os muitos outros que torceram pelo meu sucesso e de alguma maneira contribuíram ou me auxiliaram, os trabalhos mais silentes, por vezes são os de maior relevância.

Palavras não são suficientes para exaltar a gratidão que tenho por cada um de vocês, obrigado!

RESUMO

FIREWALL GNU/LINUX E IPTABLES : UM ESTUDO DE IMPLEMENTAÇÃO DE ENSINO NO PLANO DE DISCIPLINA DA FORMAÇÃO DO OFICIAL DE CARREIRA DE COMUNICAÇÕES

AUTOR: Guilherme da Silva Pereira
ORIENTADOR: Ten Com Gustavo Henrique Bastos da Mota

A informatização do Exército Brasileiro e de seus sistemas acarretaram na adesão aos softwares livres, exigindo de seus agentes uma constante capacitação visando as novas ameaças do espaço cibernético. A correta operação e domínio de um firewall e suas ferramentas pode significar o sucesso de uma operação e uma gestão eficiente de meios. Este trabalho teve como objetivo avaliar a necessidade e a possibilidade de implementação do ensino do firewall dos sistemas GNU/Linux e sua ferramenta IPTables no Curso de Comunicações da Academia Militar das Agulhas Negras. A pesquisa foi realizada através de estudos documentais e bibliográficos, após isso elaborou-se um questionário para assim obter-se o perfil de cada uma das turmas que compõe o Curso de Comunicações, com estas informações analisou-se os atuais Planos de Disciplina do Curso visando obter seus pontos fortes e oportunidades de melhoria. Os resultados das pesquisas de campo indicaram que uma considerável parcela dos Cadetes desconhecem os conceitos básicos de firewall, não se sentem aptos a configurar e operar estes sistemas e concordam que a carga horária e os conteúdos são insuficientes, a análise do Plano de Disciplina do Curso evidenciou que a unidade sobre firewall é vaga, pouco especifica e seu aprendizado não é progressivo. Comprovou-se a necessidade de modificações e implantação destes assuntos, com isso foram propostas as modificações, os tópicos a serem inseridos e suas competências. Os levantamentos realizados e ideias contidas neste trabalho podem acarretar mudanças significativas na mentalidade de segurança da informação e proteção cibernética dos futuros Oficiais de Comunicações e devem continuar a ser estudados e aprofundados em melhor espaço de tempo e meios como forma de investimento no futuro do Exército Brasileiro.

Palavras-chave: Firewall, IPTables, AMAN, Cibernética, Segurança da Informação

ABSTRACT

FIREWALL GNU / LINUX AND IPTABLES: AN IMPLEMENTATION STUDY IN THE TEACHING OF THE DISCIPLINE PLAN FOR THE TRAINING OF THE SIGNALS CAREER OFFICER

AUTHOR: Guilherme da Silva Pereira
ADVISOR: Ten Com Gustavo Henrique Bastos da Mota

The computerization of the Brazilian Army and its systems led to the adhesion to free software, requiring its agents to constantly train in the new threats of cyberspace. The correct operation and control of a firewall and its tools can mean the success of an operation and an efficient management. This paper aimed to evaluate the need and the possibility of implementing the teaching of the GNU / Linux system firewall and its IPTables tool in the Signals Course of the Agulhas Negras Military Academy. The research was carried out through documentary and bibliographic studies, after which a questionnaire was elaborated to obtain the profile of each of the classes that compose the Signals Course, with this information the current Course Discipline Plans were analyzed aiming to obtain their strengths and opportunities for improvement. The results of the field surveys indicated that a considerable portion of Cadets are unaware of the basics of firewall, do not feel able to configure and operate these systems and agree that the workload and contents are insufficient, the analysis of the Course Discipline Plan evidenced that the topic about firewall is vague, little specific and its learning is not progressive. It was verified the need for modifications and implementation of these subjects, thereby the modifications, the topics to be inserted and their competences were proposed. The surveys and ideas contained in this paper may lead to significant changes in the information security mentality and cybernetic protection of future Signals Officers and should continue to be studied and deepened in a better space of time and means as an investment in the future of the Army Brazilian.

Keywords: Firewall; IPTables; AMAN; Cybernetics; Information Security

LISTA DE QUADROS

Quadro 1 – Unidade VI: Firewall……..……36
Quadro 2 – Unidade I: Guerra Cibernética……...……37
Quadro 3 – Unidade II: Hardening de Sistemas Operacionais…….37
Quadro 4 – Unidade III: Hardening de Servidores...……38
Quadro 5 – Assuntos propostos para complementação no PLADIS……39

LISTA DE GRÁFICOS

Gráfico 1 – Idade dos cadetes de Comunicações 2019…….27
Gráfico 2 – Cadetes que realizaram o questionário……..28
Gráfico 3 – Item 2 – 2° Ano……..……29
Gráfico 4 – Item 2 – 3° Ano……..……29
Gráfico 5 – Item 2 – 4° Ano……..……29
Gráfico 6 – Item 2 – Total……..……...29
Gráfico 7 – Item 3 – 2° Ano……..30
Gráfico 8 – Item 3 – 3° Ano……...……...30
Gráfico 9 – Item 3 – 4° Ano……..……31
Gráfico 10 – Item 3 – Total……..…….31
Gráfico 11 – Item 4 – 2° Ano……..……..32
Gráfico 12 – Item 4 – 3° Ano……..……..32
Gráfico 13 – Item 4 – 4° Ano……..……..32
Gráfico 14 – Item 4 – Total……..…….32
Gráfico 15 – Item 5 – 2° Ano……..……..33
Gráfico 16 – Item 5 – 3° Ano……33
Gráfico 17 – Item 5 – 4° Ano……..……..33
Gráfico 18 – Item 5 – Total……..…….33
Gráfico 19 – Item 6 – 2° Ano……..……..34
Gráfico 20 – Item 6 – 3° Ano……..……..34
Gráfico 21 – Item 6 – 4° Ano……..……..34
Gráfico 22 – Item 6 – Total……..…….34
Gráfico 23 – Item 7 – 2° Ano……..……..35
Gráfico 24 – Item 7 – 3° Ano……..……..35
Gráfico 25 – Item 7 – 4° Ano……..……..36
Gráfico 26 – Item 7– Total……..……..36

LISTA DE ABREVIATURAS E SIGLAS

AMAN	Academia Militar das Agulhas Negras
EME	Estado Maior do Exército
EsPCEx	Escola Preparatória de Cadetes do Exército
LDAP	Lightweight Directory Access Protocol
PLADIS	Plano de Disciplina
PLANID	Plano Integrado de Disciplina
VoIP	Voice over Internet Protocol(Voz sobre o Protocolo da Internet)

LISTA DE ANEXOS

ANEXO A – MODELO DE FORMULÁRIO APLICADO…….44

SUMÁRIO

1 INTRODUÇÃO.....13
1.1 PROBLEMA.....14
1.2 DELIMITAÇÃO DO PROBLEMA DE PESQUISA.....15
1.3 OBJETIVOS.....15
1.3.1 Objetivo geral.....15
1.3.2 Objetivos específicos.....15
1.4 HIPÓTESE.....15
1.5 JUSTIFICATIVA.....16
1.6 ORGANIZAÇÃO DO TRABALHO.....17
2 REFERENCIAL TEÓRICO.....18
2.1 REVISÃO DA LITERATURA E ANTECEDENTES DO PROBLEMA.....18
2.1.1 O Ensino de Cibernética no Curso de Comunicações.....18
2.1.2 GNU/LINUX.....19
2.1.3 Redes de Computadores.....20
2.1.4 Segurança da Informação.....20
2.1.5 Firewall.....21
2.1.6 Netfilter.....22
2.1.7 IPTables.....22
3 METODOLOGIA.....24
3.1 ESTATÍSTICA.....26
4 RESULTADOS E ANÁLISES DOS DADOS.....27
4.1 RESULTADOS E ANÁLISE DA PESQUISA DE CAMPO.....27
4.1.1 Item 1 – Dados dos Cadetes de Comunicações.....27
4.1.2 Item 2 – Noção do Conceito e Serventia de um Firewall.....29
4.1.3 Item 3 – Contato prévio e Práticas com Sistemas de Firewall.....30
4.1.4 Item 4 - Noção Básica do que é IPTables.....31
4.1.5 Item 5 – Opinião Sobre a Relevância dos Conhecimentos de Segurança de Redes.32
4.1.6 Item 6 – Suficiência dos Conteúdos e Carga Horária de Segurança de Redes/Firewalls.....33

4.1.7 Item 7 - Opinião sobre a Aptidão a Gerenciar um Firewall e Prover a Segurança de Redes……35
4.2 RESULTADO E ANÁLISE DA PESQUISA DOCUMENTAL E BIBLIOGRÁFICA..…36
4.2.1 Análise do PLADIS de Cibernética……..…..…36
4.2.2 Proposta de implementação e alteração do PLADIS……..…38
5 CONSIDERAÇÕES FINAIS.....40
REFERÊNCIAS.....42
ANEXO A – MODELO DE FORMULÁRIO APLICADO.....44

1 INTRODUÇÃO

O constante e exponencial desenvolvimento das tecnologias da informação acarretaram no final do século XX em uma completa revolução na forma como resolvemos problemas, executamos trabalhos e, principalmente como vemos e interagimos com o mundo ao redor, o desenvolvimento da informática e das redes de computadores possibilitaram uma comunicação eficiente, praticamente instantânea, com qualquer ponto do globo. Toda esta rapidez expandiu as capacidades desse sistema de forma que todo o modo de vida foi modificado e pouco a pouco se tornasse completamente dependente destas tecnologias.

O cenário atual está integrado com a Internet de uma forma nunca antes vista. A enorme quantidade de informações pessoais divulgadas e a exposição constante se tornou normalidade em redes sociais, fato que não expressa grande surpresa ao se avaliar que documentos, transações bancárias e uma considerável parte da vida da população informatizada está nas redes de computadores. O meio cibernético, assim como a vida real é, praticamente, de acesso público, bastando apenas um dispositivo que acesse essas redes e uma conexão. O adicional das redes virtuais é a facilidade de manter-se anônimo durante as interações, isto acaba por ocasionar em um ambiente extremamente hostil de alto risco até para os indivíduos mais experientes e com maior conhecimento, ocasionando diariamente inúmeras vítimas de golpes, fraudes e crimes virtuais.

A segurança nas redes de computadores tem ganhando tanta importância que se tornaram motivos de segurança de estado, tendo em vista os riscos que pequenas falhas em sistemas governamentais ou de grandes empresas podem acarretar na gestão de recursos, administração de sistemas das forças armadas ou sistemas sensíveis, como usinas hidrelétricas ou nucleares, que caso falhem acarretariam em danos incalculáveis além da perda de vidas inocentes, tudo apenas ao pressionar de um botão do outro lado do planeta.

Por isso é notável a importância e domínio dos conhecimentos a cerca da segurança e proteção cibernética de forma que o Oficial de Comunicações como gestor de recursos públicos, perito e, da linha de ensino militar bélico, aquele tem apresenta maiores responsabilidades no que tange o domínio de conhecimentos na área da cibernética.

