ESCOLA DE GUERRA NAVAL

CAPITÃO DE CORVETA (FN) RAFAEL FELIPPE OLIVEIRA DA SILVA

ANÁLISE DA ADERÊNCIA DO PADRÃO INTERNACIONAL DE DEFESA CIBERNÉTICA NIST CSF 2.0 AO PROCESSO DE PLANEJAMENTO CONJUNTO BRASILEIRO.

Rio de Janeiro

2025

CAPITÃO DE CORVETA (FN) RAFAEL FELIPPE OLIVEIRA DA SILVA

ANÁLISE DA ADERÊNCIA DO PADRÃO INTERNACIONAL DE DEFESA CIBERNÉTICA NIST CSF 2.0 AO PROCESSO DE PLANEJAMENTO CONJUNTO BRASILEIRO.

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CMG (RM-1) CANTARINO

Rio de Janeiro

Escola de Guerra Naval

2025

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar.

Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Documento assinado digitalmente
gov.br
RAFAEL FELIPPE OLIVEIRA DA SILVA
Data: 29/11/2025 13:37:18-0300
Verifique em https://validar.iti.gov.br

RESUMO

Esta dissertação investiga a integração entre o NIST CSF 2.0 e o Processo de Planejamento Conjunto (PPC) brasileiro no nível operacional, com ênfase na defesa cibernética. O estudo parte da relevância crescente da cibersegurança nas operações militares conjuntas, verificando a possibilidade de harmonizar referenciais internacionais com a doutrina nacional. O objetivo central é avaliar a aplicabilidade do NIST CSF 2.0 no contexto do PPC, considerando potenciais pontos de convergência e adequação conceitual. Os resultados indicam que a aplicação do framework, quando adaptada às especificidades da doutrina militar brasileira, apresenta potencial para fortalecer a resiliência cibernética como função operacional integrada ao planejamento conjunto, abrindo perspectivas para investigações futuras sobre metodologias que ampliem essa integração.

Palavras-chave: Guerra Cibernética. Cibersegurança. NIST CSF 2.0. Processo de Planejamento Conjunto (PPC). Nível Operacional, Defesa Cibernética. Doutrina Militar Brasileira. Operações Conjuntas. Gestão de Riscos Cibernéticos. Planejamento Militar.

ABSTRACT

Analysis of the Adherence of the International Cyber Defense Standard NIST CSF 2.0 to the Brazilian Joint Planning Process.

This dissertation investigates the integration between the NIST Cybersecurity Framework (CSF) 2.0 and the Brazilian Joint Planning Process (JPP) at the Operational Level, with an emphasis on cyber defense. The study stems from the growing relevance of cybersecurity in joint military operations, examining the possibility of harmonizing international frameworks with national doctrine. The central objective is to assess the applicability of the NIST CSF 2.0 within the context of the JPP, considering potential points of convergence and conceptual alignment. The findings indicate that applying the framework, when adapted to the specificities of Brazilian military doctrine, has the potential to strengthen cyber resilience as an operational function integrated into joint planning, opening avenues for future research on methodologies that enhance this integration.

Keywords: Cyber Warfare. Cybersecurity. NIST CSF 2.0. Joint Planning Process (PPC). Operational Level. Cyber Defense. Brazilian Military Doctrine. Joint Operations. Cyber Risk Management. Military Planning.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTO E MOTIVAÇÃO DA PESQUISA

A crescente interdependência entre sistemas militares e o ciberespaço tornou este domínio um elemento central para o êxito das operações no nível operacional. Campanhas de espionagem, sabotagem digital e ataques a infraestruturas críticas já demonstraram capacidade de degradar o comando e controle, comprometer cadeias logísticas e neutralizar capacidades de combate antes mesmo do emprego cinético. No ambiente conjunto, a superioridade terrestre, marítima, aérea e espacial passa a depender diretamente da resiliência e da integridade das redes e sistemas de informação que sustentam a manobra operacional.

Assim, a cibersegurança deixa de ser um apoio técnico para se tornar função operacional essencial, cujo estudo e integração ao planejamento são decisivos para garantir liberdade de ação, negar oportunidades ao adversário e assegurar o cumprimento dos objetivos de campanha.

Diante desse cenário, esta pesquisa surge da necessidade de compreender como ferramentas de cibersegurança originalmente concebidas para o setor civil podem ser adaptadas e aplicadas ao planejamento militar. A lacuna entre os modelos teóricos da cibersegurança e sua operacionalização no contexto das Forças Armadas, especialmente no nível operacional, justifica a análise da adequabilidade de Estruturas Conceituais[1] como o NIST CSF 2.0[2] à doutrina de planejamento militar brasileira.

1.2 RELEVÂNCIA DA PESQUISA

Esta pesquisa contribui para o aprimoramento da doutrina militar brasileira em cibersegurança ao analisar a adequabilidade do NIST CSF 2.0 ao Processo de Planejamento Conjunto (PPC). Ao fazê-lo, oferece subsídios práticos e teóricos que podem fundamentar decisões operacionais e políticas públicas mais eficazes no

[1] Framework. (tradução Nossa).
[2] O National Institute of Standards And Technology Cibersecurity Framework, Versão 2.0 (NIST, 2024), será denominado nesta pesquisa, por sua abreviação internacionalmente reconhecida.

âmbito da defesa cibernética. A integração estruturada da cibersegurança no planejamento operacional revela-se essencial para a resiliência das operações militares em um ambiente cada vez mais complexo, interconectado e contestado.

Adicionalmente, o estudo avança a literatura acadêmica ao explorar a interseção entre Estruturas Conceituais civis de cibersegurança e os processos decisórios militares. A análise autoral conduzida neste trabalho identifica convergências naturais, adaptações parciais e incompatibilidades conceituais entre o NIST CSF 2.0 e o PPC, oferecendo uma leitura original e crítica dessa relação. Compreender essas dinâmicas é vital para que as Forças Armadas fortaleçam sua capacidade de mitigar riscos, explorar oportunidades no domínio cibernético, garantir a superioridade informacional e proteger seus ativos críticos.

1.3 OBJETIVO DA PESQUISA

O objetivo principal desta pesquisa é verificar a adequabilidade do uso das ferramentas do NIST CSF 2.0, no contexto do Processo de Planejamento Conjunto PPC das Forças Armadas brasileiras, com foco no nível operacional. Para isso, os elementos estruturantes do NIST CSF 2.0 serão analisados em relação a cada etapa do PPC, com o propósito de identificar convergências naturais, divergências conceituais e potenciais de adaptação que permitam sua aplicação prática no planejamento militar.

1.4 DESCRIÇÃO DA METODOLOGIA

A metodologia adotada consistiu em uma análise detalhada de cada elemento do NIST CSF 2.0 em relação a cada etapa do Processo de Planejamento Conjunto (PPC). Essa análise buscou identificar três tipos de relações: as aderências naturais, que são elementos do NIST CSF 2.0 que se alinham diretamente e sem necessidade de adaptação às práticas e conceitos do PPC; as aderências parciais, que correspondem a elementos que apresentam alguma similaridade, mas que demandam ajustes ou interpretações específicas para serem aplicados no contexto militar; e as incompatibilidades, que são elementos do NIST CSF 2.0 que não possuem equivalência ou que são fundamentalmente inconsistentes com a doutrina e a natureza do planejamento militar.

Este estudo subdivide-se em cinco capítulos principais, organizados de forma a conduzir a análise de maneira progressiva. O segundo capítulo apresenta o referencial teórico, abordando a doutrina de planejamento militar no contexto cibernético e estabelecendo as bases conceituais para a integração entre esses domínios. Já o terceiro capítulo descreve detalhadamente o NIST CSF 2.0, sua estrutura, funções e aplicabilidade. No quarto capítulo, passa-se à confrontação entre o NIST CSF 2.0 e o Processo de Planejamento Conjunto, identificando convergências, adaptações necessárias e incompatibilidades. Por fim, o quinto capítulo apresenta as conclusões extraídas da pesquisa, bem como oportunidades de investigações mais aprofundadas em temas correlatos, especialmente no que se refere ao aperfeiçoamento da integração entre estruturas conceituais de cibersegurança e a doutrina de planejamento militar no nível operacional.

2 DOUTRINA DE PLANEJAMENTO MILITAR NO CONTEXTO CIBERNÉTICO

2.1 INTRODUÇÃO

O presente capítulo constitui o referencial teórico da dissertação, estabelecendo as bases para compreender como a doutrina de defesa cibernética se integra ao planejamento militar conjunto no Nível Operacional[3]. A estrutura com progressão pedagógica, visa conduzir o leitor do planejamento tradicional à integração cibernética, focando neste Nível, elo entre a estratégia e a tática, como ponto ideal para essa inserção.

Inicialmente, apresenta-se a fundamentação histórica e legal da doutrina de planejamento conjunto, demonstrando como a integração interforças preparou o caminho para a inclusão de novos domínios operacionais. Em seguida, analisa-se a hierarquia dos níveis decisórios, delineando o contexto organizacional necessário para o emprego cibernético.

A seção central aborda o Processo de Planejamento Conjunto (PPC)[4], destacando sua estrutura, finalidade e princípios, para então introduzir a integração cibernética de forma natural. O destaque recai sobre o sistema de anexos do Plano Operacional, especialmente o Anexo H, que institucionaliza o domínio cibernético, conferindo-lhe status equivalente às demais áreas funcionais.

A introdução da Doutrina Militar de Defesa Cibernética ocorre de forma alinhada aos fundamentos já apresentados, verificando convergência metodológica e normativa com o PPC. A análise final sintetiza essa convergência, demonstrando que a defesa cibernética não é apenas complementar, mas componente indispensável à eficácia das Operações Conjuntas.

A abordagem adotada busca facilitar a assimilação dos novos conceitos, demonstrando que a integração cibernética é evolução coerente da doutrina militar.

---

[3] "A Concepção de Emprego Conjunto das Forças Armadas, em seu ciclo completo, perpassa os níveis político, estratégico, operacional e tático." (BRASIL, 2020a, p.22).

[4] "No Nível Operacional, o produto final do PPC será um Plano Operacional, em que o CmtOp estabelecerá prioridades, organizará os meios que lhe foram adjudicados, atribuirá tarefas aos comandos subordinados e estabelecerá diretrizes para o planejamento e a execução de operações militares (nos domínios aéreo, terrestre, marítimo e espacial; no espectro eletromagnético; e no ambiente informacional, que inclui o ciberespaço), coordenadas no tempo e no espaço, de tal forma que permitam alcançar o Estado Final Desejado Operacional. Esse Plano orientará o planejamento dos escalões subordinados." (BRASIL, 2020b, p.35).

2.1.1 Justificativa do Foco Operacional e Importância Cibernética

O Nível Operacional representa o espaço onde os conceitos estratégicos são interpretados materializam-se em objetivos operacionais concretos. É neste Nível que o domínio cibernético deve ser integrado ao planejamento militar conjunto. A doutrina brasileira estabelece que este é o Nível no qual se realizam o planejamento e a condução das operações militares de caráter conjunto (BRASIL, 2020b), sendo também onde as ações de defesa cibernética devem estar em consonância com os planejamentos e os objetivos definidos para a campanha ou operação (BRASIL, 2023).

