ENSINO DE CIBERNÉTICA NO CURSO DE FORMAÇÃO DE OFICIAIS DA ACADEMIA DA FORÇA AÉREA: ANÁLISE DE NECESSIDADES E IMPACTOS[1]

TEACHING CYBERNETICS IN THE AIR FORCE ACADEMY OFFICER TRAINING COURSE: NEEDS AND IMPACTS ANALYSIS

Autor: Rafael de Oliveira Guedes[2]
Orientador: Guilherme Augusto Spiegel Gualazzi[3]

RESUMO

O presente trabalho tem como objetivo analisar a necessidade e os impactos do ensino da disciplina de cibernética no Curso de Formação de Oficiais (CFO) da Academia da Força Aérea (AFA), considerando a crescente importância da segurança no ciberespaço para as instituições civis e militares. diante do cenário em que, em 2022, 78% das empresas brasileiras sofreram roubos de dados por meio de ataques de *phishing*, e 23% delas enfrentaram prejuízos financeiros (PROOFPOINT, 2023), a cibernética revela-se como uma área crítica para a proteção de informações e operações estratégicas. Para atingir o objetivo proposto, foi realizada uma pesquisa qualitativa de caráter descritivo e interpretativo, baseada em revisão bibliográfica e análise documental. Foram examinados documentos elaborados pelo Ministério da Defesa, pelo Grupo de Trabalho (GT) de 2021, além de conteúdos do Comando da Aeronáutica, do Projeto Pedagógico de Curso (PPC) da AFA e do Perfil Profissional dos Oficiais da Aeronáutica (PPOA). Também foram analisados Manuais (MCA), Diretrizes (DCA) e Planos (PCA) do Comando da Aeronáutica, com o intuito de verificar a adequação do conteúdo programático da disciplina de cibernética às demandas impostas pelo cenário atual de ameaças cibernéticas. Como resultado, identificou-se a necessidade de fortalecimento do ensino de cibernética como elemento essencial para a formação de oficiais capazes de proteger informações estratégicas e garantir a continuidade de operações críticas. Conclui-se que a inserção e o desenvolvimento contínuo da disciplina no currículo do CFO são fundamentais para atender aos imperativos da Estratégia Nacional de Defesa (END) e do Plano Nacional de Defesa (PND), fortalecendo a soberania nacional no ambiente cibernético.

Palavras-chave: Cibernética; Tecnologia da Informação; Academia da Força Aérea.

---

[1]Artigo de Conclusão de Curso apresentado ao Curso de Formação de Oficiais Aviadores (CFOAv) da Academia da Força Aérea (AFA)

[2] Cadete Aviador do 4º Esquadrão (Turma *Ártemis*, 2025).

[3]Possui graduação em Análise de Sistemas pela Universidade Metodista de Piracicaba (1992), especialização em Engenharia de Software pela UNICAMP (2005), mestrado em Engenharia de Produção (2000) e doutorado em Engenharia de Produção pela Universidade Metodista de Piracicaba (2010). É Professor Titular do Magistério Superior Federal, lotado na Academia da Força Aérea (AFA). Tem experiência na área de Ciências da Computação, atuando principalmente nos seguintes temas: gestão da informação, segurança da informação, tecnologia e sistemas de informação. Realizou o estágio de pós-doutorado na Faculdade de Zootecnia e Engenharia de Alimentos - USP-Pirassununga-SP (2018), onde desenvolveu pesquisa sobre ARP aplicada à zootecnia de precisão. E-mail: gualazzigasg@fab.mil.br

ABSTRACT

This study aims to analyze the necessity and impacts of teaching the discipline of cybernetics in the Officer Training Course (CFO) of the Air Force Academy (AFA), considering the growing importance of cybersecurity for both civilian and military institutions. In a context where, in 2022, 78% of Brazilian companies suffered data breaches through *phishing* attacks, and 23% of them experienced financial losses, cybernetics emerges as a critical area for the protection of strategic information and operations. To achieve the proposed objective, a qualitative, descriptive, and interpretative research was conducted, based on a bibliographic review and document analysis. Documents produced by the Ministry of Defense, the 2021 Working Group (GT), as well as contents from the Air Force Command, the Course Pedagogical Project (PPC) of AFA, and the Professional Profile of Air Force Officers (PPOA) were examined. Additionally, manuals (MCA), guidelines (DCA) and plans (PCA) from the Air Force Command were analyzed to assess the adequacy of the cybernetics curriculum in addressing the current challenges posed by the cyber environment. As a result, the study identified the need to strengthen the teaching of cybernetics as an essential element in the formation of officers capable of protecting strategic information and ensuring the continuity of critical operations. It is concluded that the inclusion and continuous development of the cybernetics discipline in the CFO curriculum are fundamental to meet the imperatives established by the National Defense Strategy (END) and the National Defense Plan (PND), thereby strengthening national sovereignty in the cyber domain.

Keywords:Cybernetics; Information Technology; Air Force Academy.

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AFA – Academia da Força Aérea
CCAER – Corpo de Cadetes da Aeronáutica
DCA – Diretrizes do Comando da Aeronáutica
END – Estratégia Nacional de Defesa
FAB – Força Aérea Brasileira
GT – Grupo de Trabalho
ICA – Instrução do Comando da Aeronáutica
MCA – Manuais do Comando da Aeronáutica
PCA – Plano do Comando da Aeronáutica
PND – Programa Nacional de Defesa
PPC – Projeto Pedagógico de Curso
PPOA – Perfil Profissional do Oficial da Aeronáutica
TCC – Trabalho de Conclusão de Curso
TIC – Tecnologia da Informação e Comunicação
USP – Universidade de São Paulo

SUMÁRIO

INTRODUÇÃO

A cibernética, originalmente desenvolvida no contexto da Guerra Fria, consolidou-se como um campo estratégico vital para as operações militares contemporâneas. A crescente interdependência dos sistemas de informação e a intensificação das ameaças cibernéticas transformaram o ambiente digital em um dos principais teatros de conflito moderno. No Brasil, embora não haja envolvimento direto em guerras cibernéticas internacionais, dados recentes apontam para um cenário alarmante: em 2022, o país sofreu mais de 100 bilhões de tentativas de ataques cibernéticos, afetando tanto instituições públicas quanto privadas (Jornal da USP, 2023). Este contexto revela a necessidade de preparar as Forças Armadas para enfrentar os desafios impostos pelo ciberespaço.

Diante dessa realidade, a Força Aérea Brasileira (FAB) reconheceu a importância da capacitação cibernética em seus quadros, conforme explicitado na Diretriz do Comando da Aeronáutica – DCA 11-45/2018 (Brasil, 2018) e na Estratégia Nacional de Defesa – END (BRASIL, 2020). Em resposta a essa demanda, o Ministério da Defesa, por meio do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética, propôs a inserção estruturada da disciplina de cibernética nos cursos de formação militar, incluindo os cursos ministrados na Academia da Força Aérea (AFA).