O Oficial de Comunicações deve aprimorar-se constantemente sobre esses assuntos e implementar medidas eficientes de forma a não negligenciar sua segurança pessoal, dos serviços que porventura gerenciar em sua OM. Para tal se faz necessário a avaliação da relevância e após isso a suficiência de conhecimentos que o Oficial deve possuir para empregar a ferramenta de

configuração do firewall, o IPTables, sendo esta ferramenta utilizada para gerenciar redes e proteger os sistemas sob sua responsabilidade.

A relevância de levantar tais pontos com esta pesquisa foge o escopo meramente institucional e curricular, sendo uma questão de segurança mínima que aliada a mentalidade coletiva de prevenção a falhas de segurança poderá poupar diversos problemas nas Organizações Militares. É importante citar que esses conhecimentos adquiridos e aprimorados servem tanto para a finalidade específica do bom uso do firewall em si, mas abrangem também um domínio maior de conhecimentos em redes de computadores, no geral, e no próprio uso do sistema operacional GNU/Linux, tudo isso além de estimular a solução de problemas e estimular a mentalidade preventiva, capacita melhor o pessoal que integra a operação e administração dos sistemas informacionais do Exército Brasileiro.

O seguinte trabalho busca analisar os conteúdos ministrados durante o curso de Comunicações na AMAN, no escopo da área de Cibernética e as possibilidades de emprego do Oficial no corpo de tropa em relação a segurança de redes e utilização de firewall. Tendo esta temática, o trabalho tem a finalidade de propor melhorias no ensino dos cadetes e adequar estes as necessidades do gerenciamento e manutenção de redes utilizando a ferramenta IPTABLES.

O Oficial como gestor público tem por obrigação garantir que os recursos que lhe forem destinados tenham bom funcionamento e sejam empregados de maneira segura.

Baseando-se nesses aspectos e somando-se a atual situação do ensino no Curso de Comunicações é notável a defasagem e a ausência de conhecimentos essencias nos assuntos de rede e segurança em firewalls que serão conhecimentos diferenciais no preparo de subordinados e gestão dos sistemas informatizados do Exército Brasileiro, além de representar falha grave na segurança de redes tanto em operações quanto no dia-dia nos corpos de tropa.

Tendo o Oficial de Comunicações carga elevada de instruções na área de Cibernética, este deve ser fator diferencial e fonte propagadora de conhecimentos nas OM em que estiver servindo.

1.1 PROBLEMA

Considerando o atual Plano de Disciplina (PLADIS) e assuntos ministrados durante o Curso de Comunicações na área de segurança de redes, se faz necessário um maior aprofundamento em firewalls e o domínio da ferramenta IPTables?

1.2 DELIMITAÇÃO DO PROBLEMA DE PESQUISA

Sendo o tema: “Implementação do ensino do firewall GNU/Linux e IPTables no PLADIS da formação do oficial de carreira de comunicações” inserido na população: cadetes do Curso de Comunicações; na abordagem: quantitativa; no tempo: ano de 2019; no espaço: Academia Militar das Agulhas Negras(AMAN); acompanhado da pesquisa e revisão bibliográfica acerca dos documentos e normas que servem como base para o planejamento das instruções de cibernética.

1.3 OBJETIVOS

1.3.1 Objetivo geral

Estudar e verificar a necessidade da implementação do ensino do firewall GNU/Linux e IPTables no PLADIS da formação do oficial de carreira de comunicações.

1.3.2 Objetivos específicos

a) Identificar o perfil das turmas de Cadetes de Comunicações e os principais problemas que estes possuem nos assuntos de firewall e IPTables.

b) Levantar as deficiências e problemas no ensino e aprendizagem da cadeira de Cibernética no Curso de Comunicações baseado na bibliografia estudada.

c) Analisar o PLADIS de Cibernética do Curso de Comunicações, obtendo-se os principais pontos fortes e oportunidades de melhoria.

d) Apresentar uma proposta de assuntos a serem inseridos e modificações a serem realizados no PLADIS de Cibernética do Curso de Comunicações, baseando-se nas ideias e conceitos apresentados por João Eriberto, em seus livros e artigos, e por Uruban Neto em seu livro Dominando Linux Firewall IPTables.

1.4 HIPÓTESE

H_1: O atual PLADIS da disciplina de Cibernética se mostra completo e suficiente para que o Cadetes se sintam aptos para operar e gerenciar sistemas firewall GNU/Linux e a ferramenta IPTables.

H_2: O atual PLADIS da disciplina de Cibernética no Curso de Comunicações se mostra incompleto, quanto aos sistemas de firewall GNU/Linux e a ferramenta IPTables, perante as necessidades e funções de estabelecimento da segurança mínima de uma rede e por isso os Cadetes não se sentem aptos a operar um firewall.

1.5 JUSTIFICATIVA

O Oficial de Comunicações, como detentor do conhecimento e maior capacitação na área de Cibernética de todo efetivo formado na AMAN, visto que a grade curricular inclui disciplinas que vão até Cibernética V(BRASIL,2019, p. 11), tem por obrigação ser fator diferencial especificamente no quesito de gerenciamento de redes.

Os Oficiais formados na AMAN têm como parte comum atuar como Oficial de Informática incluindo-se nesta função as missões de zelar pela segurança da informação, orientar as atividades ligadas a gerências de redes e o controle dos materiais de informática além do assessoramento ao Comando na gestão da informação(BRASIL, 2016,p. 30).

Isto por si só já seria motivo suficiente para evidenciar a importância e a necessidade de uma maior capacitação de pessoal no tocante aos conhecimentos de gestão, controle e segurança de redes no Exército, já que a função de Oficial de Informática engloba todos esses aspectos.

Quando se trata do Oficial de Comunicações este, especificamente, entre outras atividades, deve estar apto a planejar, coordenar, gerenciar a execução, instalação, operação e manutenção dos Sistemas de Comunicações Táticos da Brigada, sistemas de gerenciamento eletrônico de mensagens e de redes de dados com enlace físico ou sem fio(BRASIL,2016, p. 31).

As funções específicas do Oficial de Comunicações demonstram a carga de responsabilidade que estas carregam consigo tendo em vista que fogem do escopo meramente administrativo das Organizações Militares(que já são de grande importância) e adentram no cenário tático do emprego da força em missões reais nos múltiplos ambientes onde falhas de segurança acarretadas pela má administração, emprego incorreto e deficiente da gerência de redes e dos sistemas de defesa, como o firewall, podem significar em perdas irreversíveis no campo de batalha.

Por isso, esta pesquisa busca evidenciar oportunidades de melhoria na formação do Oficial de Comunicações quanto a segurança de redes e propor formas de implementação e aperfeiçoamento dos assuntos ministrados ao longo do Curso.

1.6 ORGANIZAÇÃO DO TRABALHO

Este trabalho possui cinco capítulos além das referências e o anexo A, os capítulos são: introdução, referencial teórico, resultado e análise de dados e considerações finais. A estruturação dos capítulos está disposta da seguinte maneira:

O primeiro capítulo, que é a introdução, é composto de uma breve apresentação dos assuntos tratados bem como o contexto geral que se insere esta pesquisa, além disso, do problema, delimitação do problema de pesquisa, objetivos (gerais e específicos), hipótese, justificativa e o presente item, organização do trabalho.

O segundo capítulo trata do referencial teórico que evidenciará todo o embasamento norteado pelas bibliografias utilizadas neste trabalho, seguindo desde o ensino de cibernética no Curso de Comunicações, introduzindo os assuntos de GNU/Linux, redes, segurança da informação até os assuntos mais complexos, que compõe o foco da pesquisa, como firewall e IPTables.

O terceiro capítulo é a metodologia, que tem como objetivo evidenciar a forma como foram levantados os dados tanto da pesquisa de campo, quanto da pesquisa documental e bibliográfica, sendo presente também neste capítulo a parte de estatística que explica como foram realizadas as análises e tratamento destes dados obtidos na pesquisa de campo.

O quarto capítulo são os resultados e análises dos dados que trata dos resultados da pesquisa de campo e dos resultados e análises da pesquisa documental e bibliográfica, incluindo todo o estudo dos dados obtidos através do questionário e suas consequências para a pesquisa. Dentro do assunto da pesquisa documental e bibliográfica está o estudo do PLADIS de Cibernética do Curso de Comunicações e as propostas de modificação e implementação neste Plano de Disciplina.

Por fim temos o quinto capítulo que trata das considerações finais acerca deste trabalho bem como suas limitações, sugestões sobre esta temática e conclusão sobre os problemas levantados e objetivos atingidos. Após o quinto capítulo temos as referências utilizadas e o anexo A, que é o modelo do questionário aplicado.

2 REFERENCIAL TEÓRICO

2.1 REVISÃO DA LITERATURA E ANTECEDENTES DO PROBLEMA

2.1.1 O Ensino de Cibernética no Curso de Comunicações

O Curso de Comunicações da AMAN apresenta, dentre diversas disciplinas, a de Cibernética III, IV, V, sendo que estas representam a continuidade dos assuntos ministrados na Escola Preparatória de Cadetes do Exército (EsPCEx) e no primeiro ano da AMAN, Cibernética I e II respectivamente. Nos ateremos neste trabalho somente às cadeiras do Curso de Comunicações.

No 2° Ano as disciplinas integradas a cadeira de Cibernética III incluem seis unidades: Virtualização, Sistema Operacional Debian, Sistema Operacional Microsoft Windows, Redes de Computadores, Redes Wireless e Infraestrutura de Rede(BRASIL,2019).

Esses assuntos servem como base e iniciam o Cadete de Comunicações a ter o contato com virtualização de sistemas, configurações básicas dos Sistemas Operacionais e redes de computadores. Desta forma o PLADIS do segundo ano tem como finalidade apresentar as ferramentas básicas e preparar o Cadete para os próximos anos onde se dará prosseguimento na formação técnica profissional do comunicante.

O 3° Ano apresenta dentro da Cibernética IV as unidades: Elementos de um Sistema de Comunicações, Secure Shell, Sistema Rádio Troncalizados, Lightweight Directory Access Protocol(LDAP), Voice over Internet Protocol(VoIP) e Firewall(BRASIL,2019).

No terceiro ano a complexidade dos assuntos aumenta consideravelmente e, por isso, cabe a correta instrução e aprendizado durante o segundo ano para se ter uma boa base de entendimento mínimo. As instruções do terceiro ano são de essencial importância por incluírem alguns serviços utilizados nas Organizações Militares e nas operações de acordo com o PLADIS, como: o Apache, SSH, Zimbra, OpenLDAP, VoIP e PFSense. Cabe ao Oficial a correta configuração e gestão destes serviços.

No terceiro ano inclui-se o assunto sobre Pfsense que é basicamente um sistema operacional que transforma um computador em um firewall e roteador, sendo uma distribuição FreeBSD(sistema operatório livre tipo unix) poderosa e leve (WILLIANSON, 2012, p. 1). O Pfsense é uma forma de firewall eficiente porém sua configuração depende da instalação de outro sistema operacional(FreeBSD) em uma máquina dedicada somente a isto, sendo um firewall externo ao computador do usuário.