O reconhecimento do domínio cibernético como parte integrante do planejamento operacional representa avanço normativo consolidado na nossa doutrina. Esta valorização se manifesta formalmente na Doutrina de Operações Conjuntas, que dedica a plenitude de seu capítulo XII ao tema Guerra Cibernética[5] nas Operações Conjuntas, e através da necessidade de ativar a Subseção de Guerra Cibernética (SGC) em sua estrutura e organização, a fim de coordenar o emprego da capacidade cibernética nas operações (BRASIL, 2020a).

Este foco se justifica porque é aquele no qual o planejamento militar se transforma em operações concretas, e a cibernética deixa de ser abstrata para se tornar ferramenta tangível de apoio e proteção ao Comando e Controle.

2.1.2 Objetivo do Capítulo e Delimitação das Fontes Doutrinárias

Este capítulo tem o objetivo de relacionar sistematicamente a doutrina de defesa cibernética com o Processo de Planejamento Militar Conjunto no Nível Operacional, ao mapear em sua estrutura geral as pontes conceituais e procedimentais entre domínios tradicionalmente distintos. O escopo de análise delimita-se às duas principais fontes doutrinárias que regem essa integração no contexto das Forças Armadas brasileiras.

---

[5] Guerra Cibernética: Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de Nível Operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC.(BRASIL, 2014 p.19).

A primeira fonte é a Doutrina de Operações Conjuntas, aprovada pela Portaria Normativa nº 84/GM-MD de 2020, fornecendo o arcabouço metodológico fundamental para compreender como o planejamento conjunto se estrutura e opera. Complementarmente, a Doutrina Militar de Defesa Cibernética (BRASIL, 2023) estabelece os conceitos, princípios e procedimentos para o planejamento, coordenação e execução das ações de defesa cibernética no âmbito das Forças Armadas.

A delimitação consciente a essas duas fontes garante foco analítico, profundidade investigativa e restringe a análise ao cerne doutrina sobre o qual verificar-se-á aderências, evitando dispersão conceitual que comprometeria a clareza argumentativa. Essas fontes representam o estágio atual do processo evolutivo da doutrina militar brasileira.

2.2 A DOUTRINA DE PLANEJAMENTO MILITAR CONJUNTO

2.2.1 Aspectos Gerais da Doutrina de Planejamento Conjunto

A doutrina de planejamento militar conjunto brasileira resulta de processo evolutivo contínuo, fundamentado em experiências históricas e marcos legais que consolidamos avanços conceituais. A doutrina atual reconhece que o estudo das últimas guerras e conflitos mostra, de forma insofismável, que, apesar de bem-sucedidas ações isoladas de FA, as grandes vitórias foram alcançadas por meio de ações adequadamente integradas de forças navais, terrestres e aéreas (BRASIL, 2020a).

A estrutura do planejamento nas Operações Conjuntas reflete organização hierárquica e funcional que garante coordenação efetiva entre diferentes níveis de comando. A doutrina estabelece que o planejamento das Operações Conjuntas pode ser realizado nos níveis estratégico, operacional e tático, sendo conduzido pelo Estado-Maior Conjunto (EMCj) correspondente [6] (BRASIL, 2020b). Entretanto, a Doutrina ressalta que o Nível Operacional é a integração entre o Tático e o Estratégico:

[6] Estado-Maior Conjunto (EMCj): Órgão de assessoramento do Comandante Operacional responsável pelo planejamento, coordenação e controle das Operações Conjuntas. O EMCj, quando ativado, é composto por representantes das três Forças Armadas (Marinha, Exército e Aeronáutica) e organiza-se em seções funcionais especializadas, sendo responsável pela condução e coordenação do Processo de Planejamento Conjunto. (BRASIL, 2020a).

> Nesse Nível, os principais conceitos estratégicos, objetivos e estado final desejado servem de base para o estabelecimento dos objetivos operacionais e das missões a serem atribuídas às Forças Componentes, observando a coerência com o Nível Estratégico. (BRASIL, 2020a, p. 23)

A evolução normativa reflete aprendizado institucional baseado em lições históricas sobre a necessidade de integração das forças, demonstrando um comportamento adaptativo. A distribuição hierárquica de responsabilidades garante que decisões sejam tomadas no Nível apropriado, estabelecendo precedente importante para a integração de novas dimensões operacionais, como o domínio cibernético.

2.3 O PROCESSO DE PLANEJAMENTO CONJUNTO (PPC)

2.3.1 Estrutura Geral do PPC

O Processo de Planejamento Conjunto é a ferramenta metodológica fundamental para a elaboração do planejamento operacional das Forças Armadas brasileiras em Operações Conjuntas[7], constituindo instrumento que organiza o raciocínio militar e garante análise sistemática das alternativas disponíveis. A responsabilidade pela condução é claramente estabelecida: O Comandante Operacional deve coordenar o Processo de Planejamento Conjunto (PPC), sendo o responsável pela consolidação e formalização dos documentos decorrentes deste planejamento juntos com suas sessões do EMCj [8] (BRASIL, 2020b).

A definição metodológica é precisa: o Processo de Planejamento Conjunto (PPC) é um método sistemático para analisar uma missão, desenvolver ações e controlar a execução do plano elaborado propondo linhas de ação alternativas caso necessário (BRASIL, 2020b).

---

[7] Operações Conjuntas: As operações militares de grande envergadura exigem o emprego de elementos pertencentes a mais de uma Força Armada. Para tal, as Forças Singulares devem somar esforços, compatibilizar procedimentos e integrar as ações, de forma a se obter maior efetividade na execução das Operações Conjuntas (Op Cj). (BRASIL, 2020a).

[8] As seções de Estado-Maior Conjunto: Divisões funcionais especializadas que compõem o EMCj, cada uma responsável por áreas específicas do planejamento e condução das Operações Conjuntas. A estrutura completa das seções inclui: D-1 (Pessoal), D-2 (Inteligência), D-3 (Operações), D-4 (Logística e Mobilização), D-5 (Planejamento), D-6 (Comando e Controle), D-7 (Comunicação Social), D-8 (Operações de Informação), D-9 (Assuntos Civis), e D-10 (Administração Financeira). A estruturação das seções é uma atribuição do Comandante Operacional, que deve constituí-las segundo a necessidade da operação que irá desenvolver, garantindo abordagem integrada e especializada para todos os aspectos operacionais do planejamento conjunto. (BRASIL, 2020b).

Essa sistematização proporciona um rigor analítico e garante que todas as alternativas sejam adequadamente consideradas, evitando decisões precipitadas ou baseadas em análises incompletas. A flexibilidade adaptativa permite que o processo seja ajustado às circunstâncias específicas sem perder sua essência metodológica.

Este método transcende a simples organização de procedimentos. Sua finalidade é claramente estabelecida: proporcionar ao Comandante e ao Estado-Maior um método para organizar o pensamento e desenvolver um “planejamento para o emprego do poder militar, facilitando a tomada de uma decisão.” (BRASIL, 2020b p.35). “O produto final do PPC será um Plano Operacional” (BRASIL, 2020b p.35).

2.3.2 Etapas do Processo Operacional

A organização do PPC em etapas sequenciais garante rastreabilidade completa do processo decisório. A estrutura é claramente definida: as etapas do processo de planejamento são: Etapa 1- Exame de Situação Operacional; Etapa 2- Elaboração de Planos e Ordens; e Etapa 3- Controle da Operação Planejada (BRASIL, 2020b). A natureza cíclica contínua e flexível do processo, possibilita retornar às partes anteriores para rever certos aspectos, obter e analisar novos dados cuja importância não tenha sido evidenciada anteriormente e constantemente avaliar a necessidade de mudanças e adaptações diante de novos eventos observados (BRASIL, 2020b).

A estruturação nestas etapas sequenciais garante sistematização permitindo verificação e validação em cada fase. A flexibilidade na execução permite adaptação a diferentes contextos operacionais sem comprometer a metodologia fundamental, proporcionando estrutura lógica que possibilita incorporar considerações cibernéticas em cada uma destas fases.

2.3.3 Anexos ao Plano

No Plano Operacional, os anexos são documentos que organizam e detalham as ações por área funcional, como Inteligência, Logística e Comando e Controle. Já os apêndices são desdobramentos desses anexos, oferecendo instruções técnicas, formulários, listas ou roteiros específicos. Ambos são essenciais para garantir a interoperabilidade, a clareza e a padronização das ações planejadas. Os anexos asseguram a divisão funcional das responsabilidades, enquanto os apêndices

aprofundam aspectos operacionais, facilitando a execução coordenada das Operações Conjuntas no Nível Operacional[9]. (BRASIL, 2020b).

A integração do domínio cibernético ao planejamento operacional conjunto ocorre pela convergência doutrinária entre dois documentos fundamentais: A Doutrina de Operações Conjuntas estabelece o arcabouço estrutural para essa integração ao formalizar o Anexo de Defesa Cibernética, componente do Plano Operacional (BRASIL, 2020b) complementada pela Doutrina Militar de Defesa Cibernética, que define os procedimentos específicos para operacionalizar essa integração (BRASIL, 2023).

Enquanto a primeira cria o instrumento formal (Anexo H) dentro da estrutura geral do planejamento conjunto, a segunda preenche esse instrumento com conteúdo específico da defesa cibernética. Esta complementaridade garante que a integração cibernética não seja meramente conceitual, mas possua tanto o veículo institucional adequado quanto os procedimentos técnicos necessários para sua implementação prática. O resultado é sistema doutrinário integrado onde a dimensão cibernética se insere organicamente no planejamento operacional.

2.3.4 Integração do Domínio Cibernético no Processo Operacional

A 2ª edição da Doutrina de Operações Conjuntas atualiza e expande a doutrina anterior ao incorporar formalmente os domínios cibernético[10] e informacional no Processo de Planejamento Conjunto (PPC), refletindo os avanços trazidos pela Doutrina Militar de Defesa Cibernética (BRASIL, 2023).