Neste contexto, o objeto de estudo deste trabalho é o ensino de cibernética na AFA, com especial atenção à análise do conteúdo programático proposto para atender aos diferentes perfis formativos da instituição. O cenário da pesquisa se delineou a partir da constatação do aumento exponencial das ameaças cibernéticas e da consequente necessidade de formar oficiais com competências específicas para atuar nesse domínio. A investigação busca, portanto, compreender se o currículo proposto atende de maneira adequada às exigências impostas pelo atual panorama de segurança cibernética.

Assim, o problema de pesquisa que norteia este estudo pode ser expresso da seguinte forma: O conteúdo programático da disciplina de cibernética a ser implementada na AFA atende às necessidades de formação impostas pelos recentes desafios cibernéticos enfrentados pelo Brasil? Esta questão é relevante por se situar em um momento de crescente dependência tecnológica, em

que a formação de profissionais aptos a proteger sistemas críticos é vital para a soberania nacional. É também viável, visto que existem documentos oficiais, dados sobre ataques cibernéticos e referenciais teóricos disponíveis para análise. Sua oportunidade se justifica pela recente movimentação institucional voltada à implementação efetiva do ensino de cibernética nos currículos da AFA.

O objetivo geral deste trabalho é analisar os tópicos a serem abordados na disciplina de cibernética proposta pelo Ministério da Defesa, em comparação com os diferentes tipos de ataques cibernéticos sofridos pelo Brasil. Para isso, foram definidos os seguintes objetivos específicos: (i) levantar os dados históricos de ataques cibernéticos sofridos pelo Brasil; (ii) detalhar e analisar o conteúdo programático proposto pelo Ministério da Defesa; (iii) comparar o conteúdo programático com os principais tipos de ataques registrados; e (iv) apresentar conclusões e considerações sobre a adequação da formação proposta.

A justificativa para a realização desta pesquisa está ancorada na necessidade de assegurar que a formação dos futuros oficiais da FAB, provenientes da Academia da Força Aérea, seja compatível com os desafios apresentados até o momento no século XXI, especialmente no âmbito da segurança cibernética. A relevância acadêmica reside na contribuição para a reflexão crítica sobre o currículo de formação militar; já a relevância prática se traduz no fortalecimento das capacidades operacionais da FAB no domínio cibernético. Considerando o caráter exploratório e analítico da pesquisa, não se formula uma hipótese fechada, mas trabalha-se com a premissa de que a atualização constante do currículo é condição indispensável para a eficácia das ações de defesa cibernética.

1 REFERENCIAL TEÓRICO

1.1 Cibernética

Estudos sobre Cibernética podem ser observados durante diversos períodos na história, entretanto, o tema foi abordado pela primeira vez em 1948 no livro “Cybernetics: or the Control and Communication in the Animal and the Machine” de Norbert Wiener. Suas ideias definem a cibernética como a teoria de comando, controle e transmissão de informações, aplicável tanto a máquinas quanto a seres vivos, ou seja, os sistemas seja de natureza biológica, social ou tecnológica respondem “mensagens” provenientes do mundo externo e são possíveis de serem reduzidas a modelos matemáticos.

Além disso, de acordo com Gabáldon e Pereira (2008), essa ciência colaborou no desenvolvimento de computadores/tecnologia através do conceito de controle e comunicação, onde seus princípios foram aplicados no funcionamento de máquinas por meio de sistemas de controle que utilizam *feedback* para ajustar e otimizar seu desempenho. Isso envolve a coleta e análise de dados de saída, que são usados para ajustar as entradas, permitindo que a máquina se adapte a mudanças no ambiente ou nas condições de operação. Além disso, utilizam-se modelos matemáticos para descrever e prever o comportamento de sistemas complexos, o que facilita a automação e aumenta a eficiência de processos mecânicos e eletrônicos. Dessa forma a cibernética ajudou a estabelecer a base teórica para a automação e a inteligência artificial, integrando a lógica de *feedback* e adaptação em sistemas computacionais.

Os princípios dessa ciência podem ser utilizados tanto para a defesa como sistemas, como por exemplo, o de aproximação de mísseis (MAWS) quanto para a exploração de sistemas digitais. Pessoas com conhecimentos avançados nessa área são capazes de manipular e explorar vulnerabilidades em redes e sistemas, criando um ambiente de constante feedback e adaptação. De tal maneira a cibernética fornece uma base para entender as dinâmicas de interação entre atacantes e sistemas, refletindo a complexidade das relações no ciberespaço. Nesse sentido, Cortez e Kubota (2013) afirmam que o investimento em educação e treinamento em segurança da informação desempenha um papel crucial na mitigação de riscos cibernéticos. Embora as medidas tecnológicas, como por exemplo, *firewalls* e sistemas de detecção de intrusões, sejam essenciais, a fragilidade em segurança cibernética frequentemente está associada à falta de conscientização e preparo dos usuários.

As firmas (empresas/instituições) que investem no treinamento de seus funcionários em Tecnologias da Informação e Comunicação (TIC) são mais aptas a identificar e mitigar incidentes cibernéticos. Conforme demonstrado por Cortez e Kubota (2013), há uma relação significativa entre o investimento em políticas de segurança, treinamento em TIC e a maior probabilidade de identificação de problemas de segurança da informação. No contexto das Forças Armadas, onde as vulnerabilidades cibernéticas podem comprometer diretamente a segurança nacional, o treinamento contínuo do efetivo é indispensável para garantir a resiliência das operações frente a ameaças externas.

1.2 *Malware*

O termo *malware* refere-se a qualquer software ou código de computador desenvolvido com o objetivo de se infiltrar em sistemas, causar danos, roubar informações ou comprometer a integridade e a privacidade dos dispositivos. De acordo com a Avast (2024), o malware é uma ameaça ampla que engloba diferentes tipos de programas maliciosos, como vírus, *worms*, cavalos de Troia, *spyware*, *adware*, *botnets*, *rootkits* e *ransomware*, sendo cada um deles projetado para atuar de forma específica, mas sempre com o intuito de violar a segurança digital.

Embora, popularmente, o termo vírus seja usado como sinônimo de malware, tecnicamente nem todo *malware* é um vírus. Enquanto o vírus é um tipo específico de malware que se replica e se espalha entre dispositivos e redes, o conceito de *malware* é mais amplo, incluindo qualquer código malicioso que atue de forma furtiva, muitas vezes sem o conhecimento do usuário, para explorar vulnerabilidades e executar ações prejudiciais.

Segundo informações da Avast (2024), o funcionamento do *malware* costuma seguir um padrão básico: a infecção do dispositivo ocorre geralmente por meio de downloads não intencionais, como ao clicar em links suspeitos em e-mails, visitar sites que estejam comprometidos ou baixar arquivos infectados de plataformas de compartilhamento. Além disso, técnicas como a disseminação por pen drives com *firmware* modificado (que escondem códigos maliciosos) ilustram a evolução dos métodos utilizados pelos cibercriminosos para burlar sistemas de segurança tradicionais.

A motivação principal por trás do uso de *malware* está relacionada à obtenção de ganhos ilícitos, como extorsão, fraude financeira, roubo de identidade e acesso indevido a dados sensíveis. Ferramentas maliciosas amplamente disponíveis na *dark web*[4] facilitam o acesso a códigos prontos, ampliando o alcance de ataques mesmo para cibercriminosos com conhecimentos limitados. Dessa forma, o *malware* tornou-se uma peça central no cenário de crimes cibernéticos, destacando-se como uma ameaça global para dispositivos de diferentes plataformas, incluindo computadores, smartphones e outros equipamentos conectados.