O 4° ano do Curso de Comunicações na disciplina de Cibernética V, a última da matéria Cibernética, apresenta as unidades: Princípios de Guerra Cibernética, Hardening de Sistemas Operacionais e Hardening de Servidores(BRASIL,2019).

As unidades do quarto ano englobam grande parte do quesito segurança da informação e representam parte fundamental dos conhecimentos que o Oficial de Comunicações deve adquirir para prover a segurança das redes, serviços e máquinas à em sua responsabilidade.

2.1.2 GNU/LINUX

Tendo os meios digitalizados e a implementação de tecnologias da informação tomado conta dos sistemas administrativos, torna-se essencial a utilização de computadores como forma de melhorar a eficiência, velocidade administrativa e a flexibilidade dos extensos processos e documentações movidos diariamente no Exército Brasileiro assim como em outras instituições, para tal não basta apenas um hardware, a parte física dos meios computacionais, para se atingir esses objetivos é necessário a parte lógica, o sistema operacional, este constitui-se de um software operando em modo núcleo que gerencia os recursos de hardware que permite o acesso a programas e aplicativos de maneira simples(TANENBAWN; BOS, 2016, p.3).

Com isso tem-se a necessidade da implementação de um sistema operacional, dentre todos no mercado, que possa suprir as demandas com baixo ou até nenhum custo. Grande parte dos softwares do Exército Brasileiro hoje são softwares livres isto se dá ao Plano de Migração para Software Livre no Exército Brasileiro, como declarado:

> a. A adoção da solução livre, ou aberta, é considerada definitiva para todo o Exército Brasileiro. Portanto, a obtenção do índice máximo de sua utilização deve ser um objetivo permanente para todas as Unidades do Exército, em opção à solução fechada, sem ônus à plena operacionalidade das atividades específicas da OM. O prazo para a sua consecução será conforme a disponibilidade de recursos humanos capacitados e habilitados – em particular nas OM não especializadas –, e a cabal compreensão de todos em relação às significativas vantagens, de toda a ordem, da implementação dessa solução. (DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA, 2007, p. 2).

A utilização destes softwares é de grande importância, pois economiza recursos e garante autonomia em relação às licenças que costumavam ser adquiridas mediante contratos que demandavam recursos econômicos valiosos. A implementação do GNU/Linux, especificamente a Distribuição Debian como sistema operacional para o Exército representou um grande avanço e “Cabe ressaltar que o Ministério da Defesa, depois de verificar os sucessos obtidos pelo Exército

Brasileiro, também resolveu implantar o Debian como distribuição para os seus servidores de rede."(ERIBERTO, 2004).

A utilização destes sistemas operacionais, apesar de ser muito flexível e customizável apresenta dificuldade superior a sistemas operacionais pagos que são mais amigáveis aos usuários. Por isso é de essencial importância que todos os militares tenham os conhecimentos mínimos para operar os softwares livres, e cabe ainda mais ao Oficial que instruirá e orientará seus subordinados sobre a utilização de redes e sistemas do Exército Brasileiro.

2.1.3 Redes de Computadores

Redes de computadores são definidas como "[…] dois ou mais computadores, interligados por qualquer meio, capazes de trocar informações entre si e/ou compartilhar recursos de hardware."(ERIBERTO, 2013, p. 38), ou seja, grande parte dos sistemas e documentações do Exército atualmente estão digitalizadas e em rede. As ligações estabelecidas entre os diversos escalões do Exército são essencias, assim como a manutenção e segurança destas ligações.

O domínio dos conhecimentos sobre redes, as noções sobre configuração e segurança são essenciais ao Oficial que poderá ocupar a função de Oficial de Informática, a doutrina diz: "[…]O oficial de informática é o encarregado das redes de informáticas da unidade e o responsável pela eficiência e continuidade de seu funcionamento."(BRASIL, 2003, p. 21), por isso cabe ao Oficial formado possuir os conhecimentos mínimos para ocupar as funções que lhe for delegada, e não apenas isso, mas também saber instruir seus subordinados a respeitos do devido uso de redes em sua Organização Militar, como citado:

> […] na OM em que existir rede local de computadores e/ou computadores com acesso à Internet, orientar as atividades ligadas à gerência de redes, principalmente nos aspectos de segurança da informação(BRASIL, 2003, p. 21).

O que evidencia a necessidade de capacitação e informação pelos Oficiais que ocuparem o cargo de Oficial de Informática, visto a responsabilidade e a relevância de suas funções.

2.1.4 Segurança da Informação

Tão importante quanto a configuração dos meios de tecnologia da informação está a implementação de medidas de segurança e proteção a esses meios, por isso cabe a todas as Organizações Militares e seus integrantes contribuírem para a integridade dos dados e dos sistemas eletrônicos, como descreve a capacidade operativa de Proteção Cibernética no Manual de Campanha de Guerra Cibernética:

> Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente. (COMANDO DE OPERAÇÕES TERRESTRES, 2017, p. 26)

Sendo a capacidade operativa de Proteção Cibernética responsabilidade de todas as Organizações Militares como definido: “Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM”(COMANDO DE OPERAÇÕES TERRESTRES, 2017, p. 25), e além destes encargos as Organizações Militares de Comunicações, realizam estas e outras funções mais complexas, o que novamente evidencia a necessidade do preparo do Oficial de Comunicações nos assuntos relacionados a Cibernética.

Não se limitando apenas a segurança de redes a nível Organização Militar, é fundamental entre os indivíduos que lideram frações instruírem seus subordinados a utilização correta e consciente face os perigos da utilização da Internet, já que de nada adianta um sistema de defesa extremamente eficiente se o operador cometer falhas simples que possibilitam a invasão dos sistemas como:

> Um problema de segurança em seu computador pode torná-lo indisponível e colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Além disto, ao ser comprometido, seu computador pode ser usado para a prática de atividades maliciosas como, por exemplo, servir de repositório para dados fraudulentos, lançar ataques contra outros computadores (e assim esconder a real identidade e localização do atacante), propagar códigos maliciosos e disseminar spam.(CERT.BR, 2012, p. 3).

A utilização da Internet e de redes de computadores não é mais uma opção, por isso cabe a todos os integrantes zelarem pela eficiência e segurança dos sistemas bem como disseminarem a mentalidade de proteção e cautela constante para com suas informações e a de instituições que fazem parte.

2.1.5 Firewall

Como definido: “Firewall não é uma máquina, e sim um conceito. Qualquer recurso empregado na segurança de uma rede, inclusive humano, fará parte do sistema de firewall”(ERIBERTO, 2013, p. 351). A utilização de sistemas de segurança atualmente é vista como obrigatoriedade tendo em vista as constantes ameaças e ataque cibernéticos, esses esforços requerem conhecimento e capacitação por parte dos operadores, justamente para a instalação destas “barreiras” para o acesso indevido de redes e sistemas.

Quanto mais simples e melhor aplicadas, melhor funcionarão estas soluções e terão mais sucesso para controlar o acesso. A defesa em profundidade como dito por (ERIBERTO, 2013, p.353) significa utilizar mais de uma barreira, elementos de acesso individuais e separados que quando unidos dificultam as invasões e quebras de segurança.

Sobre a segurança de redes:"[…] nada evitará que tentativas de invasões continuem a existir mas, o que definirá se estas serão bem-sucedidas ou não será o conhecimento embutido em seu firewall e demais ferramentas de segurança"(NETO, 2004, p. 9).

Portanto o firewall não é uma solução isolada e definitiva, muito menos um sistema fechado, a implementação de sistemas de segurança dependem dos conhecimentos de quem as implementará e a forma como utilizará e configurará estas ferramentas de segurança, valendo-se de atributos como criatividade, engenhosidade e flexibilidade, todos inerentes ao Oficial de Comunicações.

2.1.6 Netfilter

Inserido no kernel do Linux "é um filtro de pacotes[…] Assim sendo, o netfilter é capaz de manipular apenas recursos oferecidos por protocolos como IP, ICMP, TCP, UDP etc."(ERIBERTO, 2013, p. 352).

O netfilter tem característica de ser basicamente um banco de dados com três tabelas distintas[…] que trabalharão de forma a filtrar e controlar o fluxo de dados interno ao kernel(NETO, 2004, p. 19).

O controle e filtragem de dados é essencial para qualquer rede, prevenindo ameaças e limitando o acesso indevido tanto de dentro da rede local para redes externas , como de redes externas para a rede interna. Essas ações são fundamentais pois além de garantir mais segurança contribuem para o uso devido das redes do Exército de forma eficiente e economizam recursos.

2.1.7 IPTables

Como definido "iptables não é um recurso de firewall, e sim um mero comando que manipula o verdadeiro filtro de pacotes existentes no Kernel Linux, o netfilter[…]", ou seja quando tratado do "firewall iptables", nos referimos à interface de controle das tabelas do netfilter, que facilita o gerenciamento e acrescenta alguns recursos que o tornam mais prático e eficiente. Assim "[…] o iptables (além de realizar suas tarefas de forma veloz, segura e eficaz e econômica, tanto no aspecto financeiro quanto no de requerimento de hardware) nos dá um amplo leque de possibilidades tais como a implementação desde filtros de pacotes[…] redirecionamento de

endereçamento e portas, mascaramento de conexões, detecção de fragmentos, monitoramento de tráfego […] bloqueio a ataques […]”(NETO, 2004, p. 25).

O iptables isoladamente não representa uma solução definitiva para prover a segurança de uma rede ou sistema(ERIBERTO, 2013, p. 352), porém é uma opção extremamente viável tendo em vista o custo mínimo e os baixos requerimentos de hardwares, fatores estes determinantes quando se trata de implementação de soluções no Exército Brasileiro face a limitação de recursos e dos materiais já existentes.

Por isso é extremamente vantajoso ao Oficial de Comunicações, nas funções em que lhe for necessário a gestão de redes a correta configuração e gerenciamento do Netfilter com a utilização do iptables, o domínio desses conhecimentos trarão aos sistemas em sua responsabilidade mais segurança e eficiência, mas para atingir tal objetivo é necessário a obtenção de conhecimentos mínimos nos diversos aspectos que englobam as questões de segurança de redes.

3 METODOLOGIA

Esta pesquisa tem como meta principal estudar a necessidade e as possibilidades para propor a implementação do ensino na cadeira de Cibernética do Curso de Comunicações do assunto firewall nos sistemas GNU/Linux e IPTables, fundada nas hipóteses $\mathbf{H}_1$ e $\mathbf{H}_2$ apresentadas no capítulo 1.4 desta pesquisa.

Tanto o método quantitativo quanto o qualitativo estão presentes nesta pesquisa, tendo em vista a complexidade da abordagem do assunto e da problemática, utilizando dados numéricos e procedimentos estatísticos para a análise em si das informações obtidas ou já existentes. A pesquisa apresenta caráter descritivo quanto a pesquisa de campo e busca ser aplicada de forma que gere soluções ao problema exposto baseando-se nas informações obtidas na pesquisa bibliográfica e documental.