---

[9] Anexos ao Plano Operacional: Documentos complementares que detalham aspectos específicos da operação, proporcionando orientações especializadas para cada área funcional sem sobrecarregar o plano principal. Os anexos padronizados incluem: Anexo A (Inteligência), Anexo B (Comando e Controle), Anexo C (Logística e Mobilização), Anexo D (Comunicação Social), Anexo E (Assuntos Civis), Anexo F (Operações de Informação), Anexo G (Operações Especiais), Anexo H (Defesa Cibernética), Anexo I (Defesa Biológica, Nuclear, Química e Radiológica), Anexo J (Desenho Operacional), Anexo K (Interdição), Anexo L (Medidas e Indicadores de Eficácia), Anexo M (Regras de Engajamento), Anexo N (Matriz de Sincronização), Anexo O (Gerenciamento do Risco Operacional), Anexo P (Administração Financeira), e Anexo Q (Áreas de Responsabilidade). Cada anexo pode ser subdividido em apêndices para maior detalhamento técnico, mantendo a clareza operacional do plano principal. (BRASIL, 2020b)

[10] "O Espaço Cibernético é um dos cinco domínios operacionais e permeia todos os demais. São eles: o terrestre, o marítimo, o aéreo e o espacial, que são interdependentes. As atividades no Espaço Cibernético podem criar liberdade de ação para atividades em outros domínios, assim como atividades em outros domínios também criam efeitos dentro e através do Espaço Cibernético. O objetivo central da integração dos domínios é a habilidade de se alavancar capacidades de vários domínios para que sejam criados efeitos únicos e, frequentemente, decisivos." (BRASIL, 2014 p.18)

Enquanto a versão anterior focava nos ambientes tradicionais (BRASIL, 2011), a nova edição alinha-se às exigências da guerra moderna, integrando a Defesa Cibernética como função operacional por meio do Anexo H (BRASIL, 2020b). Assim, enquanto a doutrina de planejamento estabelece a estrutura processual, a doutrina cibernética fornece as diretrizes técnicas específicas para o emprego, assegurando coerência e interoperabilidade nas Operações Conjuntas.

A integração do domínio cibernético representa evolução natural e necessária da doutrina militar para incorporar as realidades do ambiente operacional contemporâneo. A necessidade é estabelecida: o processo operacional requer consideração das vulnerabilidades e oportunidades cibernéticas em todas as fases do planejamento (BRASIL, 2023). A avaliação cibernética do ambiente operacional deve identificar ativos críticos, ameaças e vulnerabilidades que possam afetar o cumprimento da missão (BRASIL, 2023).

A integração cibernética exige avaliação sistemática e abrangente do ambiente operacional, identificando fatores que possam influenciar decisivamente o cumprimento da missão. A proteção dos sistemas críticos é fundamental para manter a eficácia operacional, especialmente considerando a dependência crescente dos sistemas de Comando e Controle de tecnologias da informação.
Com a finalidade de ressaltar essa preocupação, a Doutrina Cibernética destaca:

> Para o planejamento, no nível operacional em situação de guerra e não-guerra, a SGC, que faz parte da estrutura da Seção de Operações (D-3), deverá produzir o Anexo de Guerra Cibernética ao Plano Operacional. (BRASIL, 2023, p.38).

Para sanar lacunas geradas pela crescente importância do domínio cibernético, fez-se necessária a criação de uma doutrina específica, capaz de orientar tecnicamente o emprego, assegurar coerência entre planos e integrar eficazmente o ambiente cibernético às Operações Conjuntas.

2.4 A DOUTRINA MILITAR DE DEFESA CIBERNÉTICA

A Defesa Cibernética, componente da Defesa Nacional, é missão das Forças Armadas (BRASIL, 2023), mas exige o engajamento da sociedade para proteger infraestruturas críticas no espaço cibernético. Sua eficácia depende da colaboração

entre Ministério da Defesa, comunidade acadêmica, setores público e privado e indústria de defesa, com interação nacional e internacional. Suas atividades visam atender à Defesa Nacional, integrando órgãos desde tempos de paz para facilitar respostas a crises.

Dentro desse contexto, consolidou-se uma Doutrina Militar de Defesa Cibernética no Brasil, que estabelece fundamentos, diretrizes e responsabilidades para o emprego coordenado dos meios cibernéticos, sob o controle central do Ministério da Defesa, que exerce a coordenação superior do Sistema Militar de Defesa Cibernética (SMDC)[11]. Essa doutrina liga-se às Forças Armadas por força da Lei Complementar Nº 97/99, que define as competências do Ministério da Defesa e estabelece as bases para o emprego conjunto dos meios militares, inclusive no espaço cibernético.

2.4.1 Finalidade da Doutrina

A Doutrina Militar de Defesa Cibernética visa estabelecer as diretrizes para que os componentes do Sistema Militar de Defesa Cibernética (SMDC) que participam do PPC possam desenvolver uma Estrutura Conceitual[12] abrangente para orientar as ações das Forças Armadas no domínio cibernético, representando marco na evolução doutrinária brasileira. A finalidade é claramente estabelecida:

> Estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético. (BRASIL, 2023 p.11).

Seu escopo abrange o conjunto de ações ofensivas, defensivas e exploratórias realizadas no Espaço Cibernético, no contexto de um planejamento nacional de Nível estratégico, coordenado e integrado pelo Ministério da Defesa, com vistas a proteger

[11] O Sistema Militar de Defesa Cibernética (SMDC): é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. (BRASIL, 2014 p.25).

[12] Estrutura Conceitual (Framework): Ferramenta que oferece uma estrutura pré-montada para o desenvolvimento de projetos, permitindo que o desenvolvedor se concentre nas funcionalidades específicas sem se preocupar com detalhes repetitivos ou configurações básicas. Ele automatiza tarefas comuns e fornece componentes prontos, mas mantém a flexibilidade para personalização conforme as necessidades do projeto. (ALURA, 2022).

sistemas de informação de interesse da Defesa Nacional, obter dados para Inteligência e comprometer sistemas do oponente, sempre em conformidade com o ordenamento jurídico nacional e internacional (BRASIL, 2023).

O Sistema Militar de Defesa Cibernética (SMDC) reúne recursos, doutrina e pessoal para garantir o uso seguro do ciberespaço pelas FA e proteger o SISMC2[13] e infraestruturas críticas[14] definidas pelo MD.

2.4.2 Níveis de Decisão na Defesa Cibernética

No SMDC, os níveis de decisão distribuem responsabilidades de forma escalonada: o Nível Político, envolvendo a Presidência da República e o Comitê Gestor da Internet no Brasil, cuida da Segurança da Informação e Comunicações (SIC) e da Segurança Cibernética; o Nível Estratégico, sob o EMCFA, os comandos das Forças Singulares e órgãos parceiros, coordena a Defesa Cibernética; já os Níveis Operacional e Tático concentram as ações de Guerra Cibernética, sendo esta denominação restrita ao âmbito interno das Forças Armadas (BRASIL 2023), realizadas por comandos operacionais, seus estados-maiores e forças componentes.

A hierarquia decisória espelha fielmente a estrutura geral de comando militar, garantindo alinhamento perfeito entre políticas estratégicas e planejamento operacional. Os níveis de decisão na defesa cibernética constituem sistema integrado hierarquicamente organizado que garante coerência sistêmica, facilitando significativamente a integração com os processos decisórios tradicionais das Operações Conjuntas.

2.4.3 Convergência com a Doutrina de Planejamento

As doutrinas de Operações Conjuntas e de Defesa Cibernética aderem-se de forma complementar no âmbito do Nível Operacional. Enquanto a primeira estabelece o arcabouço do PPC, oferecendo um método estruturado para analisar a missão, consolidar o Plano Operacional, e propor uma sequência lógica para o controle da operação em curso, com anexos que detalham funções específicas, a segunda

---

[13] Sistema Militar De Comando E Controle (SISMC2): Conjunto de instalações, equipamentos, comunicações, doutrina, procedimentos e pessoal essenciais para o comandamento, em Nível nacional, das crises e dos conflitos. (BRASIL, 2015).

[14] Infraestruturas Críticas: Instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério MD35-G-01 impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade. (BRASIL, 2015).

preenche esse arcabouço com um conteúdo técnico especializado em Defesa Cibernética, definindo fundamentos, responsabilidades no espaço cibernético. Por meio do Anexo H, abre-se um lugar comum entre o pensamento militar clássico e o pensamento tecnológico em unidade de pensamento em prol da Defesa.

Essa aderência é reforçada pela necessidade de considerar vulnerabilidades e oportunidades cibernéticas em todas as fases do PPC, integrando a análise de guerra cibernética aos produtos do planejamento conjunto. O resultado é um sistema doutrinário coerente, em que o planejamento militar tradicional incorpora, sem perder seu rigor metodológico, as peculiaridades do ambiente cibernético, visando atender à exigência de resposta adaptada às exigências da guerra moderna.

> O Brasil, na esteira dos acontecimentos relevantes ocorridos no espaço cibernético nos últimos anos, também reconhece esse ambiente como um domínio operacional, no qual ações cibernéticas ofensivas e defensivas tendem a potencializar ou complementar as ações realizadas nos demais domínios (terra, mar, ar e espaço). (BRASIL, 2023 p.14).

2.5 CONCLUSÃO DO CAPÍTULO

O exame realizado evidencia que o planejamento militar conjunto brasileiro se estrutura a partir de um método rigoroso, com etapas e fases bem delimitadas, mas que se caracteriza por um comportamento cíclico, contínuo e flexível. Essa natureza permite revisitar etapas, analisar novos dados e adaptar decisões à evolução do ambiente operacional.

Esse traço fundamental do PPC dialoga diretamente com a Doutrina Militar de Defesa Cibernética, que não se apresenta como um manual de procedimentos estanques, mas sim como um corpo doutrinário pautado em princípios e fundamentos, conferindo ao planejador ampla liberdade para moldar suas ações às exigências específicas de cada situação.

A doutrina de planejamento, ao longo de seu processo histórico, absorveu as lições e necessidades impostas pelo surgimento do domínio cibernético, passando a contemplar explicitamente este novo ambiente por meio de alterações em sua estrutura, seja pela criação de capítulos dedicados à guerra cibernética, seja pela formalização do Anexo H. Este anexo, por sua vez, institui um espaço funcional dentro

do PPC para que as questões cibernéticas sejam tratadas com a mesma relevância e sistematização das demais áreas operacionais.

Portanto, é justamente dessa convergência, fruto do amadurecimento doutrinário e da criação desse ponto de encontro normativo, que emerge o ambiente ideal para analisar, se é possível propor uma Estrutura Conceitual que respeite o caráter adaptativo do PPC e, ao mesmo tempo, incorpore com aderência os princípios estabelecidos pela doutrina cibernética brasileira.

3 O NIST CSF 2.0 COMO FERRAMENTA PARA O PLANEJAMENTO DA DEFESA CIBERNÉTICA

Este capítulo tem como objetivo descrever a Estrutura Conceitual de Cibersegurança do Instituto Nacional de Padrões e Tecnologia (NIST CSF 2.0), apresentando sua evolução histórica, estrutura lógica e características funcionais. A finalidade é proporcionar uma compreensão abrangente sobre este instrumento de gestão de riscos cibernéticos através da exposição sistemática de seus componentes e metodologia.

A descrição inicia-se com o exame dos antecedentes que motivaram o desenvolvimento da Estrutura Conceitual, apresentando como a crescente dependência digital se relaciona com as ameaças cibernéticas levaram à necessidade de padronização em segurança digital pelo Governo dos Estados Unidos da América, que recorre à expertise técnica acumulada pela NIST ao longo de décadas em desenvolvimento de padrões. Desta necessidade nasce uma solução estruturada para desafios contemporâneos de cibersegurança.

O capítulo detalha a arquitetura tripartida NIST do CSF 2.0 (Processo, Nível de Maturidade e Perfil [15]), destacando o Processo, cujas seis funções principais e respectivos componentes complementares formam um ciclo integrado de gestão de riscos (NIST, 2024).