[4] A dark web é uma parte oculta da internet acessível apenas por softwares especiais, usada para manter o anonimato e onde muitas vezes ocorrem atividades ilegais.

1.3 *Phishing*

De acordo com Aleroud e Zhou (2017), o *phishing* é uma forma de ataque em que os criminosos se aproveitam de técnicas de engenharia social[5] para realizar o roubo de identidade. Geralmente, o ataque ocorre através do envio de e-mails fraudulentos que imitam sites legítimos, como bancos online, plataformas de pagamento ou leilões virtuais. Esses e-mails conduzem os usuários para páginas falsas que foram cuidadosamente elaboradas para se parecer com as verdadeiras. O intuito do *phishing* é obter informações confidenciais, como nomes de usuários, senhas, números de cartões de crédito e até recursos financeiros, através da falsa representação de uma entidade confiável. Aleroud e Zhou (2017) observam que o *phishing* é caracterizado por três elementos principais: 1) a falsificação de uma entidade legítima; 2) o uso de um website no processo de fraude, o que o diferencia de outros esquemas, como o *muling*[6]; e 3) a solicitação de dados sensíveis da vítima, relacionados à entidade falsa.

De acordo com o relatório "Cost of a Data Breach" da IBM (IBM, 2024), tal forma de ataque cibernético é a prática mais comum , compondo 16% do montante das violações. Custando as organizações uma média de US$4,88 milhões no período de março de 2023 a fevereiro de 2024. Além disso , de acordo com um estudo da PSAFE (PSAFE, 2021), o Brasil foi um dos países mais afetados por ataques de *phishing*, com mais de 150 milhões de brasileiros sendo vítimas desse tipo de golpe. Esses ataques ocorreram principalmente por meio de e-mails e mensagens fraudulentas que imitavam páginas de bancos e lojas virtuais, com o objetivo de roubar dados bancários e pessoais dos usuários. Esse aumento foi especialmente perceptível durante a pandemia, quando houve uma maior adoção de serviços digitais por parte da população.

1.4 *Ransomware*

Segundo o Laboratório Nacional de Computação Científica (LNCC), *Ransomware* é uma espécie de *software* malicioso que é projetado para sequestrar dados, criptografando arquivos e tornando-os inacessíveis para o usuário, Após a infecção, o agente mal intencionado exige um

[5] Engenharia social é o uso de técnicas de persuasão psicológica para enganar indivíduos e induzi-los a revelar informações confidenciais ou realizar ações que comprometam a segurança de dados e sistemas.

[6] Mulling é uma técnica criminosa que consiste em recrutar pessoas, chamadas de *mules* (ou "mulas"), para transportar ou movimentar bens ilícitos, dinheiro ou produtos obtidos de forma ilegal, ajudando a ocultar a origem do crime. É muito usada em esquemas de fraude financeira, lavagem de dinheiro e contrabando.

pagamento, ou “resgate”, para fornecer a chave de descriptografia e restaurar o acesso aos dados. Essa ameaça se tornou um problema crescente, causando perdas e danos a instituições brasileiras. Geralmente essa prática é acompanhada por uma mensagem de sequestro que aparece na tela do usuário informando sobre a criptografia dos dados e exigindo um pagamento. Além disso, muitos *Ransomware* tentam modificar a extensão dos arquivos a fim de dificultar sua localização por parte do usuário. Nesse sentido, de acordo com a Forbes (2021), as Lojas Renner foram alvo de um dos maiores ataques de *ransomware* registrados no Brasil. Os criminosos sequestraram dados da empresa, exigindo o pagamento de resgate em criptomoedas para desbloquear os sistemas comprometidos. Como resultado, a operação da empresa foi interrompida temporariamente, causando grandes prejuízos financeiros e uma queda na reputação da marca no mercado varejista.

1.5 *Backdoor*

De acordo com a definição do site CeCyber (2022), um *backdoor* é uma espécie de *Malware* que dá a possibilidade que indivíduos acessem remotamente seu sistema sem passar pelos métodos normais de autenticação. Isso entrega acesso de maneira remota a arquivos e bancos de dados, permitindo o uso de comandos e a instalação de outros *malwares*. Existem diversas formas e situações do uso de *backdoor* (NordVPN, 2023), sendo elas: *Backdoor* malicioso: abrange *backdoor* que são projetados deliberadamente para facilitar o ataque de criminosos cibernéticos, dando acesso a dados dos usuários e monitorando suas atividades. Um exemplo que poderia ser dado seriam programas de antivírus gratuitos que alguns contêm códigos maliciosos que permitem que outros indivíduos acessem o dispositivo das vítimas; *Backdoor zero-day*: basicamente os criminosos se aproveitam de falhas de seguranças que não foram identificadas pelos desenvolvedores. Um caso conhecido foi EternalBlue, desenvolvido pela Microsoft, que foi utilizado pela Agência de Segurança Nacional dos EUA (NSA), para obter acesso de *back-end* a dispositivos com sistemas operacionais Windows. Depois de descobrirem uma vulnerabilidade nesse sistema já era tarde, hackers já haviam utilizado essa brecha, colocando milhões de usuários em risco; *Backdoors* acidentais: São erros que deixam sensibilidades na aplicação que podem posteriormente serem utilizadas por outras pessoas, diferente do zero-day, ele não necessariamente ocorre no lançamento de um software. *Backdoor* de hardware: Muito se falou sobre *backdoor* em aplicações e softwares, no entanto é possível colocá-los no hardware, ou seja, na própria estrutura física de um dispositivo. Todavia, é mais arriscado exigir acesso físico ao equipamento e portanto

não é muito utilizado. Nesse viés, o Exército Brasileiro identificou, em 2013, vulnerabilidades em diversos equipamentos de rede importados, como roteadores e switches. Esses dispositivos continham *backdoors* embutidos, o que permitia que invasores obtivessem acesso não autorizado às comunicações militares. Além disso, de acordo com o site Exame (2013), o general Sinclair Mayer, à época chefe do Departamento de Ciência e Tecnologia do Exército, destacou a importância de maior controle sobre a origem e configuração de equipamentos utilizados pelas Forças Armadas.

1.6 *DDos(Distributed of Denial of Service)*

Distributed of Denial of Service refere-se a uma tentativa de deixar algum *software* ou aplicação indisponível por meio de sobrecarga de recursos, seja memória ou capacidade de processamento. Geralmente são realizados enviando um grande volume de solicitações, fazendo com que o servidor falhe e fique indisponível. Esses ataques podem ser realizados por uma única máquina ou uma rede de dispositivos conhecidos por *botnets*, que basicamente são dispositivos "sequestrados" fazendo parte de um esquema de várias camadas com fins diversos, seja derrubada de servidores ou roubo de dados. Com o avanço tecnológico, essas ferramentas ficam mais acessíveis a criminosos com um conhecimento limitado, exigindo que as organizações fiquem atentas e vigilantes, com suas defesas atualizadas. Em 2023, ataques *DDoS* afetaram o portal Gov.br, sobrecarregando os servidores com um grande volume de acessos simultâneos. Esses ataques causaram instabilidades nos serviços oferecidos pelo governo federal, como o acesso a documentos e programas sociais. Esse incidente destacou a crescente vulnerabilidade de sistemas governamentais a esse tipo de ameaça, que utiliza redes de dispositivos sequestrados, conhecidos como botnets, para realizar os ataques (FEBRABAN TECH, 2023).