Para atingir o objetivo primeiramente se fez necessário um estudo de bibliografias que forneceram um sólido embasamento técnico e teórico na área de segurança da informação, firewall, GNU/Linux, das portarias e documentações do Exército Brasileiro que viabilizam e sustentam a necessidade de aperfeiçoamento constante do currículo do Oficial de Comunicações inserido na Era do Conhecimento e da crescente digitalização dos meios.

Após o estudo bibliográfico e documental buscou-se montar o perfil dos Cadetes de Comunicações quanto ao assunto de firewall e IPTables. Para tal foi elaborado um questionário e este foi aplicado nos Cadetes do Curso de Comunicações.

A execução da pesquisa de campo se deu através de formulários impressos distribuídos aos Cadetes, não havendo limite de tempo para o preenchimento. Após a realização dos questionários houve a centralização dos mesmos, estes foram separados de acordo com o ano de Academia Militar (2° ano, 3° ano e 4° ano) e foram contabilizadas as respostas e lançadas em planilhas. Os dados em seguida foram utilizados para elaboração de gráficos.

O questionário, presente no Anexo A desta pesquisa, foi composto por 7 itens, sendo o primeiro referente a idade e turma do Cadete, e os outros 6 itens consistiam em questões objetivas baseadas na Escala Linkert com 5 níveis(+2,+1,0,-1,-2).

> Escalas Likert são uma das escalas de autorrelato mais difundidas, consistindo em uma série de perguntas formuladas sobre o pesquisado, onde os respondentes escolhem uma dentre várias opções, normalmente cinco, sendo elas nomeadas como: Concordo muito, Concordo, Neutro/indiferente, Discordo e Discordo muito.(AGUIAR; CORREIA; CAMPOS, 2011, p. 02).

As perguntas faziam referência as noções e experiências que o Cadete possuía com o firewall do GNU/Linux e a ferramenta IPTables bem como a opinião geral sobre o ensino destes

assuntos, da área de segurança de redes no geral e da carga horária. Consideraremos os itens do questionário como: $\mathbf{I_1}$, $\mathbf{I_2}$, $\mathbf{I_3}$, $\mathbf{I_4}$, $\mathbf{I_5}$, $\mathbf{I_6}$, $\mathbf{I_7}$.

$\mathbf{I_1}$: Este item como já mencionado apenas tem como objetivo levantar dados básicos, que posteriormente servirão para o refinamento e melhor análise das informações coletadas, tais como idade e turma de aula, e também como forma de respaldar a pesquisa se o indivíduo concorda ou não com a realização da pesquisa.

$\mathbf{I_2}$: O item 2 serve como indicativo mais básico da opinião do indivíduo acerca do conceito de firewall e tem grande importância no nivelamento da opinião acerca do conhecimento sobre firewalls.

$\mathbf{I_3}$: Este item de caráter mais focado na prática aborda a questão do contato com o firewall, o que diferente de simplesmente saber o conceito e já demonstra um nível maior de aprofundamento e uma maior intimidade com a parte de segurança de redes.

$\mathbf{I_4}$: Assim com o $\mathbf{I_2}$ este item tem como objetivo apenas saber se o Cadete tem a noção da existência do firewall dos Sistemas Operacionais GNU/Linux e sua ferramenta IPTables, representando um maior escalonamento do conhecimento que o Cadete julga ter sobre esses assuntos.

$\mathbf{I_5}$: Este item já é de caráter mais subjetivo expressando a mentalidade e opinião do Cadete em relação a relevância do conhecimento de segurança de redes e a capacidade de operar estes sistemas para o Oficial de Comunicações.

$\mathbf{I_6}$: O item 6 expressa tal como o $\mathbf{I_5}$ a opinião do Cadete, levando em conta suas vivências e experiências no Curso de Comunicações, em relação a carga horária dos assuntos de seguranças de redes e firewalls.

$\mathbf{I_7}$: E como fechamento do questionário o item 7 serve como uma auto análise do Cadete considerando todos seus conhecimentos do assunto e baseado nisso este avaliará se está apto para gerenciar um firewall e garantir a segurança de redes.

Após a realização da pesquisa de campo e pesquisa bibliográfica e documental foi feita a centralização dos dados, documentos e materiais que contribuíram para a elaboração das conclusões referentes a temática central.

O questionário exprime tanto a mentalidade geral dos Cadetes do Curso quanto a imagem que cada turma possui, e também as mudanças de acordo com cada ano durante a Academia, além do domínio e o contato que os Cadetes possuem com os assuntos desta pesquisa.

Estas informações em conjunto com os atuais PLADIS e Plano Integrado de Disciplina(PLANID) do Curso de Comunicações de 2019 servem como base para que mediante os planos e necessidades do Exército Brasileiro expressos em portarias e documentações possam gerar

mudanças e assim implementar conteúdos e assuntos que carecem na formação e assim melhor preparar os Oficiais de Comunicações.

3.1 ESTATÍSTICA

A pesquisa de campo foi realizada com 99 Cadetes do Curso de Comunicações, o que representa uma amostra não-probabilística sendo 25 do 2° ano, 33 do 3° ano e 41 do 4° ano, de uma população de 112 Cadetes, sendo destes 31 do 2° ano, 38 do 3° ano e 43 do 4° ano.

Realizando uma análise estatística por meio de um software onde considera-se uma população de 112 indivíduos e uma amostra de 99 indivíduos e utilizado-se uma confiabilidade de 95% é possível obter uma margem de erro de 3,59% de acordo com o site *"www.solvis.com.br"*.Em posse dos dados e através das ferramentas do *LibreOffice* foi possível elaborar toda a parte de gráficos presentes nesta pesquisa, a parte de percentuais toda foi calculada de acordo com o site "*www.profcardy.com/calculadoras/porcentagem.php*" utilizando arredondamentos com uma casa decimal para os percentuais nas análises do texto.

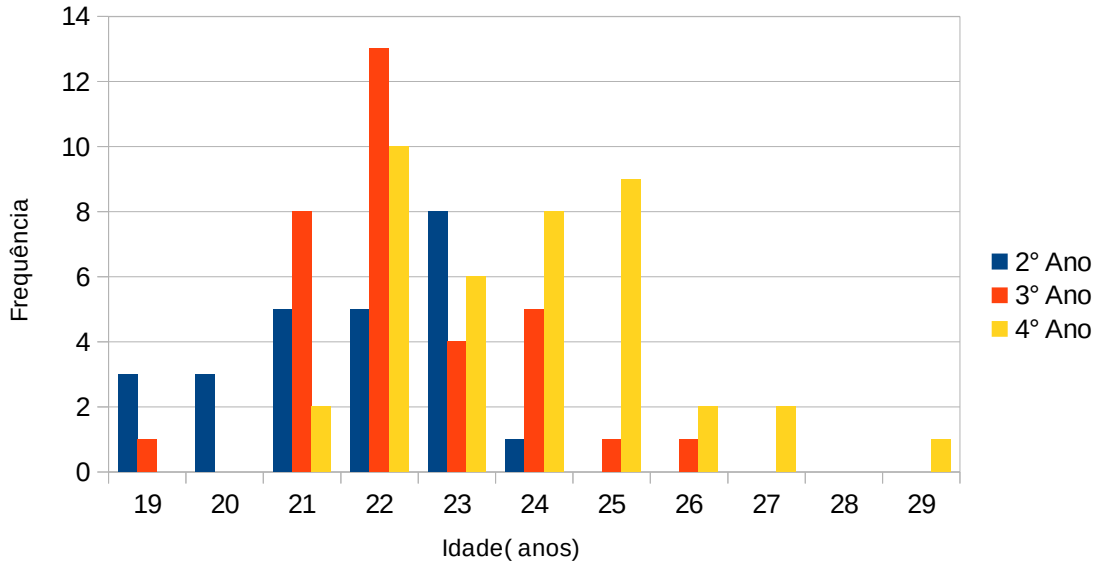
4 RESULTADOS E ANÁLISE DOS DADOS

4.1 RESULTADOS E ANÁLISE DA PESQUISA DE CAMPO

4.1.1 Item 1 – Dados dos Cadetes de Comunicações

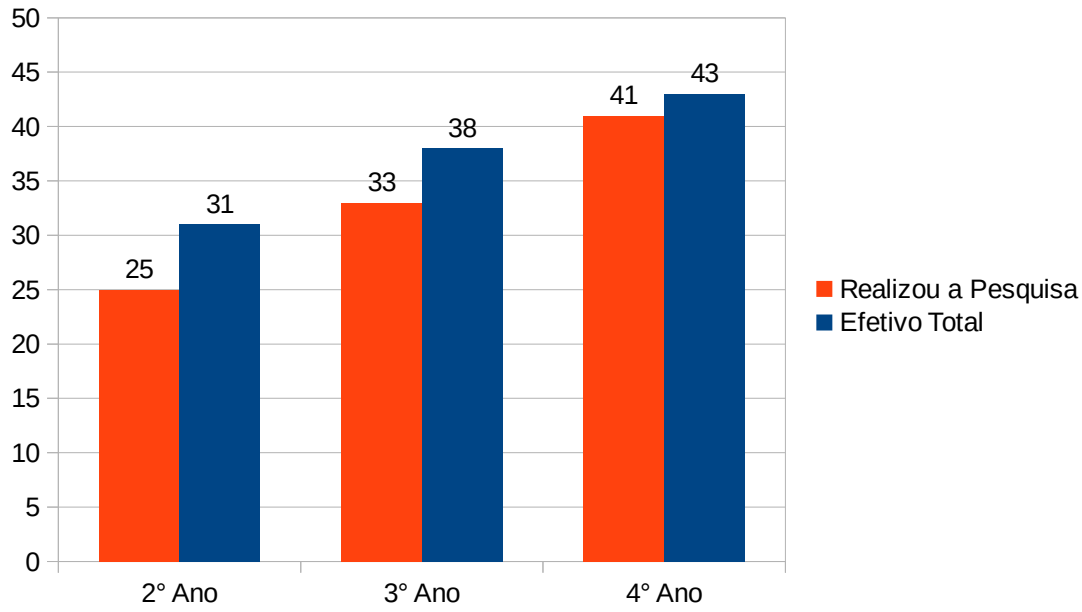
Discriminar as idades e as turmas de aula dos Cadetes é de fundamental para a análise da pesquisa já que se têm um panorama das respostas dos itens de acordo com os anos da Academia e a correlação das idades de cada turma, em posse dessas informações foram elaborados os gráficos abaixo:

Gráfico 1 – Idade dos Cadetes de Comunicações 2019



Fonte: Autor(2019)

Gráfico 2 – Cadetes que Realizaram o Questionário



Fonte: Autor(2019)

Nota-se que os Cadetes do 2° ano estão na faixa entre 19 e 24 anos, sendo a maior parte entre 21 a 23 anos; o 3° ano está na faixa entre 19 e 26 anos, mas a maioria, de fato encontra-se com 21 e 22 anos; o 4° ano a turma de distribui entre 21 a 29 anos, sendo a maioria com 22, 24 e 25 anos.