Por fim, desenvolve-se como esta estrutura modular se organiza para permitir que organizações implementem proteções cibernéticas conforme suas necessidades específicas, recursos disponíveis e perfis de risco, incluindo contextos militares.

3.1 APRESENTAÇÃO DO OBJETO DE ESTUDO

3.1.1 Antecedentes

A crescente sofisticação das ameaças cibernéticas evidenciou a necessidade de protocolos estruturados para o setor de defesa, uma vez que tais instrumentos fornecem diretrizes organizadas e práticas consolidadas para gerenciar e mitigar riscos de segurança digital. O setor militar demanda proteção de sistemas e ativos físicos ou virtuais vitais para os Estados Unidos, cuja incapacidade ou destruição teria

[15] CORE, TIERS e PROFILE (Tradução Nossa).

impacto debilitante na segurança nacional, exigindo ações para prevenir, remediar ou mitigar riscos resultantes de vulnerabilidades (ESTADOS UNIDOS, 2024a).

Neste cenário, o Instituto Nacional de Padrões e Tecnologia (NIST), vinculado ao Departamento de Comércio dos Estados Unidos, desenvolveu uma Estrutura Conceitual que auxilia organizações de todos os portes a compreender, administrar e reduzir seus riscos cibernéticos, oferecendo um roteiro de melhores práticas para orientar investimentos em proteção digital (ESTADOS UNIDOS, 2024b).

O instituto, fundado em 1901, é um dos mais antigos laboratórios de ciências físicas norte americano, e consolidou ao longo de décadas sua expertise em segurança da informação e desenvolvimento de padrões técnicos (NIST, 2024), estabelecendo competências centrais em ciência de medição, rastreabilidade rigorosa e metodologias científicas aplicadas à proteção digital.

A urgência de estabelecer políticas federais estruturadas de cibersegurança foi amplamente documentada por especialistas como Clarke e Knake (2010), que alertaram sobre a desproporcional dependência americana do ciberespaço e a consequente vulnerabilidade a ataques de proporções similares a Pearl Harbor[16]. Os autores argumentaram que os Estados Unidos necessitavam criar uma estratégia cibernética focada em capacidades defensivas para infraestruturas críticas, uma vez que a supremacia ofensiva não compensaria as fraquezas defensivas no ciberdomínio.

Esta análise fundamentou a percepção governamental de que a ausência de uma estratégia defensiva poderia causar uma escalada de conflitos cibernéticos para guerras convencionais, estabelecendo as bases conceituais para futuras iniciativas federais de padronização em cibersegurança. Neste contexto, surge a necessidade de estabelecer uma política estruturada de cibersegurança, reconhecendo que Estrutura Conceituais de cibersegurança são vitais para o setor de defesa, fornecendo diretrizes estruturadas e melhores práticas para gerenciar e mitigar riscos cibernéticos (COGENT INFOTECH, 2024).

[16]Richard A. Clarke e Robert K. Knake, em sua obra “Cyber War: The Next Threat to National Security and What to Do About It” (2010), alertam para a desproporcional dependência dos Estados Unidos em relação ao ciberespaço, o que os tornaria vulneráveis a ataques cibernéticos de magnitude catastrófica. Os autores empregam a analogia de Pearl Harbor para ilustrar o potencial impacto devastador de um ataque cibernético bem-sucedido contra a infraestrutura crítica americana, argumentando que a supremacia ofensiva no ciberdomínio não seria suficiente para compensar as fraquezas defensivas. Eles enfatizam a urgência de se estabelecerem políticas federais estruturadas de cibersegurança, com foco primordial em capacidades defensivas para proteger ativos vitais.

Coube ao NIST consolidar sua autoridade técnica no domínio da cibersegurança governamental através da adoção de seus protocolos pelas agências federais americanas e da exigência como requisito contratual para fornecedores do Departamento de Defesa.

O Departamento de Defesa incorpora o NIST CSF 2.0 em sua Arquitetura de Referência de Cibersegurança (ESTADOS UNIDOS, 2023), enquanto a Força Aérea americana utiliza a Estrutura Conceitual como base de seu programa de cibersegurança (ESTADOS UNIDOS, 2020). A Marinha desenvolveu o programa MilGears[17] para apoiar a força de trabalho de cibersegurança mapeando capacidades cibernéticas conforme diretrizes NIST (NIST, 2021).

Internacionalmente, forças armadas de países aliados demonstram crescente adoção dos princípios da Estrutura Conceitual NIST. O Ministério da Defesa do Reino Unido implementou o NIST CSF 2.0 para fortalecer suas defesas cibernéticas (TRUSTWAVE, 2024), enquanto a Real Força Aérea Canadense integrou a Estrutura Conceitual de gestão de riscos cibernéticos NIST em sistemas militares não tripulados (SZUMLANSKI, 2024). Na Austrália, o governo adotou padrões NIST como referência para melhores práticas de cibersegurança (ANITECH GROUP, 2023), demonstrando a aplicabilidade global da Estrutura Conceitual em contextos de defesa.

3.1.2 Visão Geral do NIST CSF 2.0

Originado por demanda do governo americano em 2013, a Estrutura Conceitual tem passado por atualizações periódicas estratégicas para manter sua relevância e aplicabilidade contemporânea. As revisões sucessivas, versão 1.0 (2014), 1.1 (2018) e 2.0 (2024), preservam deliberadamente sua natureza adaptativa e linguagem acessível, garantindo compreensão por profissionais de diferentes níveis técnicos (NIST, 2024).

[17] O programa MilGears é uma suíte de ferramentas desenvolvida pelo Departamento de Defesa dos Estados Unidos (DoD) com o objetivo de auxiliar militares, veteranos e potenciais recrutas no planejamento e desenvolvimento de suas carreiras. Ele funciona analisando o histórico individual de educação militar e civil, treinamentos e experiência de trabalho, gerando um relatório conciso que inclui credenciais civis e oportunidades de carreira. A plataforma visa facilitar a transição de militares para a vida civil e o aprimoramento contínuo de suas habilidades durante o serviço, ajudando-os a visualizar e alcançar seus objetivos profissionais.

Uma Estrutura Conceitual de segurança cibernética constitui um conjunto estruturado de diretrizes, padrões e práticas recomendadas que orientam organizações na identificação, proteção, detecção, resposta e recuperação de ameaças digitais. Funciona como um roteiro organizacional que traduz conceitos técnicos complexos em ações práticas e mensuráveis.

A Estrutura Conceitual do NIST, especificamente, representa um modelo voluntário baseado em padrões existentes que oferece uma linguagem comum para organizações comunicarem requisitos de cibersegurança com fornecedores e parceiros (NIST, 2024). Diferencia-se de outras Estrutura Conceituais por sua abordagem não-prescritiva, permitindo que organizações de qualquer setor ou porte adaptem suas diretrizes conforme necessidades específicas, prioridades de risco e recursos disponíveis. Conforme estabelecido oficialmente:

> O NIST CSF 2.0 fornece orientações para a indústria, agências governamentais e outras organizações para gerenciar riscos de cibersegurança. Ele oferece uma taxonomia de resultados de cibersegurança em alto nível que pode ser utilizada por qualquer organização.[18] (NIST, 2024, p. ii).

Esta característica permite que organizações adaptem as diretrizes às suas necessidades operacionais particulares, mantendo a proteção de sistemas críticos.

O NIST CSF 2.0 estrutura-se em três partes logicamente organizadas. A primeira parte, chamada de PROCESSO, possui seis funções principais que formam um ciclo contínuo de gestão de riscos cibernéticos denominados [19] : Governar (Governança e Gestão estratégica de ativos), Identificar (identificação de ativos e riscos), Proteger (implementação de salvaguardas), Detectar (descoberta de eventos de segurança), Responder (desenvolvimento de ações apropriadas diante de incidentes) e Recuperar (manutenção de planos de resiliência e restauração). (NIST, 2024).

A segunda parte, chamada de NÍVEL DE MATURIDADE, apresenta uma tabela de classificação que permite ao planejador realizar uma autoavaliação da maturidade organizacional da instituição de modo a ter um ponto de partida para implementação das medidas de segurança cibernética (NIST, 2024).

---

[18] The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization. (Tradução Nossa).

[19] Govern, Identify, Protect, Detect, Respond, Recover. (Tradução Nossa).

A terceira parte, chamada de PERFIL, permite uma abordagem sistemática da organização visando avaliar sua postura atual de cibersegurança, estabelecendo objetivos de melhoria para comunicar requisitos de segurança de forma padronizada promovendo aperfeiçoamento até alcançar a postura desejada (NIST 2024).

Complementando a Estrutura Conceitual, o NIST emite diversas publicações especiais[20], algumas das quais o Governo americano emprega amplamente em agências federais, exigindo-as como requisito mínimo para relacionar-se com contratantes do Departamento de Defesa, como o NIST SP 800-171[21] referente à segurança da informação em contratos.

3.2 O PROCESSO

É o elemento central do NIST CSF 2.0, núcleo estruturante da Estrutura Conceitual, composto por seis funções (Governar, Identificar, Proteger, Detectar, Responder, Recuperar). Essas funções tornam as atividades de cibersegurança, aplicáveis a qualquer setor. Destaca-se que a função Governar foi incluída na última atualização para reforçar a gestão estratégica do risco cibernético. Cada função é subdividida em categorias e subcategorias[22], permitindo que as organizações adaptem a Estrutura Conceitual às suas realidades. O Processo serve como base para criar perfis personalizados de cibersegurança, alinhando proteção digital aos objetivos estratégicos da organização (NIST, 2024).

[20]As Publicações Especiais (Special Publications - SP) do NIST são documentos técnicos numerados que fornecem diretrizes sobre segurança da informação, cibersegurança e gestão de riscos, sendo amplamente utilizados como referência oficial por governos, empresas e aliados, inclusive em contratos. (NIST, 2024)

[21]Publicação que fornece às agências federais requisitos de segurança para proteger Informações Controladas Não Classificadas (CUI) em sistemas e organizações não federais.

[22]São subdivisões das funções principais do Processo (Govern, Identify, Protect, Detect, Respond, Recover). Elas representam grupos temáticos de resultados específicos esperados, servindo como ponte entre os objetivos estratégicos e as ações práticas de segurança cibernética. A presente descrição não se aprofundará nas subcategorias. (NIST 2024).

Figura 1 - O PROCESSO

Fonte: O Autor

3.2.1 A Função IDENTIFICAR e o Mapeamento Ativo de Riscos

A função IDENTIFICAR constitui a base fundamental do NIST CSF 2.0, concentrando-se na compreensão dos riscos cibernéticos organizacionais. Proporciona visibilidade sobre ativos, vulnerabilidades e ameaças através de processos sistemáticos de inventário, avaliação e categorização detalhada. (NIST, 2024).