1.7 *Spoofing*

Segundo Wu e Li (2015), o spoofing refere-se a um ataque no qual o invasor busca manipular sistemas de autenticação, com o intuito de enganar o mecanismo de verificação e fazer com que uma identidade falsa seja aceita como legítima. No contexto de sistemas de verificação

automática de fala, esse tipo de ataque pode ocorrer por meio de métodos como imitação de voz, reprodução de gravações de áudio, síntese de fala ou conversão de voz. Além disso, o spoofing também se manifesta em outras modalidades biométricas, como impressões digitais falsificadas, uso de máscaras faciais ou fotos em sistemas de reconhecimento facial, bem como em ataques de falsificação de IP, e-mails ou sinais em redes de comunicação. Tais técnicas visam criar uma correspondência fraudulenta com a identidade de um usuário autorizado, comprometendo a segurança de diferentes sistemas de autenticação. A crescente vulnerabilidade a ataques de spoofing tem despertado a atenção da comunidade científica, que se dedica ao desenvolvimento de contramedidas eficazes para enfrentar esses desafios.

Casos de *spoofing* no Brasil têm afetado bancos que utilizam sistemas de verificação por voz. Criminosos utilizam gravações de áudio e técnicas de conversão de voz para enganar esses sistemas, conseguindo acesso a contas bancárias de clientes. Esse tipo de ataque levanta questões sobre a segurança de sistemas biométricos e levou instituições financeiras a reforçarem suas medidas de autenticação (IBM, 2024).

1.8 O Relatório do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética nas Forças Armadas

O Relatório do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética nas Forças Armadas, elaborado em 2021, estabelece diretrizes para que ocorra a padronização do ensino de cibernética nas nossas 3 forças, abrangendo o Exército, a Marinha e a Aeronáutica. Esse relatório surge da necessidade de alinhar as formações acadêmicas em cibernética , considerando o crescente papel da segurança da informação e a integração de tecnologias avançadas nas operações militares. O documento destaca a cibernética como essencial para a segurança nacional, pois as ameaças podem acabar por afetar infraestruturas críticas de maneira direta, sistemas de comando controle e até mesmo a soberania de um país. Para lidar com esses riscos, o Grupo de Trabalho (GT) recomendou a criação de um currículo mínimo padronizado, a ser adotado nas escolas de formação. O objetivo é garantir que todos os militares que lidam com tecnologia da informação tenham uma formação uniforme e eficiente (BRASIL, 2021).

O relatório estabelece três níveis de formação, sendo eles: Básico, Intermediário e Avançado. Cada um voltado ao perfil de atuação dos militares após sua formação. Esses perfis vão

desde operadores de sistemas administrativos até administradores de redes e gestores de segurança cibernética, abrangendo áreas de conhecimento como proteção de sistemas, criptografia, gerenciamento de incidentes e defesa cibernética em operações militares (BRASIL, 2021). Na Academia da Força Aérea (AFA), a adoção dessas diretrizes visa garantir que os cadetes do Curso de Formação de Oficiais (CFO) tenham a preparação necessária para enfrentar os desafios do ambiente cibernético. No caso da AFA, foi decidido que o perfil intermediário será implementado, buscando fornecer aos cadetes uma formação sólida e prática em defesa cibernética. O relatório também destaca a importância de conscientização contínua por meio de palestras e treinamentos, além da necessidade de atualização constante do currículo para acompanhar a evolução das ameaças e tecnologias (BRASIL, 2021).

Dessa forma, o relatório do GT serve como uma importante base teórica para a avaliação do conteúdo programático da disciplina de cibernética na AFA. Neste estudo, serão comparados os tópicos sugeridos pelo relatório com os principais ataques cibernéticos sofridos pelo Brasil nos últimos anos, com a finalidade de verificar se o programa de formação desse setor na AFA é adequado para capacitar os futuros oficiais a lidarem com essas ameaças.

O quadro 1 (Área de Concentração e Linhas de Pesquisa) abaixo apresenta as linhas de pesquisa recomendadas para o ensino de defesa cibernética nas Forças Armadas, conforme o Relatório do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética (Brasil,2021). Essas linhas estão organizadas por áreas de concentração, como Criptografia, Segurança de Sistemas, Legislação, entre outras, e servem de base para orientar o que deve ser ensinado em todos os níveis de formação cibernética (básico, intermediário e avançado). Cada área agrupa temas que são importantes para a formação de profissionais de defesa cibernética, desde fundamentos teóricos, como Doutrina e Direito Cibernético, até conteúdos mais técnicos, como Análise de *Malware*, Segurança de Redes e Inteligência Artificial aplicada à segurança. Essas linhas de pesquisa ajudam a planejar melhor os conteúdos que devem ser incluídos nos cursos de formação militar dos mais diferentes níveis, desde Escolas de Formação até Escolas de Altos Estudos, garantindo que os alunos estejam preparados para os desafios atuais da segurança digital.

QUADRO 1 Área de Concentração e Linhas de Pesquisa

Disciplina	Linha de Pesquisa
Doutrina	Cibernética
Ciência da Computação	Sistemas de Computação
Segurança de Sistemas	Segurança de Sistemas Operacionais Segurança da WEB Segurança de Sistemas Móveis Segurança de Sistemas Distribuídos Segurança da Computação em Nuvem
Segurança de Rede	Detecção e Prevenção de Intrusão Segurança de Infraestrutura de Rede Ataques de Negação de Serviço e Proteção Segurança de Rede sem Fio
Segurança e Medição baseado em dados	Medição de Fraudes, *Malware* e Spam Medidas de Comportamento Humano e Segurança
Análise de Segurança	Análise de *Malware* Análise de Protocolos de Rede Ataques com novas percepções, técnicas ou resultados Análise Automatizada de Segurança de Projetos e implementação de Hardware Perícia e Diagnósticos para Segurança Análise de Segurança Automatizada de Códigos Fonte e Binários Machine Learning Forense Cibernética
Segurança de Hardware	Arquiteturas Seguras de Computador Segurança de Sistemas Incorporados Método para a Detecção de Hardware malicioso Canais Laterais
Legislação e Ensino	Direito Internacional e Cibernética Legislação e Cibernética Educação e Capacitação em Cibernética
Criptografia	Análise de Criptografia Aplicada e Protocolos Criptográficos Análise de Implementação Criptográfica Novos Protocolos Criptográficos

Fonte: Elaborado pelo autor, com base em: BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Defesa Cibernética. *Relatório GT-ENaDCiber*. Brasília, DF, 2021.

2 METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa de natureza qualitativa, de caráter descritivo e exploratório. Optou-se por esta abordagem por permitir uma análise mais aprofundada dos documentos e contextos relacionados ao ensino de cibernética na formação militar, bem como das demandas impostas pelo ambiente cibernético contemporâneo.