É evidente no gráfico a tendência ao envelhecimento das turmas de acordo com o ano de Academia, porém a pesquisa indica resultados equilibrados quanto às idades dos Cadetes. Baseado na idade com maior número de repetições: a idade de 23 anos sozinha representa 32% do 2° ano, enquanto que 22 anos representa 39,4% do 3°ano e 22 anos representa 24,4% do 4° ano.

Quanto a participação dos Cadetes por ano: no 2° ano 25 Cadetes de 31 participaram o que representa 80,64%, no 3° ano 33 de 38 representando 86,84% e, por fim, no 4° ano 41 de 43 que equivale a 95,34% dos Cadetes. No total 99 dos 112 Cadetes responderam representando 88,4% da população total.

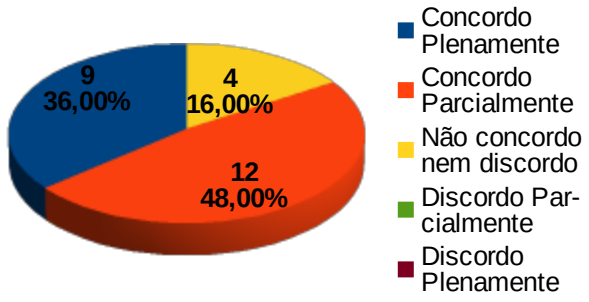
A grande participação dos Cadetes de Comunicações é fator de grande importância para que se alcance os objetivos deste trabalho, já que o mesmo está inserido tanto na área educacional do quanto na área operacional do Oficial de Comunicações. Os levantamentos de idade e a separação entre os anos guiam a análise dos próximos itens e permitem levantar as diferenças em que cada ano de formação acarreta nas concepções e no conhecimento de firewall e IPTables.

4.1.2 Item 2 – Noção do Conceito e Serventia de um Firewall

Este item levanta se os Cadetes sabem ou não o que é um firewall e sua aplicabilidade, os resultados foram majoritariamente positivos, sendo no 2° ano apenas respostas ou positivas ou neutras de acordo com a escala, fato que difere do 3° e 4° ano onde apresentam resultados negativos, mesmo que em percentuais inferiores a 12,20%.Esta diferenciação do 2° para os demais anos já representa um diferencial da turma, pelo menos em relação ao conceito básico de firewall.

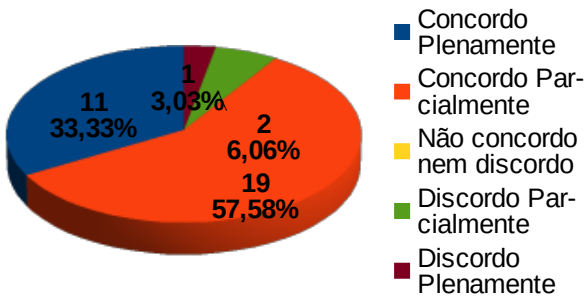
No total temos que 85,9% dos Cadetes apresentaram respostas positivas em relação ao item, apesar de serem bons resultados os gráficos mostram que ainda existem oito Cadetes que desconhecem o conceito mínimo e aplicabilidade de um firewall, isto representa uma falha grave no processo de ensino-aprendizagem e avaliação dos conteúdos de segurança de redes e firewalls, já que os resultados negativos aparecem no 4° e no 3° ano, esse fato corrobora com a $\mathbf{H}_2$. Todos os resultados mencionados podem assim ser vistos nos gráficos abaixo:

Gráfico 3 – Item 2 – 2° Ano



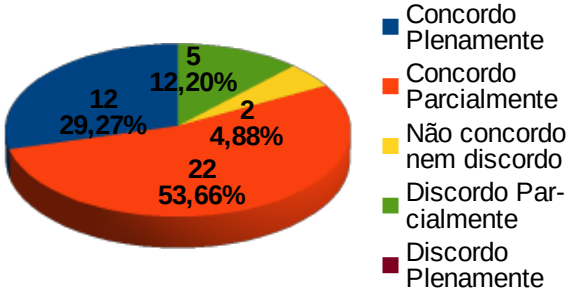
Fonte: Autor(2019)

Gráfico 4 – Item 2 – 3° ano



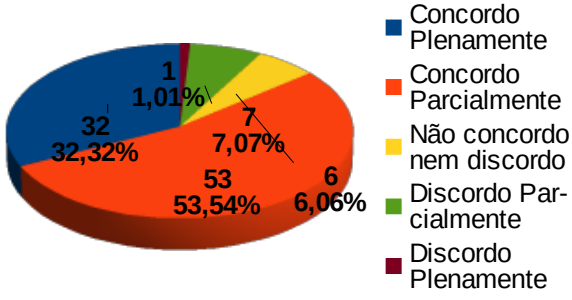
Fonte: Autor(2019)

Gráfico 5 – Item 2 – 4° Ano



Fonte: Autor(2019)

Gráfico 6 – Item 2 – Total



Fonte: Autor(2019)

4.1.3 Item 3 – Contato prévio e Práticas com Sistemas de Firewall

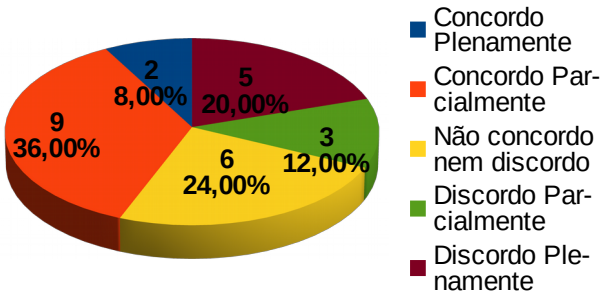
O terceiro item como já mencionado apresenta caráter que remonta mais a prática em si e avalia se o Cadete já travou contato com algum sistema de firewall. A distribuição das respostas é visivelmente mais equilibrada e como este item serve como um escalonamento do conhecimento referente ao $\mathbf{I_2}$ o quantitativo de Cadetes que responderam positivamente caiu de forma considerável, assim crescendo os números de respostas negativas.

Notou-se ainda que no 3° ano as respostas negativas alcançam 57,6%, no 4° ano 43,9% e no 2° ano 32%. Novamente o 2° ano se diferencia das outras turmas apresentando o menor percentual negativo e novamente o maior percentual positivo, o 3° ano desta vez além de apresentar o maior percentual negativo, este representa mais da metade dos participantes da pesquisa.

No geral a maioria das respostas tenderam a serem negativas 45,9% do total, mas havendo ainda uma expressiva quantidade positiva de 36,4%, as respostas neutras variaram de 15,15% dos participantes a 24%.

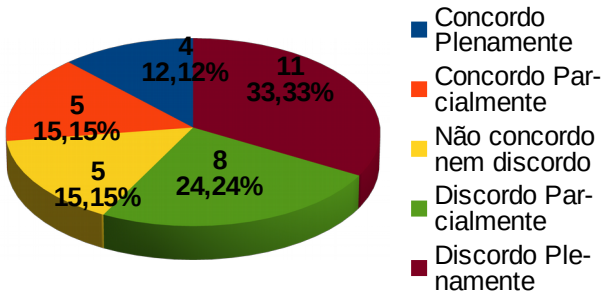
A sensível queda do percentual de respostas positivas está correlacionada ao fato deste item ser escalonado com o anterior de forma a avaliar capacidades ou conhecimentos mais complexos, mas apesar disto ainda expressa dados preocupantes já que estas noções ainda são elementares diante dos tópicos presentes nos assuntos de segurança de redes, estas respostas indicam ainda mais que no item anterior as ideias expressas na $\mathbf{H_2}$ reforçando a necessidade da mudança e da complementação do ensino em redes.

Gráfico 7 – Item 3 – 2° ano



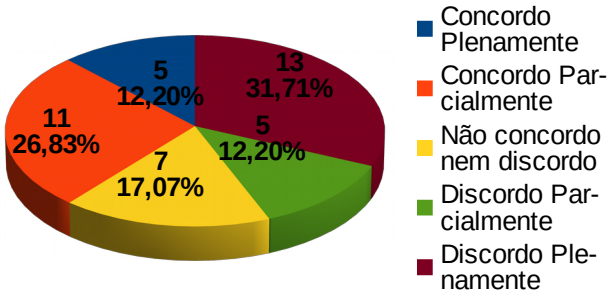
Fonte: Autor(2019)

Gráfico 8 – Item 3 – 3° ano



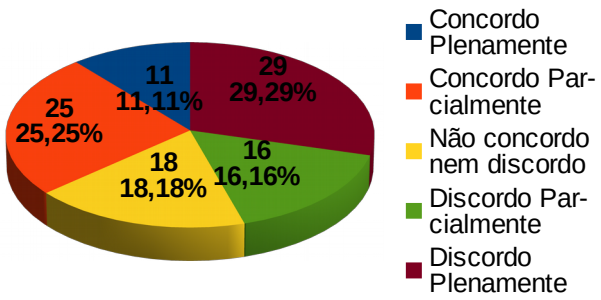
Fonte: Autor(2019)

Gráfico 9 – Item 3 – 4° ano



Fonte: Autor(2019)

Gráfico 10 – Item 3 – Total



Fonte: Autor(2019)

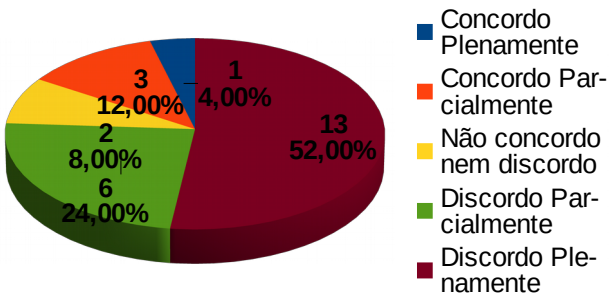
4.1.4 Item 4 - Noção Básica do que é IPTables

O item 4 segue a linha de raciocínio de escalonar os conhecimentos dos Cadetes e por isso indaga sobre o conhecimento da ferramenta IPTables, nos gráficos é possível identificar que o resultado no 2° ano foram majoritariamente negativos com 76%, no 3° ano 51,5% negativos e no 4° ano com 48,8% negativos. O total ficou semelhante, sendo 56,6% Cadetes que responderam negativamente em relação a afirmação da questão e 32,3% respondendo de forma positiva.

O resultado do 2° ano perante os outros anos indica a diferenciação dos conhecimentos que o Cadete deve acumular durante sua formação o que é mostrado também pelo comparativo entre o 4° e o 3° ano, sendo o 4° ano com maior percentual positivo e menor negativo, estes fatos apesar de resultados coerentes com a ideia de aperfeiçoamento do Oficial de Comunicações, quando colocados em conjunto com o quantitativo de Cadetes que responderam a questão de forma negativa, sendo praticamente a metade no caso do 4° e 3° ano, onde já deveriam pelo menos ter alguma noção do IPTables por se tratar de uma ferramenta do firewall do Sistema Operacional que o Exército utiliza por doutrina.