Esta função abrange três categorias fundamentais[23]: O Gerenciamento de Ativos, que estabelece inventários completos para mapear o ambiente organizacional, a Avaliação de Riscos, que analisa vulnerabilidades e ameaças para compreender riscos específicos, e o Aprimoramento, que identifica oportunidades de melhoria nos processos de identificação.

A implementação requer que operadores desenvolvam metodologias de descoberta e catalogação de ativos digitais (CISA, 2021). O planejamento operacional envolve estabelecer cronogramas de varredura automatizada, definir responsabilidades para inventário manual, configurar ferramentas de descoberta e implementar processos de classificação, conforme orientações do NIST (NIST, 2018). Operadores estruturam fluxos integrando coleta com validação humana.

A função IDENTIFICAR conecta-se com todas as demais funções do Processo, pois alimenta a GOVERNAR com contexto organizacional, fornece dados para a função PROTEGER, ao implementar salvaguardas, subsidia a DETECTAR, com conhecimento sobre comportamentos normais, orienta a RESPONDER, na priorização e informa a RECUPERAR qual o status inicial dos ativos a serem restaurados.

[23] Asset Management, Risk Management e Improvement. (NIST, 2024, Tradução Nossa).

A função demonstra aplicabilidade em guerra cibernética. Sua capacidade de proporcionar consciência situacional, identificar ativos críticos e avaliar vulnerabilidades constitui pré-requisito operacional.

3.2.2 As ações da Função PROTEGER

A função PROTEGER constitui o núcleo das salvaguardas organizacionais no NIST CSF 2.0, concentrando-se na implementação de medidas preventivas para limitar ou conter o impacto de eventos cibernéticos. Estabelece controles técnicos e administrativos para proteger ativos críticos através de múltiplas camadas de defesa.

Esta função representa a concretização das capacidades defensivas da organização, pois "são empregadas salvaguardas para gerir os riscos cibernéticos da organização"[24] (NIST, 2024, p.19)

Esta função abrange cinco categorias fundamentais: o Gerenciamento de Identidade, Autenticação e Controle de Acesso, que administra identidades e acessos organizacionais; a Conscientização e Treinamento, que desenvolve capacidades humanas através de programas educacionais; a Segurança da Informação, que protege informações organizacionais em todos os estados; a Segurança da Plataforma, que assegura integridade de sistemas e aplicações; e a Resiliência da Infraestrutura Tecnológica, que assegura estruturas de TI robustas e tolerantes a falhas.

A implementação requer que operadores estabeleçam arquiteturas de defesa em profundidade através de controles técnicos e administrativos integrados (CISA, 2025). O planejamento operacional envolve configurar sistemas de autenticação multifator, implementar políticas de menor privilégio, estabelecer programas de treinamento em conscientização cibernética e desenvolver procedimentos de backup, conforme diretrizes do NIST (NIST, 2018). Operadores estruturam camadas defensivas combinando tecnologia, processos e pessoas.

A função PROTEGER conecta-se com todas as demais funções da Estrutura Conceitual, pois utiliza informações da IDENTIFICAR para priorizar salvaguardas baseadas em criticidade de ativos, alimenta a DETECTAR com dados referentes a eventos de segurança que permitem monitoramento contínuo, fornece controles que

[24] Safeguards to manage the organization's cybersecurity risks are used (Tradução Nossa)

limitam impactos para a função RESPONDER através de contenção automática, e estabelece bases seguras para a função RECOVER.

A função demonstra aplicabilidade em guerra cibernética. Sua capacidade de estabelecer defesas em profundidade, proteger ativos críticos e manter operações sob ataque constitui fundamento operacional para resistência em conflitos cibernéticos. A implementação coordenada permite que organizações mantenham capacidades essenciais durante ataques.

3.2.3 Monitoramentos e Análises da Função DETECTAR

A função DETECTAR constitui a capacidade da organização de identificar incidentes cibernéticos de maneira tempestiva, com foco na detecção de comportamentos atípicos, sinais de invasão e outros eventos potencialmente perigosos. Para isso, estabelece mecanismos de monitoramento contínuo que viabilizam o reconhecimento precoce de ameaças, por meio da análise sistemática das informações de segurança. "Possíveis ataques e comprometimentos cibernéticos são identificados e analisados". (NIST, 2024, p. 21).

Esta função abrange duas categorias fundamentais: o Monitoramento Contínuo, que observa ativos organizacionais para encontrar anomalias, indicadores de comprometimento e outros eventos potencialmente adversos através de observação permanente de redes, ambiente físico, atividades de pessoal e serviços externos, e a Análise de Eventos Adversos, que analisa anomalias e indicadores para caracterizar eventos e detectar incidentes cibernéticos mediante correlação de informações.

A implementação requer que operadores estabeleçam sistemas de monitoramento contínuo através de ferramentas automatizadas de processos analíticos (CISA, 2025). O planejamento operacional envolve configurar sistemas de detecção de intrusão, implementar análise comportamental, estabelecer correlação de eventos e desenvolver capacidades de análise forense, conforme diretrizes do NIST (NIST, 2018). Operadores estruturam múltiplas fontes de coleta de dados que combinam varredura automatizada, análise algorítmica e validação humana.

A função DETECTAR conecta-se com todas as funções da Estrutura Conceitual: utiliza informações do IDENTIFICAR para priorizar monitoramento baseado em criticidade de ativos, aproveita os dados de eventos de segurança gerados pela PROTEGER para alimentar análises, fornece alertas e inteligência que

orientam a função RESPONDER através de caracterização de incidentes, e estabelece dados forenses que suportam a RECUPERAR.

A função demonstra aplicabilidade em guerra cibernética. Sua capacidade de identificar ataques em tempo real, caracterizar ameaças sofisticadas e fornecer inteligência acionável constitui fundamento operacional para consciência situacional em conflitos cibernéticos. A implementação coordenada permite que organizações mantenham vigilância contínua durante ataques persistentes e altamente sofisticados.

3.2.4 Agilidade na Reação a Incidentes da Função RESPONDER

A função RESPONDER constitui a capacidade organizacional de executar ações apropriadas em relação a incidentes cibernéticos detectados no NIST CSF 2.0, concentrando-se na gestão coordenada de respostas para minimizar impactos e restaurar operações normais. Estabelece procedimentos que permitem reação eficaz através de análise detalhada do dano, comunicação coordenada com diversos setores do sistema e mitigação rápida. São "Ações adotadas em relação a um incidente cibernético detectado."[25] (NIST, 2024, p. 22).

Esta função abrange quatro categorias fundamentais[26]: Gerenciamento de incidentes, que coordena as respostas através de execução coordenada de planos, triagem e elaboração de relatórios; Análise de Incidentes, que conduz investigações para compreender os eventos ocorridos e preservar os registros; Resposta de Comunicação de Incidentes, que coordena atividades com as partes interessadas[27]; e Mitigação de Incidentes, que executa atividades para prevenir expansão e mitigar efeitos.

---

[25] Actions regarding a detected cybersecurity incident are taken” (Tradução Nossa).

[26] 1- Gerenciamento: Subtópicos incluem execução do plano de resposta a incidentes em coordenação com terceiros relevantes, triagem e validação de relatórios de incidentes, categorização e priorização de incidentes, escalação ou elevação de incidentes conforme necessário, e aplicação de critérios para iniciar recuperação de incidentes. 2- Análise: Subtópicos incluem análise para estabelecer eventos ocorridos durante incidente e causa raiz, registro de ações executadas durante investigação com preservação de integridade e proveniência. coleta de dados e metadados de incidentes com preservação de integridade e proveniência, estimativa e validação da magnitude do incidente; 3- Relatórios e Comunicação durante a Resposta a Incidentes: Subtópicos incluem notificação de stakeholders internos e externos sobre incidentes e compartilhamento de informações com stakeholders designados; e 4- Mitigação: Subtópicos incluem contenção de incidentes e erradicação de incidentes. (NIST, 2024).

[27] stakeholders (Tradução Nossa): De forma simples, são pessoas, grupos ou organizações que podem afetar ou ser afetados pelas ações, decisões, políticas ou operações de uma empresa ou projeto.

A implementação busca responder questões fundamentais: como conter rapidamente propagação de ameaças, como coordenar equipes multidisciplinares durante crises, como preservar evidências forenses e como manter operações durante incidentes. (NIST, 2024).

O planejamento operacional desta função envolve o estabelecimento de planos de resposta, as equipes, os procedimentos de comunicação e a criação capacidades de análise forense (NIST, 2024). Conforme constam em veículos especializados como Bleeping Computer (2018) e Supply Chain Dive (2018), a empresa dinamarquesa Maersk conseguiu restaurar cerca de 4.000 servidores e 45.000 computadores em apenas dez dias, demonstrando que uma recuperação rápida após um ataque cibernético, passa por uma adequada estrutura de resposta a incidentes[28].

A função RESPONDER demonstra aplicabilidade direta em guerra cibernética. Sua capacidade de coordenar respostas rápidas, gerenciar incidentes complexos e manter operações durante ataques constitui fundamento operacional para resiliência em conflitos cibernéticos. A implementação coordenada permite que organizações respondam eficazmente a ataques sofisticados e coordenados.

Além disso, esta função conecta-se com todas as demais da Estrutura Conceitual, pois utiliza informações da IDENTIFICAR para priorizar resposta baseada em criticidade de ativos, aproveita controles da PROTEGER para implementar contenção, recebe alertas da DETECTAR para iniciar procedimentos de resposta, e coordena com a RECUPERAR uma transição eficaz para restauração operacional.

3.2.5 A Restauração e Retomada de Ativos com a Função RECUPERAR

A função RECUPERAR constitui a capacidade organizacional de restaurar sistemas, dados e operações afetados por incidentes cibernéticos, conforme definido no NIST CSF 2.0, concentrando-se na implementação de atividades de recuperação para retornar à operação normal. Estabelece procedimentos que incluem validação de integridade de backups, restauração de sistemas comprometidos, verificação de ativos recuperados e declaração formal do fim da recuperação baseada em critérios.

[28] O ataque “Maersk NotPetya”, ocorrido em 27 de junho de 2017, foi um dos maiores e mais impactantes ataques cibernéticos contra infraestrutura corporativa já registrados. Ele atingiu a AP Moller–Maersk, gigante dinamarquesa do transporte marítimo e logística, que movimenta cerca de 20% do comércio mundial em contêineres. (GREENBERG, 2018).

Esta função abrange duas categorias fundamentais[29]: O Plano de Recuperação de Incidentes, que estabelece planos de recuperação que incluem papéis, responsabilidades, estratégias e métricas; e a Comunicação de Recuperação de Incidentes, que coordena atividades de restauração com partes internas e externas através de comunicação sobre progresso e atualizações públicas.

A implementação busca responder questões fundamentais: como restaurar rapidamente operações críticas, como validar integridade de sistemas restaurados, como coordenar comunicações durante recuperação e como estabelecer normas operacionais pós-incidente.

Operadores definem cronogramas de recuperação, designam responsabilidades específicas para cada fase, estabelecem critérios de validação de sistemas e criam protocolos de comunicação com partes interessadas internas e externas (CISA, 2025).