O universo da pesquisa compreende os cursos de formação da Academia da Força Aérea (AFA), com foco específico na disciplina de cibernética prevista para ser implementada, conforme orientação do Ministério da Defesa e recomendações do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética das Forças Armadas. A análise abrange os diferentes perfis de formação existentes na AFA, considerando a proposta de trilhas curriculares voltadas ao desenvolvimento de competências específicas no domínio cibernético, conforme sugerido pelo Relatório do GT.

Como amostra de análise, foram utilizados documentos institucionais oficiais, como o Relatório do Grupo de Trabalho de Defesa Cibernética (BRASIL, 2021), a Estratégia Nacional de Defesa (END) (BRASIL, 2020), o Plano Nacional de Defesa (PND) (BRASIL, 2020), bem como diretrizes e planos do Comando da Aeronáutica – a exemplo da DCA 11-45/2018 (COMANDO DA AERONÁUTICA, 2018) e do PCA 37-11/2017 (COMANDO DA AERONÁUTICA, 2017). Além disso, foram consultados relatórios de mercado especializados que relatam a incidência e as características dos ataques cibernéticos sofridos pelo Brasil nos últimos anos, como os relatórios anuais da Proofpoint (2023) e da Check Point Research (2023).

Os instrumentos de coleta de dados consistiram em pesquisa bibliográfica e documental. A pesquisa bibliográfica foi realizada com base em estudos acadêmicos, relatórios técnicos e legislações pertinentes à cibernética, segurança da informação e defesa cibernética. A pesquisa documental teve como principal foco a análise de documentos normativos da FAB e do Ministério da Defesa, bem como dados estatísticos sobre ataques cibernéticos registrados.

Para o tratamento e análise dos dados, empregou-se a técnica de análise de conteúdo, com a sistematização e categorização dos tópicos relevantes à formação cibernética e à ocorrência dos ataques. Procedeu-se à comparação entre os conteúdos previstos na proposta de ensino e as demandas reais evidenciadas pelos incidentes cibernéticos registrados, buscando identificar

eventuais lacunas, convergências e oportunidades de aprimoramento. A escolha por este método de análise justifica-se por sua adequação em estudos que exigem interpretação crítica e construção de inferências baseadas em evidências documentais.

Quanto aos limites metodológicos, destaca-se a restrição à disponibilidade e à atualidade de documentos públicos e relatórios sobre segurança cibernética, o que pode impactar a abrangência da análise. Além disso, por tratar-se de uma pesquisa baseada majoritariamente em fontes secundárias, eventuais lacunas nas informações originais também constituem limitações a serem consideradas.

Por fim, ressalta-se que o percurso metodológico adotado está alinhado com o objetivo de oferecer uma avaliação crítica e fundamentada sobre a adequação do ensino de cibernética na formação dos oficiais da AFA, contribuindo para a evolução e o aprimoramento da capacitação militar no domínio cibernético, em conformidade com as exigências contemporâneas de defesa nacional.

3 RESULTADOS E DISCUSSÕES

O avanço tecnológico das últimas décadas trouxe, além de inovações significativas para a sociedade, um novo cenário de ameaças que impactam diretamente a segurança nacional. O ambiente cibernético, cada vez mais presente nas operações militares, exige das Forças Armadas uma adaptação permanente no preparo de seus quadros. Nesse contexto, foi conduzida a presente pesquisa, que analisou o conteúdo programático de cibernética proposto pelo Grupo de Trabalho (GT) de Alinhamento do Ensino de Defesa Cibernética, em comparação com as ameaças cibernéticas efetivamente enfrentadas pelo Brasil.

3.1 Levantamento de dados e cenário atual

O Brasil vem enfrentando, nos últimos anos, uma intensificação significativa nas ameaças cibernéticas. De acordo com levantamentos recentes, apenas no ano de 2022, foram registradas mais de 100 bilhões de tentativas de ataques cibernéticos no país, direcionadas tanto ao setor público quanto ao privado (JORNAL DA USP, 2023). Instituições estratégicas, como a Polícia Federal e o Supremo Tribunal Federal, também foram alvos, evidenciando a vulnerabilidade de estruturas críticas.

Entre os tipos de ataques mais frequentes, destacam-se:

- *Ransomware* e *Malware*: voltados ao sequestro de dados e à interrupção de serviços essenciais;
- *Phishing* e Engenharia Social: técnicas utilizadas para capturar informações sensíveis;
- Ataques *DDoS (Distributed Denial of Service)*: que visam comprometer a disponibilidade de sistemas; e
- Vazamento e Exfiltração de Dados: com impacto direto na segurança institucional.

Essas ameaças vêm se ampliando tanto em número quanto em complexidade. Em 2023, o Brasil foi classificado como o segundo país mais vulnerável a ataques cibernéticos no mundo, em função de fatores como a baixa conscientização sobre *phishing* e infraestrutura de segurança cibernética inadequada (THE RIO TIMES, 2023). No mesmo período, registrou-se que mais de 95% da atividade de *phishing* direcionada a usuários brasileiros foi atribuída a um único grupo criminoso, destacando a fragilidade das defesas nacionais contra esse tipo de ameaça (GOOGLE CLOUD, 2023).

Além disso, o número de ataques de *ransomware* contra o Brasil apresentou um crescimento expressivo. Segundo a Check Point Research (2023), o país foi o segundo mais atacado por *ransomware* na América Latina, com um aumento superior a 37% no número de incidentes em comparação ao ano anterior (CHECK POINT RESEARCH, 2023).

Paralelamente, no ambiente militar, a crescente digitalização das operações impõe a necessidade de formar oficiais capacitados não apenas para operar sistemas complexos, mas também para protegê-los. No entanto, até o momento, a formação em defesa cibernética na Academia da Força Aérea (AFA) ocorre apenas de forma indireta, por meio de conteúdos distribuídos em disciplinas correlatas, sem uma estrutura curricular própria dedicada ao tema.

Neste cenário, o Ministério da Defesa, através do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética, propôs a implantação de uma disciplina específica, estruturada conforme perfis de usuário, entre os quais destaca-se o Perfil Intermediário, destinado a militares que operarão sistemas administrativos e operacionais críticos. A proposta busca adequar a formação militar às novas exigências impostas pelo domínio cibernético contemporâneo.