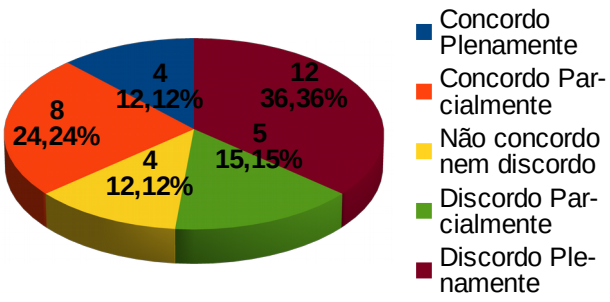
A hipótese $\mathbf{H_2}$ é reforçada com os resultados desse item, vemos que parte considerável dos Cadetes do 4° e 3° ano não têm conhecimento da ferramenta IPTables, o que indica a real necessidade de implementação de tópicos específicos no PLADIS do Cadete nesse assunto.

Gráfico 11 – Item 4 – 2° ano



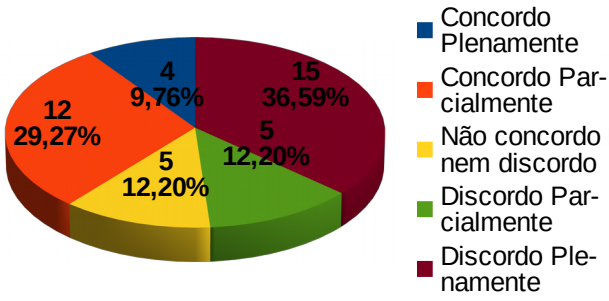
Fonte: Autor(2019)

Gráfico 12 – Item 4 – 3° ano



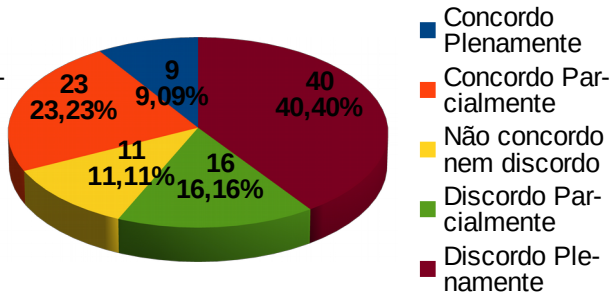
Fonte: Autor(2019)

Gráfico 13 – Item 4 – 4° ano



Fonte: Autor(2019)

Gráfico 14 – Item 4 – Total



Fonte: Autor(2019)

4.1.5 Item 5 – Opinião Sobre a Relevância dos Conhecimentos de Segurança de Redes

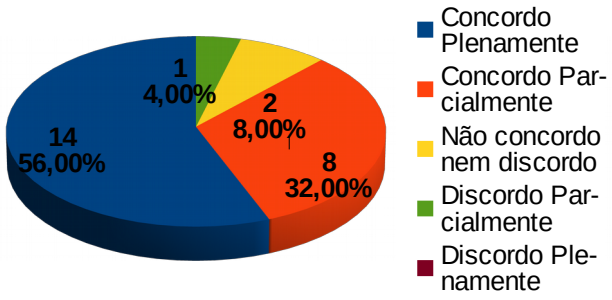
O item 5 foi elaborado com o objetivo de focar na análise subjetiva e pessoal de cada indivíduo quanto a importância dos conhecimentos em segurança de redes para o Oficial de Comunicações. Como forma de complementar o levantamento realizado pelos itens anteriores este trata da concepção e mentalidade em relação a segurança de redes.

Como já mostrado neste trabalho a informatização dos meios do Exército Brasileiro, e do mundo como um todo, torna o domínio dos conhecimentos de segurança de redes e suas ferramentas algo essencial para o Oficial de . O questionário, especificamente este item, busca entender a visão que está presente em cada uma das turmas de Comunicações sobre este assunto de tal relevância.

Nos gráficos é claro a que a maior parte dos Cadetes se mostram concordar com a assertiva optando pela alternativa “Concordo Plenamente” que indica máxima aprovação, sendo os resultados positivos 88% no 2° ano, 90,1% no 3° ano e 97,6% no 4° ano e os resultados negativos não maiores que 4%.

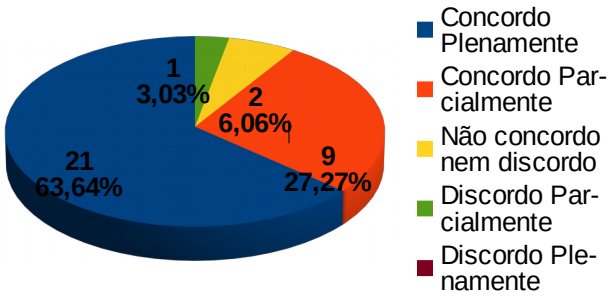
Os resultados totais indicam que apenas 2 dos 99 Cadetes que realizaram a pesquisa discordaram da importância dos conhecimentos de segurança de redes para o Oficial de Comunicações, o que mostra uma concordância em maioria com a relevância dos conhecimentos de segurança de redes e uma mentalidade que predominantemente valorizará estes conhecimentos.

Gráfico 15 – Item 5 – 2° ano



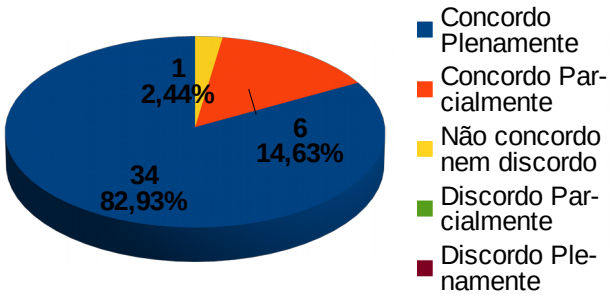
Fonte: Autor(2019)

Gráfico 16 – Item 5 – 3° ano



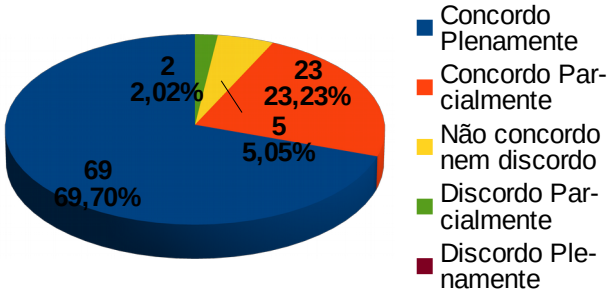
Fonte: Autor(2019)

Gráfico 17 – Item 5 – 4° ano



Fonte: Autor(2019)

Gráfico 18 – Item 5 – Total



Fonte: Autor(2019)

4.1.6 Item 6 – Suficiência dos Conteúdos e Carga Horária de Segurança de Redes/Firewalls

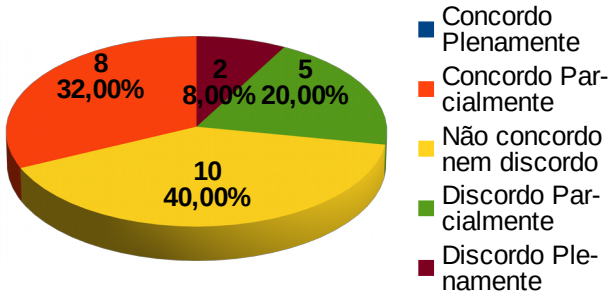
Este item segue a mesma linha de raciocínio do item anterior, trata-se de uma assertiva que faz referência a suficiência da carga horária e dos assuntos ministrados sobre segurança de redes e firewalls. O Cadete informaria baseado em suas concepções e vivências se concorda com a afirmação, ou seja, trata-se também de um item opinativo onde é possível levantar o que está presente na mentalidade das turmas.

Nos gráficos o 2° ano claramente destoa do 4°e 3° apresentando até certa dúvida nas respostas sobre a assertiva, isto é evidenciado pela maior fatia do gráfico de 40% ser representada por uma alternativa neutra, este fenômeno pode ser explicado devido ao natural pouco contato do 2° ano com as disciplinas e a inexperiência.

O 4° e 3° ano concordam entre si com relação as respostas em sua maioria negativas referente a assertiva, sendo no 4° ano onde isso é nítido, com 70,7% das respostas do 4° ano discordando da assertiva e 63,6% do 3° ano, as respostas foram positivas em 19,5% do 4° ano e 21,2% do 3° ano. Ao todo temos que 57,6% tendem a discordar e 23,2% tendem a concordar, o que resta são 19,2% que permanecem neutros.

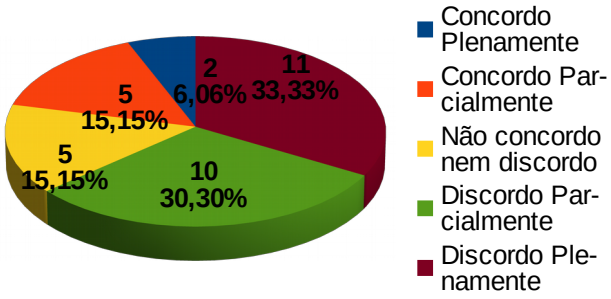
Como o Cadete responde baseado apenas em suas experiências, visão de mundo e conhecimentos já adquiridos é evidente que a maioria dos Cadetes discordam que a carga horária atual seja suficiente, esta mentalidade pode ser acarretada justamente pelo que explica a $\mathbf{H_2}$, ou seja, que o PLADIS precisa ser aperfeiçoado visando as necessidades atuais referentes a estes assuntos.

Gráfico 19 – Item 6 – 2° ano



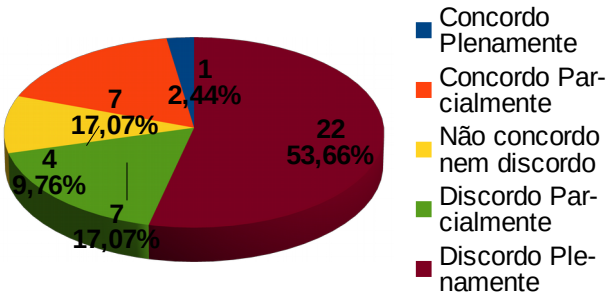
Fonte: Autor(2019)

Gráfico 20 – Item 6 – 3° ano



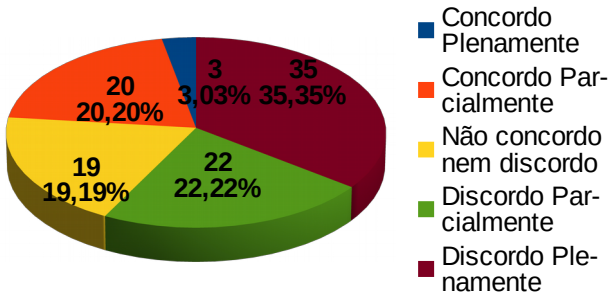
Fonte: Autor(2019)

Gráfico 21 – Item 6 – 4° ano



Fonte: Autor(2019)

Gráfico 22 – Item 6 – Total



Fonte: Autor(2019)

4.1.7 Item 7 – Opinião sobre a Aptidão a Gerenciar um Firewall e Prover a Segurança de Redes

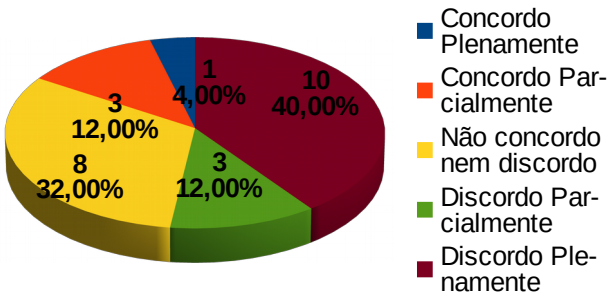
A assertiva do item 7 representa o fechamento do questionário e é uma referência direta a H_1, hipótese esta que trata da ideia que os Cadetes não estão ou não se sentem aptos para operar sistemas de firewall. Sendo esse item de caráter mais subjetivo e opinativo ele busca fazer com que o Cadete realize uma auto avaliação sobre seus conhecimentos e experiências e avalie se está apto ou não.