O planejamento operacional envolve desenvolver planos de recuperação com objetivos de tempo específicos (RTO), estabelecer pontos de recuperação aceitáveis (RPO), implementar procedimentos de teste de integridade e criar capacidades de comunicação (NIST, 2024).

O Departamento de Defesa dos Estados Unidos prioriza estratégias de recuperação através de backups imutáveis que resistem a alterações maliciosas, análises forenses automatizadas para identificar último estado confiável dos dados, monitoramento de anomalias durante processo de restauração e validação criptográfica de integridade para garantir continuidade de missão crítica (ROSIEK, 2024).

A função demonstra aplicabilidade direta em guerra cibernética. Sua capacidade de restaurar rapidamente operações críticas, validar integridade de sistemas e manter continuidade de missão constitui fundamento operacional para

[29]1- Incident Recovery Planning: Subtópicos incluem plano de recuperação incorpora lições aprendidas, ações de recuperação são selecionadas, escopo definido, priorizado e executado, integridade de backups e outros ativos de restauração é verificada antes de usá-los, funções de missão crítica e gestão de riscos cibernéticos são consideradas para estabelecer normas operacionais pós-incidente, integridade de ativos restaurados é verificada, sistemas e serviços são restaurados e status operacional normal é confirmado, O fim da recuperação de incidente é declarado baseado em critérios e a documentação relacionada ao incidente é completada; e 2- Incident Recovery Communication: Subtópicos incluem, atividades de recuperação e progresso na restauração de capacidades operacionais são comunicados a stakeholders internos e externos designados, atualizações públicas sobre recuperação de incidente são compartilhadas usando métodos e mensagens aprovados. (NIST, 2024).

resiliência em conflitos prolongados. A implementação coordenada permite que organizações mantenham capacidades operacionais essenciais durante ataques sustentados estrategicamente direcionados.

RECOVER conecta-se com todas as funções da Estrutura Conceitual: utiliza informações do IDENTIFY para priorizar recuperação baseada em criticidade de ativos, aproveita controles do PROTECT para implementar salvaguardas durante restauração, recebe informações do DETECT para avaliar extensão de comprometimento, e coordena com RESPOND para transição eficaz de contenção para restauração operacional.

3.2.6 GOVERN: Direção e Governança

A função GOVERN representa a principal inovação do NIST CSF 2.0, estabelecendo capacidades organizacionais fundamentais para desenvolver, implementar e supervisionar estratégias abrangentes de cibersegurança alinhadas aos objetivos organizacionais estratégicos e requisitos regulamentares específicos.

Esta função materializa a governança cibernética através de estruturas organizacionais robustas que definem autoridades executivas específicas, estabelecem métricas quantificáveis de conformidade mensuráveis, criam comitês especializados de supervisão com responsabilidades claramente delimitadas e implementam processos estruturados de revisão periódica que orientam decisões estratégicas críticas em todos os níveis hierárquicos organizacionais.

O NIST CSF 2.0 define Governar como "A estratégia, as expectativas e as políticas de gestão de riscos cibernéticos da organização são estabelecidas, comunicadas e monitoradas."[30] (NIST, 2024, p. 15). Essa função surgiu para suprir uma lacuna relevante identificada na versão CSF 1.1, que não contemplava uma estrutura formal voltada à governança estratégica da cibersegurança.

Organizações implementavam as cinco funções originais (Identificar, Proteger, Detectar, Responder e Recuperar) sem direcionamento executivo consistente, resultando em desalinhamento entre práticas operacionais e objetivos organizacionais. Governar estabelece fundamentos estratégicos que orientam

[30] “The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored”. (Tradução Nossa).

implementação coordenada das demais funções através de seis categorias [31] : Contexto Organizacional, Estratégia de Gestão de Riscos, Papéis, Responsabilidades e Autoridades, Política, Supervisão e Gestão de Riscos na Cadeia de Suprimentos. (NIST, 2024).

> A função Governar fornece o contexto necessário para que as organizações estabeleçam e monitorem sua gestão de riscos cibernéticos, estratégia, expectativas e políticas. O NIST descreve a função Govern como "transversal", sendo projetada para ajudar as equipes de segurança a priorizarem os resultados definidos nas outras cinco funções. [32] (EXPEL, 2024, online).

Operadores estruturam governança através de definição quantitativa precisa da chamada “Aptidão ao Risco”[33], estabelecimento de políticas específicas detalhadas para cada domínio tecnológico crítico, designação de responsabilidades executivas claras com autoridades bem delimitadas e implementação de métricas abrangentes de supervisão contínua baseadas em indicadores mensuráveis. Segundo CISA (2025), planejamento estratégico de governança requer integração sistemática coordenada entre liderança executiva sênior, equipes técnicas especializadas e partes interessadas externas relevantes para criar estruturas decisórias eficazes e resilientes.

Organizações estabelecem comitês multidisciplinares especializados, definem autoridades específicas hierárquicas para tomada de decisão estratégica, implementam processos estruturados de revisão periódica sistemática e desenvolvem mecanismos sofisticados de comunicação que garantem alinhamento estratégico contínuo entre objetivos organizacionais e práticas operacionais de cibersegurança.

GOVERNAR relaciona-se fundamentalmente com todas as funções do NIST CSF 2.0, estabelecendo diretrizes estratégicas abrangentes para IDENTIFICAR, definindo políticas detalhadas para PROTEGER, autorizando procedimentos específicos para DETECTAR, aprovando protocolos para RESPONDER e supervisionando atividades coordenadas de RECUPERAR.

---

[31] Organizational Context, Risk Management Strategy, Roles, Responsibilities, and Authorities, Policy, Oversight e Supply Chain Risk Management. (Tradução Nossa).

[32] The Govern function provides context that helps orgs establish and monitor their cybersecurity risk management, strategy, expectations, and policy. NIST describes the Govern function as "cross-cutting," and it's designed to help security teams prioritize the outcomes outlined in the other five functions (TRADUÇÃO NOSSA)

[33] Risk Apetite (Tradução Nossa): é a quantidade e o tipo de risco que uma organização está disposta a buscar ou manter (ISO 31037:2022, 3.3.27)

Esta função cria a estrutura decisória que permeia todo ciclo de vida da cibersegurança organizacional, garantindo alinhamento estratégico contínuo.

A aplicabilidade em guerra cibernética fundamenta-se na necessidade crítica de estruturas decisórias robustas durante conflitos prolongados e intensos. GOVERN estabelece autoridades claras, processos de escalação bem definidos e mecanismos de supervisão que permitem coordenação estratégica eficaz sob pressão operacional, garantindo que decisões cibernéticas mantenham alinhamento com objetivos militares durante operações de combate.

3.3 Os Níveis de Maturidade: Da Maturidade Parcial à Adaptativa

Os Níveis de Maturidade constituem uma caracterização do rigor das práticas de governança e gestão de riscos cibernéticos organizacionais no NIST CSF 2.0. Representam uma progressão estruturada desde respostas informais até abordagens ágeis, informadas por risco e em melhoria contínua. Os Níveis de Maturidade fornecem contexto sobre como uma organização visualiza riscos cibernéticos e os processos implementados para gerenciá-los, estabelecendo quatro níveis distintos de maturidade organizacional (NIST, 2024).

Os Níveis de Maturidade servem para estabelecer o tom geral de como uma organização gerenciará seus riscos cibernéticos, complementando metodologias existentes de gestão de risco em vez de substituí-las. Funcionam como um padrão comparativo interno, facilitando a comunicação sobre maturidade de práticas de segurança. Organizações utilizam Níveis de Maturidade para informar seu Perfil Atual e o Perfil Alvo, orientando progressão quando riscos são maiores ou quando análise custo-benefício indica redução viável de riscos cibernéticos negativos.

O NIST CSF 2.0 define:

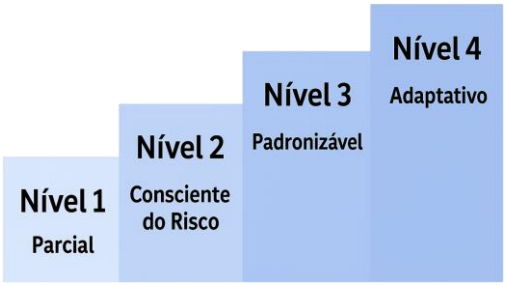
> Os Níveis caracterizam o rigor da governança e das práticas de gestão de riscos cibernéticos de uma organização e fornecem contexto sobre como ela enxerga os riscos de cibersegurança e os processos existentes para gerenciá-los.[34] (NIST, 2024, p. 7).

[34] "Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks". (Tradução Nossa).

Conforme o Nível de maturidade, uma organização pode ser classificada em: Parcial, Consciente do Risco, Padronizável e Adaptativo [35], refletindo práticas organizacionais desde gestão parcial até abordagens adaptativas e continuamente aprimoradas.

Os Níveis de Maturidade conectam-se integralmente com toda a estrutura do NIST CSF 2.0, caracterizando o rigor das práticas de governança e gestão de riscos cibernéticos. Fornecem contexto para implementação das seis funções do Processo, orientando organizações na seleção de níveis apropriados, recursos disponíveis e requisitos regulamentares.

Figura 2 – OS NÍVEIS DE MATURIDADE



Fonte: O AUTOR

Os Níveis de Maturidade orientam a construção dos Perfis Organizacionais e servem como referência para comunicar às partes interessadas o Nível de maturidade das práticas de cibersegurança adotadas pela organização.

3.4 OS PERFIS: DO ATUAL AO DESEJADO

No NIST CSF 2.0, o Perfil descreve a postura atual e/ou o objetivo futuro de cibersegurança da organização, funcionando como referência para orientar as ações das seis funções do Processo. É composto pelo Perfil Atual[36], que indica os resultados hoje alcançados, e pelo Perfil Desejado[37], que define as metas priorizadas para gestão de riscos (NIST, 2024).

[35] Respectivamente: TIER 1, TIER 2, TIER 3 e TIER 4. (Tradução Nossa).
[36] Current Profile. (Tradução Nossa).
[37] Target Profile. (Tradução Nossa).

Os Perfis permitem personalizar a aplicação do CSF de acordo com necessidades específicas, missão, tolerância ao risco e recursos disponíveis. Também ajudam a identificar as lacunas entre o estado atual e o desejado, apoiando o desenvolvimento de planos e a definição de investimentos.

Além disso, servem para comunicar de forma clara requisitos e expectativas a fornecedores, parceiros e terceiros, estabelecendo metas mensuráveis a serem atingidas. Dessa maneira, o Perfil integra o diagnóstico interno com o planejamento futuro e fortalece o alinhamento entre objetivos gerais da organização e as práticas de cibersegurança.

O NIST CSF 2.0 define que "Um Perfil Organizacional descreve a postura atual e/ou alvo de cibersegurança de uma organização com base nos resultados obtidos pelo uso do Processo."[38] (NIST, 2024, p. 6).

Perfis são utilizados para "Compreender, adaptar e priorizar a implementação do CSF com base nas necessidades específicas da organização, sua missão, tolerância ao risco e recursos disponíveis."[39] (NIST, 2024, p.6), permitindo que se personalize a aplicação da Estrutura Conceitual conforme contexto operacional específico.