3.2 Análise do Conteúdo Programático Proposto

A trilha formativa sugerida pelo Relatório do GT para o Perfil Intermediário contempla 60 horas de instrução, divididas entre as seguintes áreas:

Quadro 2 Carga horária do perfil intermediário

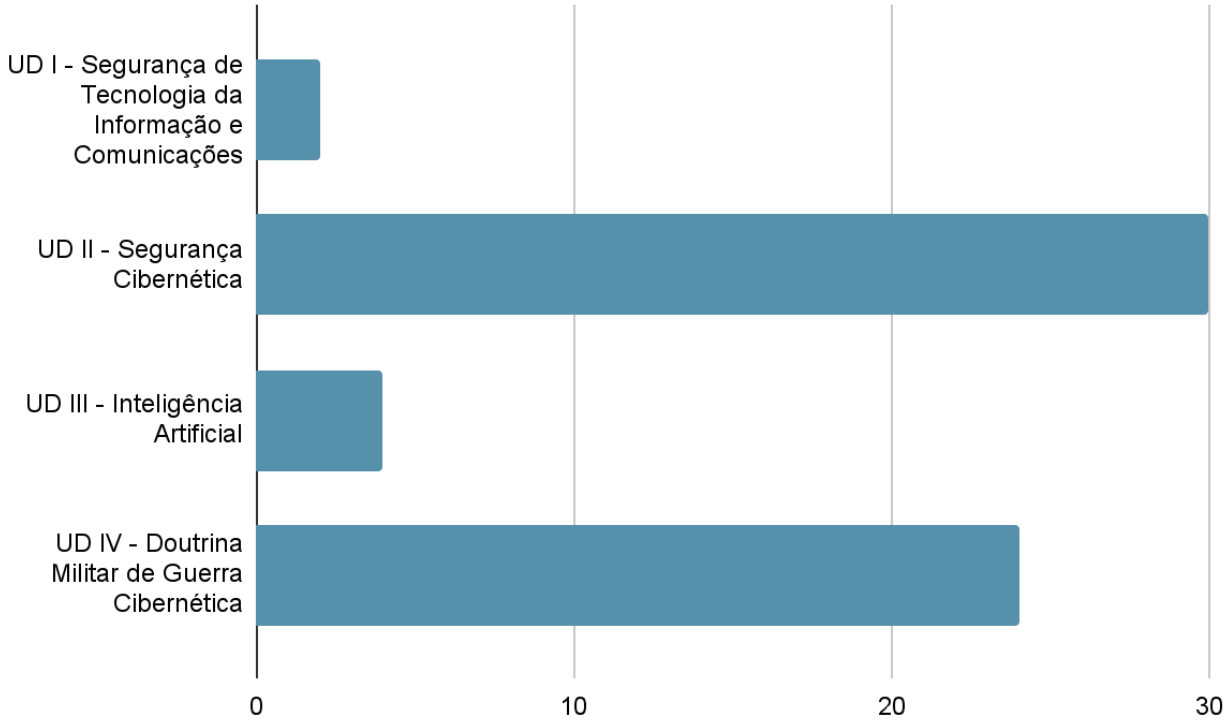
Disciplinas	Carga Horária	Unidade didática
1. Fundamentos de Segurança da Informação 2. Segurança na Internet 3. Segurança em dispositivos móveis 4. Mídias Sociais 5. Lei Geral de Proteção de Dados (LGPD) 6. Atuação de Hackers (Ataques Cibernéticos)	02h	UD I - Segurança de Tecnologia da Informação e Comunicações (Palestra)
1. Fundamentos de Segurança Cibernética 2. Tipos de Ataque 3. Códigos Maliciosos (*Malware*) 4. Criptografia Aplicada 5. Comunicação Segura 6. Ameaças Cibernéticas	30h	UD II - Segurança Cibernética
1. Big Data e Inteligência Artificial.	04h	UD III - Inteligência Artificial
1. Fundamentos de Defesa Cibernética 2. Sistema Militar de Defesa Cibernética 3. Defesa e Guerra Cibernética nas Operações Militares.	24h	UD IV - Doutrina Militar de Guerra Cibernética

Fonte: Elaborado pelo autor, com base em: BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Defesa Cibernética. Relatório GT-ENaDCiber. Brasília,DF, 2021.

Visualmente, a distribuição pode ser observada no Gráfico 1 (Carga horária versus Unidades Didáticas) a seguir, que apresenta a carga horária destinada a cada Unidade Didática proposta para o ensino de defesa cibernética do perfil intermediário. Nota-se que as Unidades Didáticas II (Segurança Cibernética) e IV (Doutrina Militar de Guerra Cibernética) concentram a maior carga horária, com 30 horas cada, refletindo a ênfase prática e estratégica atribuída a esses temas no perfil

de formação. Em contrapartida, a Unidade I (Segurança de TIC) e a Unidade III (Inteligência Artificial) recebem cargas horárias significativamente menores, o que sugere uma abordagem introdutória ou complementar dessas áreas no contexto do curso.

Gráfico 1 Carga horária versus Unidades Didáticas



Fonte: Elaborado pelo autor, com base em: BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Defesa Cibernética. Relatório GT-ENaDCiber. Brasília, DF, 2021.

A estrutura curricular sugerida pelo Relatório do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética (BRASIL, 2021) concentra esforços nas seguintes competências: proteção cibernética de sistemas militares, abordando ameaças e defesas técnicas; compreensão da guerra cibernética no ambiente militar, incluindo aspectos doutrinários; introdução a tecnologias emergentes, como inteligência artificial aplicada à segurança; e sensibilização para segurança de informações e mídias digitais. Essas competências compõem a base formativa do perfil intermediário proposto para os cursos de formação de oficiais das Forças Armadas, incluindo os ministrados na Academia da Força Aérea (AFA). O equilíbrio entre fundamentos técnicos e doutrina militar aponta para uma proposta que busca formar oficiais com visão operacional e estratégica do domínio cibernético.

3.3 Discussão dos Resultados

A análise comparativa entre o cenário atual de ameaças cibernéticas e o conteúdo programático proposto evidencia avanços significativos no ensino de cibernética na Academia da Força Aérea (AFA), embora alguns pontos ainda demandem aprimoramento.

O currículo proposto contempla, de forma geral, as principais ameaças detectadas no ambiente cibernético contemporâneo:

- *Ransomware* e *malware* são tratados nas disciplinas de Segurança Cibernética e Hardening de Sistemas[7].
- Engenharia social e *phishing* são abordados nas palestras de Segurança de TIC e em conteúdos de políticas de segurança da informação.
- Ataques *DDoS* e vulnerabilidades de rede aparecem nos tópicos de segurança de redes e monitoramento de tráfego.

Apesar da grande abrangência de temas, a análise dos conteúdos revela algumas fragilidades. Em especial, a carga horária destinada à Inteligência Artificial, com cerca de apenas quatro horas, conforme o Relatório do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética (BRASIL, 2021) , mostra-se reduzida diante da relevância crescente dessa tecnologia no contexto da segurança cibernética. A literatura especializada aponta que a Inteligência Artificial tem sido amplamente empregada em vetores de ataque como *deepfakes*, automação de phishing, malwares adaptativos e técnicas de evasão que dificultam a detecção de intrusos (WU; LI, 2015). Segundo a Proofpoint (2023), há um aumento significativo no uso de automação em ameaças que exploram vulnerabilidades humanas e técnicas, exigindo que os profissionais de defesa estejam preparados para identificar e mitigar riscos emergentes.