Os resultados indicam que mais da metade nos 3 anos discordam da afirmativa, com 52% no 2° ano 75,8% no 3° e 70,3% no 4° ano. As respostas positivas ficaram em 16% no 2° ano, 12,1% no 3° ano e 14,14% no 4° ano, cabendo destacar que no 2° ano o quantitativo de repostas neutras se mostrou bem elevado com 22% em comparação com os 12,1% e 14,6% do 3° e 4° ano respectivamente. O total ficou em 67,7% tendendo a discordarem com assertiva, 14,1% tendendo a concordarem e 18,2% permanecendo neutros.

O alto valor de respostas negativas neste questionário possui uma carga maior de relevância em comparação aos outros itens devido a esta assertiva basicamente representar a mentalidade geral do Cadete em relação a estar apto a empregar a segurança de redes em firewalls e o que indica a pesquisa é que em todos os anos a maioria dos Cadetes não se sentem preparados.

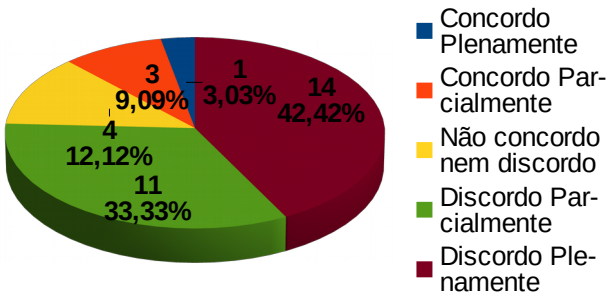
O 4° ano apresentou a taxa de 70,3%, onde 39% discordaram plenamente da assertiva e 31,7% discordaram parcialmente, por estarem no último ano de formação e mais próximos de serem empregados nas mais diversas missões no corpo de tropa estes deveriam se sentir preparados. Este item reforça a hipótese H_2 proposta pela pesquisa e evidencia as deficiências a serem solucionadas.

Gráfico 23 – Item 7 – 2° ano



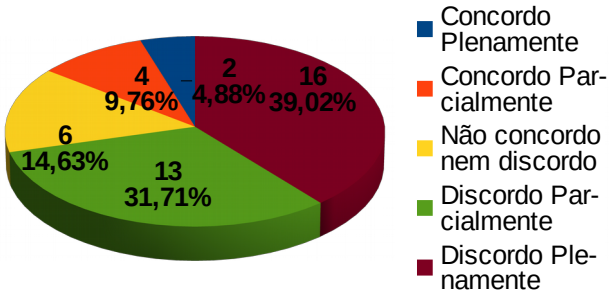
Fonte: Autor(2019)

Gráfico 24 – Item 7 – 3° ano



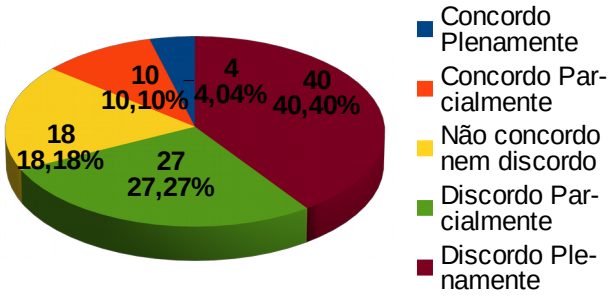
Fonte: Autor(2019)

Gráfico 25 – Item 7 – 4° ano



Fonte: Autor(2019)

Gráfico 26 – Item 7 – Total



Fonte: Autor(2019)

4.2 RESULTADO E ANÁLISE DA PESQUISA DOCUMENTAL E BIBLIOGRÁFICA

4.2.1 Análise do PLADIS de Cibernética

Como enunciado no capítulo 2.1.1 deste trabalho, que trata sobre o ensino de Cibernética no Curso de Comunicações, o PLADIS dos 3 anos abordam uma grande variedade de assuntos da área, esta pesquisa focou nos tópicos que fazem menção a firewalls e segurança de redes, já que o foco da pesquisa trata de IPTables e o mesmo não se incluía no PLADIS de forma específica e direta.

Tendo em mente isto, buscou-se analisar qual seria a melhor forma de implementar estes assuntos de forma eficiente e que o Cadete possa ter um aprendizado progressivo, sendo importante não apenas como implementar, mas quando implementar. Cabendo ressaltar que a ausência e a pouca especificidade de tópicos no PLADIS podem ser causas e comprovam a $\mathbf{H_2}$.

A implementação no 2° ano se mostra inviável já que este ano deve focar em dar ao Cadete uma boa base e fornecer os conteúdos essências sobre GNU/Linux para prepará-lo para os anos seguintes. O 3° ano foca sua totalidade basicamente em servidores onde é possível evidenciar a Unidade VI:

Quadro 1 – Unidade VI: Firewall

UD VI: Firewall	**Cg H: 18**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. PFSense	01	-	- Instalar e administrar o PFSense de acordo com a bibliografia de referência, protegendo os sistemas de informação e redes de dados. (PROCEDIMENTAL) **ET: Aprimoramento técnico-profissional**

Fonte: PLADIS do 3° Ano do Curso de Comunicações(2019)

Esta unidade do 3° ano foca em um servidor de firewall muito conhecido, o PFSense. Este é muito completo e serve como firewall externo instalado em uma máquina. Sendo a única menção a firewall no PLADIS do 3° ano, a concepção de ensinar a solução em ampla escala antes de se ensinar os conceitos básicos e fazer com que o aluno aprenda as configurações locais não permite a aprendizagem progressiva e devida proposta.

No caso esta unidade seria mais interessante ser colocada no 4° ano na parte de hardening de servidores após ensinado sobre firewall do GNU/Linux e IPTables, fazendo assim o Cadete ter um melhor aprendizado dos assuntos.

Os quadros a seguir retirados do PLADIS do 4° ano de 2019 do Curso de Comunicações indicam os assuntos de Cibernética V ministrados:

Quadro 2 – Unidade I : Guerra Cibernética

UD I: Guerra Cibernética	**Cg H: 01**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. Princípios de Emprego da Guerra Cibernética	01	-	- Conhecer o funcionamento da Guerra Cibernética e seus princípios, a fim de compreender sua extensão, seus possíveis alvos e ameaças. (CONCEITUAL)

Fonte: PLADIS do 4° Ano do Curso de Comunicações(2019)

Quadro 3 – Unidade II : Hardening de Sistemas Operacionais

UD II: Hardening de Sistemas Operacionais	**Cg H: 12**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. Hardening do Sistema Operacional Debian e Microsoft Windows	08	-	Realizar o Hardening dos sistemas Windows e Linux, de acordo com a bibliografia de referência, protegendo os sistemas de informação e redes de dados. (PROCEDIMENTAL)

Fonte: PLADIS do 4° Ano do Curso de Comunicações(2019)

Quadro 4 – Unidade III: Hardening de Servidores

UD III: Hardening de Servidores	**Cg H: 13**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. Hardening dos servidores e serviços de rede	09	-	Realizar o Hardening dos Servidores de rede e serviços, de acordo com a bibliografia de referência, protegendo os sistemas de informação e redes de dados. (PROCEDIMENTAL) **ET - Dedicação**

Fonte: PLADIS do 4° Ano do Curso de Comunicações(2019)

Estes quadros apesar de apresentarem conteúdos necessários para que o Oficial de Comunicações atinja o objetivo de guarnecer a segurança dos sistemas em sua responsabilidade, estes carecem de uma especificidade nos quesitos de hardening de sistemas operacionais e dos servidores, por isso se faz necessário a implementação de tópicos específicos dos assuntos ministrados.

Alinhado com tudo isso está o objetivo principal deste trabalho e pesquisa, que é justamente implementar no PLADIS do Curso de Comunicações o assunto de segurança de sistemas e redes com firewall e IPTables., por isso foi elaborado uma proposta de alteração do PLADIS embasada na pesquisa documental e bibliográfica.

4.2.2 Proposta de implementação e alteração do PLADIS

Tendo em mente todas as deficiências e oportunidades de melhoria do Plano de Disciplina de Cibernética do Curso de Comunicações buscou-se alterar os mesmos de forma manter a aprendizagem gradual e melhor especificar os tópicos de Firewall GNU/IPTables baseando-se nas documentações governamentais e do Exército Brasileiro e bibliografias confiáveis.

A primeira alteração que visa o melhor aprendizado do Cadete é que os conteúdos da Unidade VI(Quadro 1) do PLADIS do 3° ano sejam ministrados no 4° ano após o ensino dos conceitos básicos de firewall e IPTables para posteriormente aprender sobre Pfsense e servidores de firewall.

O PLADIS do 4° ano carece de especificidade dos assuntos de hardening, como já mencionado, por isso propõe-se os assuntos a serem inseridos no PLADIS dentro área da pequisa

deste trabalho. Assim é proposto adicionar os seguintes assuntos e objetivos na Unidade II(Quadro 3):

Quadro 5 – Assuntos propostos para complementação no PLADIS

UD II: Hardening de Sistemas Operacionais **ASSUNTOS PROPOSTOS**	**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
a. Firewall em Linux	Compreender o que é um firewall e seu histórico. (CONCEITUAL) Identificar os tipos de firewall: firewall filtro de pacotes, firewall NAT e firewall híbrido. (CONCEITUAL) Compreender o que é netfilter. (CONCEITUAL) Identificar as três tabelas do netfilter(filter, nat e mangle) e suas especificidades. (CONCEITUAL) Compreender o que é a ferramenta IPTables, seus aplicativos(iptables, ip6tables, iptables-save, iptables-restore) e seus conceitos básicos. (CONCEITUAL) Realizar a instalação do IPTables nos sistemas GNU/Linux. (PROCEDIMENTAL) Compreender os comandos no IPTables e sua sintaxe. (CONCEITUAL) Executar as configurações de regras de firewall no IPTables através das suas tabelas(filter, nat e mangle). (PROCEDIMENTAL) Implementar os scripts de regras de firewall já existentes para o IPTables de forma a limitar o acesso do usuário atendendo as necessidades de uma rede. (PROCEDIMENTAL) **ET: Aprimoramento técnico-profissional**
b. IPTables	

Fonte: Autor (2019)

Este quadro foi elaborado para suprir as necessidades já evidenciadas na pesquisa de campo e no próprio PLADIS em si, a carga horária para que sejam ministrados esse conteúdo é questão para análises e estudos futuros, os assuntos acrescentados e os seus objetivos seguem linha de desenvolvimento de acordo com Neto(2004) de forma que o Cadete entenda o que é um firewall, sua estrutura, como configurá-lo e, por fim, realize uma implementação baseada em scripts já existentes de regras no IPTables, de forma a melhor preparar os futuros Oficiais de Comunicações para as necessidades e incertezas do atual cenário cibernético.