Figura 3 – PASSOS PARA ESTABELECER UM PERFIL ORGANIZACIONAL

Fonte: O AUTOR

Os Perfis conectam-se com toda a arquitetura do NIST CSF 2.0, servindo como ponte entre o Processo abstrato e a implementação prática. Utilizam resultados das

[38]A CSF Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. (Tradução Nossa).

[39]“understand, tailor, and prioritize CSF implementation based on an organization's specific needs, mission, risk tolerance, and available resources” (Tradução Nossa).

seis funções (Governar, Identificar, Proteger, Detectar, Responder, Recuperar) para criar uma representação de identidade da cibersegurança atual. Integram-se com o Nível de Maturidade identificado para caracterizar rigor de práticas organizacionais e com as informações referenciadas[40] e para mapear controles específicos. Facilitam ciclo contínuo de avaliação, planejamento e melhoria que conecta estratégia executiva com implementação prática de cibersegurança.

3.5 REFLEXÕES PARA O USO EM DEFESA

Em síntese, o NIST CSF 2.0 oferece uma forma sistematizada de compreender e gerenciar riscos cibernéticos, articulando suas seis funções principais em um ciclo contínuo no qual cada etapa reforça e depende das demais. A função Governar desempenha um papel central ao estabelecer diretrizes estratégicas, políticas e papéis organizacionais que sustentam a execução integrada das demais funções.

Esse arranjo, construído em forma cíclica modular e com terminologia clara, facilita sua compreensão e adoção por diferentes áreas e níveis hierárquicos, independentemente do grau de familiaridade técnica dos profissionais envolvidos.

Os Níveis de Maturidade complementam essa estrutura ao permitir que cada organização avalie o grau de maturidade de suas práticas de segurança cibernética. Por meio dessa análise, torna-se possível identificar pontos fortes e lacunas, definindo o Nível de formalidade necessário para processos internos e priorizando recursos. Ao mesmo tempo, o diagnóstico realizado pelos Níveis de Maturidade depende das informações consolidadas pelo Processo, mas também devolve a ele parâmetros que orientam a intensidade e o foco das ações em cada função, criando um movimento de retroalimentação que reforça o caráter adaptativo da Estrutura Conceitual.

Já os Perfis Organizacionais viabilizam o planejamento para transitar do estado atual para o desejado, alinhando o progresso técnico às demandas internas e

[40]Do original “Informative References” cuja definição é: “São mapeamentos que indicam relações entre o Processo e diversos padrões, diretrizes, regulamentações e outros conteúdos. As Referências Informativas ajudam a orientar como uma organização pode alcançar os resultados do Processo. Essas referências podem ser específicas de um setor ou tecnologia. Podem ser produzidas pelo NIST ou por outra organização. Algumas Referências Informativas possuem escopo mais restrito do que uma Subcategoria. (...) pode ser apenas uma das várias referências necessárias para atingir o resultado descrito em uma Subcategoria. Outras Referências Informativas podem ser de Nível mais elevado, como um requisito de uma política que aborda parcialmente diversas Subcategorias. Ao utilizar o CSF, uma organização pode identificar as Referências Informativas mais relevantes.” (Tradução Nossa).

externas, como contratos a serem cumpridos ou regulações específicas. Esses Perfis refletem a visão consolidada dos riscos e controles obtida pelas funções do Processo e, ao mesmo tempo, fornecem a elas um roteiro que prioriza e sequência as iniciativas necessárias. Os Perfis também se conectam diretamente aos Níveis de Maturidade, uma vez que a definição de metas futuras depende do entendimento do estágio de maturidade alcançado e dos recursos disponíveis para avançar.

Esse conjunto articulado Processo, Níveis de Maturidade e Perfis confere à Estrutura Conceitual uma aplicabilidade ampla, permitindo que organizações de diferentes setores e tamanhos empreguem seus conceitos de forma integral ou parcial, adaptando-os à sua realidade operacional. Cabe a cada instituição realizar o trabalho de contextualização, ajustando os princípios e práticas da Estrutura Conceitual aos seus próprios riscos, objetivos estratégicos e capacidade de investimento, dentro de uma linguagem acessível em Nível de entendimento e em com linguagem coerente à sua cultura organizacional, garantindo que o modelo se torne efetivo às suas necessidades específicas.

Dessa maneira, o NIST CSF 2.0 estabelece uma base metodológica que pode apoiar desde ações pontuais até programas contínuos e integrados de gestão de riscos cibernéticos.

4 A COMPARAÇÃO DAS DOUTRINAS

4.1. INTRODUÇÃO

4.1.1. Propósito da Análise

Este capítulo tem como propósito fundamental apresentar uma análise sobre a aderência do NIST CSF 2.0 ao Processo de Planejamento Conjunto (PPC), no nível operacional, com o foco de identificar, de forma imediata, a existências de convergências, aderências parciais que demandem considerações e, igualmente importante, onde residem incompatibilidades conceituais ou práticas.

4.1.2. Abordagem Metodológica

A metodologia empregada nesta análise foi qualitativa e comparativa, entres os pontos de contato do NIST CSF 2.0 (As três estruturas básicas do NIST e as seis funções do processo) com as três etapas do PPC.

A análise aqui desenvolvida está estritamente delimitada ao nível operacional do planejamento militar. Questões de natureza estratégica ou tática, embora relevantes para o contexto cibernético mais amplo, não serão abordadas diretamente neste capítulo. O foco reside na operacionalização da defesa cibernética no âmbito do PPC, visando aprimorar a capacidade de planejamento e execução de operações conjuntas no domínio cibernético.

4.2 Identificação de Aderências: O Processo do NIST CSF 2.0 e o PPC

4.2.1 A função IDENTIFICAR e o Exame de Situação Operacional

A função IDENTIFICAR, do NIST CSF 2.0, que se concentra na compreensão e gestão dos riscos de segurança cibernética para sistemas, ativos, dados e capacidades, encontra uma aderência natural com a etapa de Exame de Situação Operacional do PPC. Nesta fase do planejamento militar, é desejável que o Comandante e seu Estado Maior compreendam o domínio cibernético.

A identificação de ativos críticos, ameaças e vulnerabilidades cibernéticas, conforme preconizado pela função IDENTIFICAR complementa diretamente a avaliação do ambiente operacional, permitindo uma visão mais completa dos riscos e oportunidades.

No entanto, a aderência pode ser parcial quando se trata da linguagem e da cultura organizacional, enquanto o NIST CSF 2.0 utiliza termos mais corporativos, o ambiente militar exige uma tradução para sua terminologia específica, como a classificação de sistemas de armas ou redes de Comando e Controle enquanto Ciber ativos. A ausência de um mapeamento direto de termos pode gerar uma aderência parcial que demande adaptação.

4.2.2. A função PROTEGER e a Elaboração de Planos e Ordens

A função PROTEGER do NIST CSF 2.0 visa desenvolver e implementar salvaguardas apropriadas para garantir a entrega de serviços de infraestrutura crítica. Esta função possui uma aderência natural com a etapa de Elaboração de Planos e Ordens do PPC, especialmente na construção do Anexo H – Defesa Cibernética.

As medidas de proteção, como controle de acesso, treinamento de conscientização e segurança de dados, são essenciais para a resiliência das operações militares. A compatibilidade de conceitos é alta, pois ambos buscam a prevenção de incidentes.

Contudo, a aderência pode ser parcial em relação à abrangência. Enquanto o PROTECT abrange uma gama ampla de controles, o Anexo H do PPC foca nas medidas diretamente relacionadas à defesa cibernética militar, o que pode exigir uma seleção e adaptação dos controles do NIST para o contexto específico das operações conjuntas. A implementação de certas salvaguardas pode ser mais complexa em ambientes militares devido a restrições operacionais e tecnológicas.

4.2.3. As funções DETECTAR, RESPONDER, RECUPERAR e o Controle de Operação Planejada

As funções DETECTAR (identificar a ocorrência de um evento de segurança cibernética), RESPONDER (tomar ações para conter um evento de segurança cibernética detectado) e RECUPERAR (desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados devido a um evento de segurança cibernética) do NIST CSF 2.0, encontram uma aderência natural com a etapa de Controle da Operação Planejada do PPC.

A capacidade de detectar incidentes cibernéticos em tempo real, responder a eles de forma eficaz e recuperar sistemas e dados comprometidos é vital para a

continuidade das operações militares. A sinergia é evidente na necessidade de consciência situacional, tomada de decisão rápida e gestão de crises.

No entanto, a aderência pode ser parcial devido à natureza dinâmica e imprevisível do ambiente de combate. Enquanto o NIST oferece uma Estrutura Conceitual robusta, a aplicação em um cenário de guerra cibernética exige adaptações significativas nos procedimentos e na velocidade de resposta. A coordenação entre as equipes de segurança cibernética e as forças operacionais pode ser um ponto de aderência parcial que demanda treinamento e integração contínuos.

4.2.4. A Função GOVERNAR e a Estrutura Doutrinária Brasileira

A função GOVERNAR do NIST CSF 2.0, que se concentra em desenvolver e implementar a estratégia de segurança cibernética da organização, encontra uma aderência parcial com a estrutura doutrinária brasileira, especialmente nos Níveis Decisórios da Defesa Cibernética. Embora a doutrina militar brasileira já possua uma estrutura de governança bem definida, o GOVERNAR oferece uma Estrutura Conceitual explícita para definir a aptidão ao risco, políticas e responsabilidades de governança, alinhando a estratégia cibernética com os objetivos militares mais amplos.

A aderência é parcial porque a natureza hierárquica e prescritiva das forças armadas pode não se alinhar completamente com a abordagem mais flexível e baseada em risco do NIST, assim como a implementação de um modelo de governança cibernética baseado na Função GOVERNAR exigiria uma adaptação cuidadosa para respeitar a cadeia de comando do Nível Operacional.

4.3. Desafios e Incompatibilidades

A ausência de um equivalente direto para os Níveis de Maturidade e Perfis do NIST CSF 2.0 representa uma aderência parcial, pois essas ferramentas poderiam ser úteis para avaliar o rigor das práticas e planejar sua evolução, mas demandariam uma adaptação conceitual ampla para o contexto militar.

4.3.1. A Linguagem do NIST CSF 2.0

A diferença fundamental entre a natureza do NIST CSF 2.0 e a doutrina militar brasileira reside em seus propósitos e contextos de origem. O NIST CSF foi concebido

como uma Estrutura Conceitual voluntária e flexível, destinado a organizações de diversos setores para um contexto corporativo internacional.

Sua linguagem e abordagem são inerentemente corporativas, visando a conformidade e a eficiência em um ambiente de negócios. Em contraste, a doutrina militar brasileira, por sua própria natureza, é hierárquica e focada na eficácia operacional em cenários de conflito.