Em comparação com programas de formação introdutória sobre Inteligência Artificial oferecidos por instituições brasileiras, observa-se que a carga horária de quatro horas é consideravelmente inferior. Por exemplo, a Universidade Federal da Bahia (UFBA) oferece o curso “Capacitação em Inteligência Artificial” com 30 horas de duração; a Universidade Estadual do Rio Grande do Sul (UERGS) ministra o curso “Inteligência Artificial no Mundo Acadêmico” com 40 horas; o Instituto Federal de São Paulo (IFSP) promove o curso “Introdução à Inteligência Artificial para Tomada de Decisões” com 76 horas; e a Universidade Corporativa Semesp oferece “Introdução à Inteligência Artificial para Educadores do Ensino Superior” com 10 horas também voltado à introdução conceitual do tema.

[7] Hardening de sistemas é o processo de reforçar a segurança de um sistema computacional (como servidores, redes ou dispositivos) por meio da eliminação de vulnerabilidades e redução da superfície de ataque.

Diante desses parâmetros, constata-se que a alocação de apenas quatro horas para o estudo de Inteligência Artificial na formação militar é significativamente inferior até mesmo aos cursos introdutórios de nível civil, o que reforça a necessidade de ampliação desse conteúdo e de inserção de atividades práticas voltadas à aplicação da IA em segurança cibernética. Tal medida é essencial para alinhar a formação dos futuros oficiais às exigências contemporâneas do ambiente digital e aos desafios da guerra cibernética moderna.

Outro aspecto relevante refere-se à natureza das atividades formativas previstas. O Relatório do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética (2021) indica que, inicialmente, o ensino será focado em aulas expositivas e exercícios teóricos, recomendando apenas em uma fase posterior a introdução de práticas simuladas de resposta a incidentes. Essa abordagem limita o desenvolvimento de competências práticas essenciais para a atuação em cenários cibernéticos reais.

Considerando a velocidade de evolução das ameaças digitais, a necessidade de constante atualização do conteúdo programático é imperativa. O ambiente cibernético exige que os futuros oficiais não apenas compreendam os conceitos teóricos, mas também sejam capazes de responder de forma ágil e eficaz a incidentes, utilizando técnicas atualizadas e pensamento crítico diante de novas ameaças.

De maneira geral, a proposta do GT representa um avanço relevante em comparação com a situação anterior da AFA, em que a formação em defesa cibernética era dispersa e pouco estruturada. A implementação de uma disciplina específica, com conteúdos atualizados e práticas operacionais consistentes, é essencial para fortalecer a preparação dos futuros oficiais, ampliando a capacidade da Força Aérea Brasileira de atuar eficazmente no domínio cibernético, em consonância com seus objetivos estratégicos.

4 CONSIDERAÇÕES FINAIS

A crescente digitalização das operações militares e a intensificação das ameaças no ambiente cibernético evidenciam a necessidade de fortalecer a formação dos oficiais da Força Aérea Brasileira (FAB) no domínio cibernético. O levantamento de dados demonstrou que o país figura entre os principais alvos de ameaças cibernéticas no mundo, sofrendo mais de 100 bilhões de tentativas de ataques apenas em 2022. Nesse contexto, formar oficiais capacitados para

compreender, prevenir e mitigar ameaças no ciberespaço tornou-se uma exigência estratégica para a preservação da soberania nacional.

Este trabalho teve como objetivo analisar a adequação do conteúdo programático de cibernética proposto pelo Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética às demandas impostas pelos recentes ataques sofridos pelo Brasil. A análise do conteúdo programático sugerido revelou uma estrutura sólida, com foco nas áreas de segurança cibernética, doutrina militar de guerra cibernética e tecnologias emergentes. Observou-se que as disciplinas propostas abordam de maneira abrangente as principais ameaças enfrentadas atualmente, tais como *ransomware*, *phishing*, *Distributed of Denial Service (DDoS)* e vazamento de dados sensíveis. Contudo, foi identificado que a carga horária dedicada a temas emergentes, como inteligência artificial, poderia ser ampliada para refletir com maior precisão a evolução das ameaças cibernéticas.

O estudo também evidenciou que, até o momento, a formação em defesa cibernética na Academia da Força Aérea se limita a conteúdos dispersos em outras disciplinas e eventos pontuais, carecendo de uma disciplina estruturada e dedicada. A implementação da trilha formativa para o perfil intermediário, conforme proposta pelo Relatório do GT, representa, portanto, um avanço necessário e estratégico.

Retomando o problema de pesquisa: "O conteúdo programático da disciplina de cibernética a ser implementada na AFA atende às necessidades de formação impostas pelos recentes desafios cibernéticos enfrentados pelo Brasil?", os resultados obtidos indicam que, em grande medida, a proposta curricular responde de forma adequada aos desafios identificados. Ainda assim, ajustes pontuais, como o aprofundamento em áreas emergentes e a ampliação da formação prática, são recomendados para garantir maior aderência à complexidade do ambiente cibernético atual.

Em conclusão, a efetiva implantação e constante atualização do ensino de defesa cibernética na AFA são essenciais para preparar os futuros oficiais a atuarem de forma eficiente em todos os domínios operacionais, incluindo o cibernético. A formação proposta não apenas fortalecerá a capacidade de defesa da Força Aérea Brasileira, como também contribuirá para a proteção de infraestruturas críticas e para a preservação da soberania do país frente aos novos desafios impostos pela guerra cibernética contemporânea.

AGRADECIMENTOS

Agradeço à Academia da Força Aérea (AFA) pela formação acadêmica e militar recebida, que proporcionou a base necessária para a realização deste trabalho. Estendo meus agradecimentos ao Ministério da Defesa e aos integrantes do Grupo de Trabalho de Alinhamento do Ensino de Defesa Cibernética, cujas diretrizes e estudos embasaram a pesquisa. Registro, de modo especial, minha gratidão ao Professor Guilherme Augusto Spiegel Gualazzi, pela orientação, incentivo e relevantes contribuições ao longo do desenvolvimento deste estudo.

Dirijo, ainda, um agradecimento sincero à minha família, em especial à minha mãe, Margareth Santos de Oliveira Guedes, exemplo de dedicação e abnegação, que, mesmo nos momentos mais difíceis, nunca permitiu que eu desistisse, ainda que, por diversas vezes, eu tenha sentido vontade de fazê-lo. Ao meu pai, José Sérgio Guedes Filho, cujo esforço e dedicação foram fontes constantes de inspiração e que, cerca de seis anos atrás, incentivou-me a ingressar na Escola Preparatória de Cadetes do Ar (EPCAR), marco inicial dessa trajetória. Ao meu irmão, Gabriel de Oliveira Guedes, que sempre esteve ao meu lado nos momentos da infância e adolescência e que, com seu exemplo, também me serviu de inspiração ao longo da caminhada. À minha namorada, Bianca Piccoli, agradeço pelo apoio incondicional nos momentos mais difíceis, sendo alicerce fundamental para a superação dos inúmeros desafios enfrentados ao longo da formação. A todos os docentes e colegas de curso, que, direta ou indiretamente, colaboraram para a concretização deste trabalho, expresso minha sincera gratidão. A jornada não foi fácil; porém, compreendo que nada na vida que realmente vale a pena é alcançado sem esforço, renúncia e perseverança.

"No que diz respeito ao empenho, ao esforço e à dedicação, não existe meio termo: ou você faz uma coisa bem feita ou não faz." Ayrton Senna.