5 CONSIDERAÇÕES FINAIS

Este trabalho buscou verificar a necessidade de implementação do ensino de firewall GNU/Linux e IPTables no PLADIS do Curso de Comunicações, bem como realizar uma proposta de inserção e modificação nestes assuntos visando a melhor formação e preparação do Cadete para cumprir as diversas missões que receberá no Corpo de Tropa.

Para tal primeiro foi levantado o problema e as temáticas a serem estudadas baseadas em necessidades e deficiências que o Cadete possui na disciplina de Cibernética, com isso foi realizado um estudo bibliográfico e documental que amparasse a pesquisa e fornecesse os conhecimentos e informações para elaborar este trabalho.

Com a pesquisa documental e análise das documentações do Exército Brasileiro foi comprovado que os conhecimentos de firewall e o domínio de suas funcionalidades são essências ao Oficial de Comunicações, seja pelo Exército Brasileiro, através das diretrizes do Ministério do Planejamento, Orçamento e Gestão, adotar os Softwares Livres e com isso utilizações dos sistemas operacionais GNU/Linux, ou pela crescente digitalização dos meios e com isso a ampliação do número de ameaças e ataques a órgãos governamentais no espaço cibernético.

Após este levantamento de informações procurou-se entender a mentalidade e montar o perfil de cada uma das turmas do Curso de Comunicações no que tange aos assuntos de firewall GNU/Linux e IPTables, para isso foi elaborado um questionário composto por questões objetivas onde o Cadete exprimia seu pensamento através de uma escala em cinco níveis de concordância e discordância.

Sendo o questionário de caráter voluntário, anônimo e sem tempo para realização os Cadetes puderam expressar suas opiniões livremente. Após a realização destes e centralização dos dados foram elaborados gráficos que permitiram melhor observação e análises do que foi levantado.

O primeiro ponto que foi evidenciado no questionário foi que uma considerável parte dos Cadetes desconhecem os conceitos mais básicos de firewall e a maioria do grupo analisado não tinha ciência da ferramenta IPTables, isto já indicou que a $\mathbf{H_2}$ tem validade.

Através de questões opinativas sobre a forma como os Cadetes avaliam sua capacitação, experiências, a carga horária dos assuntos e sua relevância para o Oficial de Comunicações ficou evidente que grande parte não se sente apta a prover a segurança das redes que estiverem em sua responsabilidade(confirmando a $\mathbf{H_2}$), sendo grande parte deste grupo Cadetes do 4°ano que deveriam já possuir estas capacidades.

O questionário evidenciou as deficiências e a alarmante situação que encontram-se os Cadetes de Comunicações em relação ao assunto de segurança com firewalls e uso da ferramenta

IPTables, cabendo, assim, grande urgência para a correção destas deficiências, visto que a ausência de conhecimentos e má gestão dos sistemas informacionais da União poderá acarretar em perdas significativas e burocracia desnecessária, ou até, em casos de conflitos, em perdas de vidas e a derrota no campo de batalha.

Foi avaliado em conjunto com os questionários o PLADIS da matéria de Cibernética do Curso de Comunicações e através de uma verificação deste conclui-se que o assunto de firewall era citado somente uma única vez e já fazendo referência a um sistema avançado utilizado como solução externa para redes através do Pfsense. Nas unidades onde deveria ser citado, como em hardening, faltava especificidade além disso os objetivos de aprendizagem, bem como os assuntos, se mostravam vagos, fatos que comprovam a $\mathbf{H_2}$.

Com isso foi realizada uma proposta de implementação e modificação de unidades e assuntos no PLADIS do 3° e 4° ano do Curso Comunicações como tentativa de sanar as deficiências e suprir as necessidades de conhecimentos dos assuntos firewall em GNU/Linux e IPTables.

Assim através deste trabalho e todo o seu processo de realização foi alcançado o objetivo geral e seus objetivos específicos, ou seja, o estudo comprovou a necessidade de implementação de conteúdos no PLADIS e através dos estudos com bibliografias confiáveis se obteve os conhecimentos e amparo para que se pudesse realizar uma proposta de assuntos e objetivos a serem inseridos ou modificados.

Cabe ressaltar que se faz necessário uma maior quantidade de estudos e avaliações com os Cadetes para averiguar os conhecimentos que cada um possui e assim conseguir uma visão mais precisa sobre os problemas no ensino aprendizagem do Curso, assim como uma averiguação sobre a situação de outros tópicos da segurança da informação, que também possuem grande importância, na matéria de Cibernética. Estes estudos por limitações de tempo e meios não foram possíveis de serem realizados na presente pesquisa, mantendo-se o foco nas questões já apresentadas.

O devido ensino e aprendizagem dos assuntos apresentados por meio desta pesquisa podem acarretar na mudança do perfil dos Cadetes e melhorar a mentalidade de segurança da informação nos sistemas informacionais do Exército Brasileiro e assim aumentar a capacidade de proteção cibernética e operacionalidade dos elementos apoiados bem como melhorar a eficiência e segurança da vida administrativa das Organizações Militares.

REFERÊNCIAS

AGUIAR, Bernardo; CORREIA, Walter; CAMPOS, Fábio. Uso da Escala Likert na Análise de Jogos. **Anais do X Simpósio Brasileiro de Games e Entretenimento Digital, 07-09 de novembro de 2011 Salvador**, 2011.

BRASIL. Exército Brasileiro.**R1: Regulamento Interno e dos Serviços Gerais.** Brasília, DF, 2003.

BRASIL. Exército Brasileiro. **EB70-MC-10.232: Guerra Cibernética**. 1ª ed. Brasília, DF, 2017.

BRASIL. Ministério da Defesa. **Aditamento ADAE N° 003/2016 ao Boletim DECEX Nr 32**. Rio de Janeiro, RJ, 2016.

BRASIL. Ministério da Defesa. **MD31-M-0: Doutrina Militar de Defesa Cibernética.** 1ª ed. 2014.

BRASIL. Ministério da Defesa. **Plano de Disciplina e Plano Integrado de Disciplina 2° Ano/ Curso de Comunicações.** Resende, RJ. 2019.

BRASIL. Ministério da Defesa. **Plano de Disciplina e Plano Integrado de Disciplina 3° Ano/ Curso de Comunicações.** Resende, RJ. 2019.

BRASIL. Ministério da Defesa. **Plano de Disciplina e Plano Integrado de Disciplina 4° Ano/ Curso de Comunicações.** Resende, RJ. 2019.

BRASIL. Ministério da Defesa. **Plano de migração para software livre no exército brasileiro**. 3ª ed. Brasília, DF, 2007.

CERT.BR. **Cartilha de segurança para internet**: 2ª. São Paulo: Comitê Gestor da Internet no Brasil, 2012. 140 p.

ERIBERTO, João. **Análise de tráfego em redes tcp/ip**: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional. São Paulo: Novatec, 2013. 416 p.

ERIBERTO, João. **Descobrindo o Linux**: Entenda o sistema operacional GNU/Linux. 3ª ed. São Paulo: Novatec, 2012. 924 p.

ERIBERTO, João. Motivos pelos quais o Exército Brasileiro adotou a distribuição Debian para os servidores de rede. p. 1-4, nov. 2004. Disponível em: <http://eriberto.pro.br/artigos/debian_no_exercito.pdf>. Acesso em: 01 out. 2018.

NETO, Uruban. **Dominando linux firewall iptables**. Rio de Janeiro: Ciência Moderna, 2004. 98 p.

TANENBAUM, ANDREW; BOS, HERBERT. **Sistemas operacionais modernos**. 4ª ed. São Paulo: Pearson Education do Brasil, 2016. 758 p.

VIVA O LINUX. **Iptables - conceitos e aplicação**. Disponível em: <https://www.vivaolinux.com.br/artigo/iptables-conceitos-e-aplicacao>. Acesso em: 14 set. 2018.

WILLIAMSON, Matt. **Livro do pfsense 2.0**: Um guia prático com exemplos ilustrados de configurações, para usuários iniciantes e avançados sobre o PfSense 2.0. 1 ed. [S.L.: s.n.], 2012. 200 p.

ANEXO A – MODELO DE FORMULÁRIO APLICADO

Questionário

Este questionário tem por finalidade ser integrante da pesquisa "Estudo de implementação de ensino do firewall GNU/Linux e IPTables no Plano de Disciplina da formação do Oficial de carreira de Comunicações" e funciona baseado em questões objetivas de acordo com o grau de concordância com cada afirmação em cinco níveis. Sua participação é voluntária e de grande importância para esta pesquisa, você não será identificado e as informações colhidas serão sigilosas, portanto responda livremente da forma que julgar mais coerente com seus pensamentos.

1-Dados gerais:

Idade: _____

Turma de Aula: _____

Concordo em participar deste questionário:

( )Sim ( )Não

2 – Considero ter noção ou conhecimento básico do que é um firewall e para que o mesmo serve:

( )Concordo plenamente

( )Concordo parcialmente

( )Não concordo nem discordo

( )Discordo parcialmente

( )Discordo plenamente

3 – Já tive contato ou configurei algum sistema de firewall em algum momento de minha vida:

( )Concordo plenamente

( )Concordo parcialmente

( )Não concordo nem discordo

( )Discordo parcialmente

( )Discordo plenamente

4 – Em relação ao Sistema Operacional GNU/Linux e seu firewall, tenho ciência da ferramenta IPTables:

( )Concordo plenamente

( )Concordo parcialmente

( )Não concordo nem discordo

( )Discordo parcialmente

( )Discordo plenamente

5 – Considero que os conhecimentos de segurança de redes e operação destes são importantes para o Oficial de Comunicações:

( )Concordo plenamente

( )Concordo parcialmente

( )Não concordo nem discordo

( )Discordo parcialmente

( )Discordo plenamente

6 – Considero que os conteúdos ministrados em segurança de redes/firewalls e sua carga horária ao longo curso de formação do Oficial de Comunicações são suficientes:

( )Concordo plenamente

( )Concordo parcialmente

( )Não concordo nem discordo

( )Discordo parcialmente

( )Discordo plenamente

7 – Me considero apto para gerenciar um firewall e assim garantir controle e segurança das redes em que estiver responsável:

( )Concordo plenamente

( )Concordo parcialmente

( )Não concordo nem discordo

( )Discordo parcialmente

( )Discordo plenamente