Esta distinção gera incompatibilidades conceituais de natureza cultural. Termos e conceitos do NIST, tem um sentido empresarial e não se traduzem diretamente para a tomada de decisão militar. Acrescenta-se ainda que a cultura militar, baseada em disciplina e hierarquia, pode encontrar atrito com a flexibilidade inerente a uma estrutura de Cibersegurança voluntária. Essas diferenças terminológicas e contextuais impedem uma aderência direta e demandam tradução e interpretação cuidadosas para qualquer tentativa de integração.

4.3.2. Elementos sem Equivalência Direta

Alguns elementos do NIST CSF 2.0 não possuem um equivalente direto na doutrina militar brasileira, o que representa um desafio significativo para sua aplicação. Os Níveis de Maturidade e Perfis do NIST CSF 2.0 são exemplos claros.

Os Níveis de Maturidade permitem que as organizações avaliem a maturidade de seus programas de segurança cibernética, enquanto os Perfis fornecem um mecanismo para alinhar os requisitos de segurança com os objetivos de negócios.

Esta pesquisa não identificou um sistema formalizado de avaliação de maturidade cibernética que se compare diretamente aos Níveis de Maturidade do NIST CSF 2.0. Da mesma forma, a ideia de "perfis" para adaptar a Estrutura Conceitual a diferentes setores ou objetivos de negócios não se alinha diretamente com a natureza universal e padronizada da doutrina militar.

A ausência desses equivalentes diretos significa que, para que esses elementos do NIST CSF 2.0 sejam úteis no contexto militar, eles precisariam ser completamente adaptados ou, em alguns casos, descartados. A análise sugere que a tentativa de forçar uma equivalência onde não existe pode levar a distorções e a uma aplicação ineficaz da Estrutura Conceitual, sendo mais produtivo focar nos elementos que possuem maior aderência natural ou parcial.

4.4. Análise dos Resultados

4.4.1. Síntese das aderências Naturais e Parciais

A análise revelou que o NIST CSF 2.0 possui pontos de aderência natural e parcial significativos com o PPC, especialmente nas funções IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER e RECUPERAR. As funções de IDENTIFICAR e PROTEGER se alinham bem com as etapas iniciais do PPC, fornecendo uma estrutura lógica para a avaliação de riscos e a implementação de salvaguardas preventivas.

As funções de DETECTAR, RESPONDER e RECUPERAR, por sua vez, complementam as atividades de controle da operação, oferecendo um modelo para a gestão de incidentes cibernéticos. As aderências parciais surgem principalmente da necessidade de tradução de linguagem e adaptação cultural, onde conceitos corporativos precisam ser reinterpretados para o ambiente militar. Mesmo nos pontos de convergência, a especificidade do contexto militar exige que a aplicação do NIST CSF seja sempre filtrada pela doutrina e pelos princípios operacionais brasileiros.

A principal limitação observada nas aderências naturais e parciais é a ausência de um guia explícito na doutrina militar para a operacionalização da defesa cibernética, lacuna que o NIST CSF pode ajudar a preencher com sua estrutura detalhada.

A função GOVERNAR, embora relevante para a gestão estratégica, encontra uma aderência apenas parcial devido à natureza hierárquica e prescritiva das forças armadas, que difere da abordagem mais flexível do NIST.

4.4.2. Síntese das Incompatibilidades

As incompatibilidades aparentes surgem da natureza e do propósito distintos do NIST CSF 2.0 e da doutrina militar. Elementos como os Níveis de Maturidade e Perfis do NIST CSF 2.0 não possuem equivalência direta na doutrina brasileira, na visão do autor.

A linguagem e o contexto corporativo do NIST CSF 2.0, em contraste com o vocabulário e a cultura militar, também representam uma barreira. A tentativa de integrar esses elementos sem uma adaptação profunda pode resultar em ineficácia ou na perda da clareza doutrinária. Portanto, entende-se que, para esses elementos,

o descarte ou uma reinterpretação radical seria mais apropriado do que uma adaptação superficial.

4.4.3. Avaliação Geral de Viabilidade

A viabilidade de aproveitamento do NIST CSF 2.0 no PPC no nível operacional é considerável, mas não universal. É possível observar que parte dos conceitos e práticas do NIST CSF podem ser aproveitados de forma natural ou com adaptações razoáveis, especialmente as Funções IDENTIFICAR, PROTECTEGER, DETECTAR, RESPONDER e RECUPERAR.

As áreas onde a integração é mais viável são aquelas relacionadas à operacionalização de medidas de segurança cibernética e à gestão de incidentes. Por outro lado, elementos como os Níveis de Maturidade e Perfis e certos aspectos da função GOVERNAR, apresentam incompatibilidades significativas que tornam sua integração inviável ou excessivamente complexa no Nível Operacional.

Em um contexto imediato, recomenda-se que sejam empreendidos esforços para estudos futuros sobre a extração dos princípios e das melhores práticas do NIST CSF 2.0, que complementam diretamente as lacunas operacionais da doutrina brasileira, evitando-se a importação de elementos que não se alinham à cultura e à estrutura militar. O aproveitamento deve ser seletivo e pragmático, visando o aprimoramento da defesa cibernética sem comprometer a clareza e a eficácia da doutrina vigente.

5 CONCLUSÃO DA PESQUISA

Este trabalho buscou explorar a complexa interseção entre a doutrina de planejamento militar e o crescente domínio cibernético, com um enfoque particular no nível operacional. A jornada iniciou-se com a análise aprofundada do Processo de Planejamento Conjunto (PPC) brasileiro, estabelecendo suas bases históricas, estrutura e a evolução que permitiu a formalização do Anexo H – Defesa Cibernética. Compreendeu-se que a integração do ciberespaço não é um adendo, mas uma dimensão intrínseca e indispensável à eficácia das operações conjuntas modernas.

O Capítulo 2 demonstrou como a doutrina militar brasileira, ao longo do tempo, adaptou-se para incorporar novas realidades, culminando na inserção formal da defesa cibernética como uma função operacional. Essa evolução reflete a consciência da dependência crescente das Forças Armadas em relação aos sistemas de informação e a necessidade de proteger e operar eficazmente nesse ambiente.

O Capítulo 3 descreveu o objeto de estudo, sua estrutura em três partes, dentre as quais, uma delas possui seis funções que oferecem um modelo adaptativo para qualquer contexto organizacional.

Posteriormente, a análise se aprofundou na relação entre o NIST CSF 2.0 e o PPC. Essa investigação revelou que, embora o NIST CSF seja uma Estrutura Conceitual de origem corporativa e voluntária, ele oferece pontos de aderência significativos com a doutrina militar brasileira.

Com base no exposto, esta pesquisa atingiu o objetivo de verificar a adequabilidade do uso das ferramentas da Estrutura de Cibersegurança NIST CSF 2.0, identificando aderências nas atividades de identificar ativos críticos, implementar salvaguardas, detectar ameaças, responder a ataques e recuperar sistemas, são elementos que se alinham diretamente com as necessidades do planejamento e da execução de operações militares no Domínio Cibernético.

Este estudo indica que a moldura conceitual presente no NIST CSF 2.0 pode oferecer subsídios relevantes para o avanço da integração entre estruturas civis de cibersegurança e a doutrina de planejamento militar no nível operacional.

Recomenda-se que investigações futuras se concentrem no desenvolvimento de metodologias para a customização do NIST CSF 2.0 a diferentes cenários operacionais, bem como na sua integração com ferramentas específicas de avaliação de maturidade cibernética voltadas ao contexto militar. Adicionalmente, sugere-se

examinar os impactos da interoperabilidade doutrinária com países aliados que já adotam o framework, identificando benefícios e desafios de uma eventual padronização multinacional de práticas de ciberdefesa aplicáveis a operações combinadas.

REFERÊNCIAS

ALURA. O que é Framework? Entenda de uma vez por todas. Alura, 2022. DispoNível em: https://www.alura.com.br/artigos/Framework. Acesso em: 29 jun. 2025.

BLEEPING COMPUTER. Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack. DispoNível em: https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/. Acesso em: 13 jul. 2025.

BRASIL. Ministério da Defesa. MD31-M-07: Doutrina Militar de Defesa Cibernética. 2. ed. Brasília, DF: Ministério da Defesa, 2023.

BRASIL. Ministério da Defesa. Glossário das Forças Armadas – MD35-G-01. 5. ed. Brasília: Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas, 2015.

BRASIL. Ministério da Defesa. MD30-M-01: Doutrina de Operações Conjuntas. Vol. 1. 1.ed. Brasília, DF: Ministério da Defesa, 2011a.

BRASIL. Ministério da Defesa. MD30-M-01: Doutrina de Operações Conjuntas. Vol. 1. 1.ed. Brasília, DF: Ministério da Defesa, 2011b.

BRASIL. Ministério da Defesa. MD30-M-01: Doutrina de Operações Conjuntas. Vol. 1. 2.ed. Brasília, DF: Ministério da Defesa, 2020a.

BRASIL. Ministério da Defesa. MD30-M-01: Doutrina de Operações Conjuntas. Vol. 2. 2.ed. Brasília, DF: Ministério da Defesa, 2020b.

CISA. Cybersecurity Incident Response. 2025. DispoNível em: https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurityincident-response. Acesso em: 10 jul. 2025.

COLLYER, Daniel. Case Study: Maersk's Response to NotPetya – How Cybersecurity Best Practices Mitigated a Major Cyberattack. SOS Intelligence, 2024. DispoNível em: https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-bestpractices-mitigated-a-major-cyberattack/. Acesso em: 10 jul. 2025.

CLARKE, Richard A., KNAKE Robert. Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport Livros e Multimídia, 2015. [5288] p. Ebook.

DEPARTMENT OF DEFENSE. DoDI 8530.02, Cyber Incident Response. 2023. DispoNível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853003p.PDF. Acesso em: 10 jul. 2025.

GREENBERG, Andy. The untold story of NotPetya, the most devastating cyberattack in history. *Wired*, 22 ago. 2018. DispoNível em:

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Acesso em: 13 jul. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO Guide 73:2009 – Risk Management – Vocabulary*. Geneva: ISO, 2009.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. NIST Special Publication 800-171, Rev. 3. Gaithersburg, MD: NIST, 2024. Disponível em: https://doi.org/10.6028/NIST.SP.800-171r3. Acesso em: 10 ago.

NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST.CSWP.29. 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: 10 jul. 2025.

NIST. Computer Security Incident Handling Guide. NIST Special Publication 800-61

Revision 3. 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Acesso em: 10 jul. 2025.

SUPPLY CHAIN DIVE. Maersk reconstructed entire IT infrastructure in 10 days following NotPetya. DispoNível em: https://www.supplychaindive.com/news/maersk-reconstructed-entire-it-infrastructure-in-10-days-following-nyetya/515776/. Acesso em: 13 jul. 2025.

ROSIEK, Travis. Seven cyber resilience recommendations for DoD mission continuity and data recovery. Federal News Network, 2024. DispoNível em: https://federalnewsnetwork.com/commentary/2024/10/seven-cyber-resilience-recommendations-for-dod-mission-continuity-and-data-recovery/. Acesso em: 10 jul. 2025.