REFERÊNCIAS

ALEROUD, Ahmed; ZHOU, Lina. Phishing environments, techniques, and countermeasures: A survey. Computers & Security, v. 68, p. 160-196, 2017. DOI: 10.1016/j.cose.2017.04.006.

AVAST. *O que é malware?* Disponível em: https://www.avast.com/pt-br/c-malware. Acesso em: 29 jun. 2025.

BRASIL.COMANDO DA AERONÁUTICA. *Plano de Curso de Formação de Oficiais – PCA 37-11/2017*. Brasília, DF: COMAER, 2017.

BRASIL.COMANDO DA AERONÁUTICA. Diretriz do Comando da Aeronáutica – DCA 11-45/2018. Brasília, DF: COMAER, 2018.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Defesa Cibernética. Escola Nacional de Defesa Cibernética. Relatório GT-ENaDCiber. Brasília, DF, 2021.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa. Brasília, DF: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf. Acesso em: 5 maio 2025.

BRASIL. Ministério da Defesa. *Plano Nacional de Defesa*. Brasília, DF: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf. Acesso em: 19 out 2024.

BRASIL SOFREU MAIS DE 100 BILHÕES DE TENTATIVAS DE ATAQUES CIBERNÉTICOS NO ÚLTIMO ANO. Disponível em: https://jornal.usp.br/radio-usp/brasil-sofreu-mais-de-100-bilhoes-de-tentativas-de-ataques-ciberneticos-no-ultimo-ano/ Acesso em: 5 set. 2024.

CECYBER. Backdoor: o que é e como evitar. Disponível em: https://cecyber.com/blog/backdoor-o-que-e-e-como-evitar/ . Acesso em: 6 out. 2024.

CHAVES, Viviane Hengler Corrêa; BERNARDO, Cristiane Hengler Corrêa. Norbert Wiener: história, ética e teoria. História (São Paulo), v. 39, e2020017, 2020. Disponível em: http://dx.doi.org/10.1590/1980-4369e2020017 . Acesso em: 4 out. 2024.

CHECK POINT RESEARCH. *Cyber Security Report 2023: Cyber Attack Trends*. Check Point Software Technologies, 2023. Disponível em: https://research.checkpoint.com/2023/cyber-security-report-2023-cyber-attack-trends/ . Acesso em: 28 abr. 2025.

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. Revista de Administração, São Paulo, v. 48, n. 4, p. 757-769, 2013.

DE ALMEIDA, M. F. A palavra convence, o exemplo arrasta: uma análise acerca da liderança no Corpo de Cadetes da Aeronáutica. Rio de Janeiro: Universidade da Força Aérea, 2018.

EXAME. *Ministério verificará se há backdoor em equipamentos de rede*. Exame, 28 mar. 2013. Disponível em: https://exame.com/tecnologia/ministerio-verificara-se-ha-backdoor-em-equipamentos-de-rede/. Acesso em: 14 out 2024.

FAN, R. Ministério da Defesa vai investigar backdoors em equipamentos de rede. DefesaNet. Disponível em: https://www.defesanet.com.br/seguranca/ministerio-da-defesa-vai-investigar-backdoors-em-equipamentos-de-rede/ . Acesso em: 6 out. 2024.

FEBRABAN TECH. Brasil é segundo país mais atingido por ciberataques na América Latina, diz relatório. Disponível em: http://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio. Acesso em: 5 out. 2024.

FORBES BRASIL. Lojas Renner é alvo de ataque cibernético. *Forbes Brasil*, 19 ago. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/08/lojas-renner-e-alvo-de-ataque-cibernetico/. Acesso em: 4 out 2025.

GABALDÓN, Luis Gerardo; PEREIRA, Wílmer. Usurpação de identidade e certificação digital: propostas para o controle do fraude eletrônico. Sociologias, [s.l.], n. 20, p. 164-190, 2008. Disponível em: https://doi.org/10.1590/S1517-45222008000200008. Acesso em: 4 out. 2024.

GOOGLE CLOUD. *Cyber Threats Targeting Brazil*. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil/. Acesso em: 28 abr. 2025

IBM. 2024 Cost of a Data Breach Report. http://www.ibm.com/security/data-breach. Acesso em: 12 out. 2024.

KIM, Joon Ho. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. Horizontes Antropológicos, [s.l.], v. 10, n. 21, p. 199-219, 2004. Disponível em: https://doi.org/10.1590/S0104-71832004000100009. Acesso em: 4 out. 2024.

LOBATO,L.; KENKEL, K.Michael. A ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. Google Scielo, [s.l.: s.n.].

MINISTÉRIO DA DEFESA. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Doutrina. Portaria EMAER nº 43/1SC. Manual de Liderança da FAB: MCA 2-1. Boletim do Comando da Aeronáutica, Brasília, DF, 2016.

NordVPN.O QUE É BACKDOOR E COMO SE PROTEGER. Disponível em: https://nordvpn.com/pt-br/blog/backdoor-o-que-e/. Acesso em: 6 out. 2024.

CREDITED. *Denial of Service: o que é e como se proteger*. Credited, [s.d.]. Disponível em: https://credited.com.br/glossario/denial-of-service-o-que-e-e-como-se-proteger/. Acesso em: 7 out 2024.

O QUE ÉPHISHING? IBM. Disponível em: https://www.ibm.com/br-pt/topics/phishing Acesso em: 4 out. 2024.

O QUE É UM RANSOMWARE? Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/o-que-e-um-ransomware. Acesso em: 4 out. 2024.

OLHAR DIGITAL; DI LORENZO, Alessandro. Ataques cibernéticos crescem quase 70% no Brasil em um ano. Disponível em: https://olhardigital.com.br/2024/07/19/seguranca/ataques-ciberneticos-crescem-quase-70-no-brasil-em-um-ano/#:~:text=O%20setor%20de%20Governo%2FFor%C3%A7as%20Armadas%20foi%20o%20segundo. Acesso em: 5 set. 2024.

PROOFPOINT. *State of the Phish 2023*. Relatório anual. 2023. Disponível em: https://itforum.com.br/noticias/phishing-empresas-brasileiras-dinheiro Acesso em: 5 maio 2025.

PSAFE. Phishing atinge 150 milhões de brasileiros em 2021. Disponível em: http://athenasecurity.com.br/phishing-atinge-150-milhoes-de-brasileiros-em-2021. Acesso em: 5 out. 2024.

RIOTIMESONLINE. *Brasil é classificado como o segundo país mais vulnerável a ataques cibernéticos em 2023 devido a seis ameaças*. Disponível em: https://www.riotimesonline.com/brazil-ranked-second-most-vulnerable-to-cyberattacks-in-2023-due-to-6-threats/. Acesso em: 28 abr. 2025.

RODRIGUES, Ana Beatriz. Polícia Federal, STF e Anatel sofrem ataques cibernéticos. SpaceMoney. Disponível em: https://www.spacemoney.com.br/noticias/policia-federal-stf-e-anatel-sofrem-ataques-ciberneticos/. Acesso em: 5 set. 2024.

WU, Zhizheng; LI, Haizhou. Spoofing and countermeasures for speaker verification: A survey. Speech Communication, v. 66, p. 130-153, 2015. DOI: 10.1016/j.specom.2014.10.005