UNIVERSIDADE DE BRASÍLIA
FACULDADE DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

José Ricardo Souza Camelo

Ciclo do Conhecimento Organizacional Aplicado à Consciência Situacional de Defesa Cibernética Nacional: Um Framework Estratégico

Brasília/DF
2024

Ciclo do Conhecimento Organizacional Aplicado à Consciência Situacional de Defesa Cibernética Nacional: Um Framework Estratégico

Tese de doutorado apresentada ao Programa de Pós-Graduação em Ciência da Informação da Universidade de Brasília, como requisito para obtenção do título de Doutor em Ciência da Informação.

Orientador: Profa. Dra. Lillian Maria Araujo de Rezende Alvares

Brasília

2024

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Souza Camelo, José Ricardo
SC181cc Ciclo do Conhecimento Organizacional Aplicado à Consciência Situacional de Defesa Cibernética Nacional: Um Framework Estratégico / José Ricardo Souza Camelo; orientador Lillian Maria Araujo de Rezende Alvares. -- Brasília, 2024.
266 p.

Tese(Doutorado em Ciência da Informação) -- Universidade de Brasília, 2024.

1. Conhecimento organizacional. 2. Consciência situacional. 3. Defesa cibernética. 4. Framework. I. Araujo de Rezende Alvares, Lillian Maria , orient. II. Título.

UNIVERSIDADE DE BRASÍLIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Ata Nº: 47

Aos vinte e três dias do mês de fevereiro do ano de dois mil e vinte e quatro, instalou-se a banca examinadora de Tese de Doutorado do aluno **José Ricardo Souza Camelo**, matrícula 19/0002239. A banca examinadora foi composta pelos professores Dr. Marcio de Carvalho Victorino / membro interno / PPGCINF/UnB, Dr. Eduardo Dutra Amadeu Moresi / membro externo / Universidade Católica de Brasília, Dr. João Marinonio Enke Carneiro / membro externo / Escola de Comando e Estado-Maior do Exército (ECEME), Dr. Cláudio Gottschalg Duque / Suplente / PPGCINF/UnB e Dra. Lillian Maria Araujo de Rezende Alvares / orientadora / presidenta / PPGCINF/UnB. O discente apresentou o trabalho intitulado **"Ciclo do Conhecimento Organizacional Aplicado à Consciência Situacional de Defesa Cibernética Nacional: Um Framework Estratégico"**.

Concluída a exposição, procedeu-se a arguição do(a) candidato(a), e após as considerações dos examinadores o resultado da avaliação do trabalho foi:

(X) Pela aprovação do trabalho;

( ) Pela aprovação do trabalho, com revisão de forma, indicando o prazo de até 30 dias para apresentação definitiva do trabalho revisado;

( ) Pela reformulação do trabalho, indicando o prazo de (Nº DE MESES) para nova versão;

( ) Pela reprovação do trabalho, conforme as normas vigentes na Universidade de Brasília.

Conforme os Artigos 34, 39 e 40 da Resolução 0080/2021 - CEPE, o(a) candidato(a) não terá o título se não cumprir as exigências acima.

Dra. Lillian Maria Araujo de Rezende Alvares (PPGCINF/UnB)
(PRESIDENTA)

Dr. Marcio de Carvalho Victorino (PPGCINF/UnB)
(MEMBRO TITULAR INTERNO)

Dr. Eduardo Dutra Amadeu Moresi (Universidade Católica de Brasília)
(MEMBRO EXTERNO)

Dr. João Marinonio Enke Carneiro (Escola de Comando e Estado-Maior do Exército)
(MEMBRO EXTERNO)

Dr. Cláudio Gottschalg Duque (PPGCINF/UnB)
(MEMBRO SUPLENTE)

José Ricardo Souza Camelo
(DOUTORANDO)

Documento assinado eletronicamente por **Lillian Maria Araujo de Rezende Alvares**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 01/03/2024, às 13:08, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Eduardo Amadeu Dutra Moresi**, **Usuário Externo**, em 01/03/2024, às 13:26, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Michelli Pereira da Costa**, **Vice-Coordenador(a) da Pós-Graduação da Faculdade de Ciência da Informação**, em 04/03/2024, às 15:21, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **José Ricardo Souza Camelo**, **Usuário Externo**, em 07/03/2024, às 14:01, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Marcio de Carvalho Victorino**, **Professor(a) de Magistério Superior da Faculdade de Ciência da Informação**, em 12/03/2024, às 18:20, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **João Marinonio Enke Carneiro**, **Usuário Externo**, em 02/07/2024, às 10:15, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **10821461** e o código CRC **97A98163**.

Referência: Processo nº 23106.005843/2024-03 SEI nº 10821461

DEDICATÓRIA

Às minhas filhas Helena A. F. Camelo e Clara A. F. Camelo, meus tesouros e as maiores e mais belas responsabilidades que Deus me deu.

AGRADECIMENTOS

Em verdade, essa jornada de estudos foi iniciada em 2002, quando pela primeira vez ingressei no curso de doutorado da Faculdade de Ciência da Informação (FCI), na Universidade de Brasília. À época, fui apresentado à professora Doutora Kira Tarapanoff por seu ex-orientando, o professor Doutor Eduardo Moresi, um amigo de longa data e colega de profissão da turma de engenharia de 1989 do Instituto Militar de Engenharia, que me recomendou a ela como um futuro orientando de doutorado. Fui muito feliz nas avaliações da seleção para a pós-graduação e fui aprovado no processo. A professora Kira Tarapanoff chamou-me para falarmos do ingresso no curso e, num primeiro momento de silêncio, com um leve sorriso no rosto e um gesto de mão indicando minha colocação na seleção, demonstrou sua alegria e, como percebi no seu olhar, seu orgulho com o resultado.

Mas a vida nos reserva acontecimentos que podem fugir em muito às nossas expectativas e forças para com eles lidar e, um ano após iniciada a minha caminhada nos estudos, sobrevieram graves dificuldades de ordem familiar que se acumularam durante o curso e, no terceiro ano e às portas da qualificação, culminaram com meu afastamento para tratamento de saúde e para não mais retornar. Nesse meio-tempo, a professora Kira se desligou da FCI e se mudou para outro estado e acordamos que seria mais prudente eu seguir com outro orientador. Nesse sentido, não posso deixar de citar a professora Dra. Sely Costa, que me recebeu com toda a consideração e confiança como seu orientando, proporcionando-me orientação segura, respeito e amizade a toda prova.

Retornei ao curso como aluno especial 11 anos após meu desligamento e, passado o certame de seleção, fui aprovado para a turma de 2019, tendo o privilégio de ter como nova orientadora, a professora Dra. Lillian Alvares. Por uma feliz coincidência, a professora Lillian foi orientanda da professora Kira Tarapanoff. Outra feliz coincidência, como que um bom agouro para meu retorno ao doutorado, foi o fato de a professora Kira ter ministrado a aula inaugural da minha turma. Ao me encontrar com ela após a palestra, não resisti em repetir o seu gesto de 2002, pois, muito embora eu tivesse tido uma posição mais modesta dentre todos os aprovados, tive a mesma colocação entre os orientados da professora Lillian, lembrando que, diferente da seleção de 2002, cujo resultado era tomado em termos absolutos da colocação geral, na seleção de 2018, os resultados eram relativos a cada linha de pesquisa e por orientador.

Não me atreverei em prosseguir narrando mais desventuras que pareciam insistir em me impedir de concluir o curso mais uma vez. Porém, não há como deixar de mencionar a pandemia de COVID-19, que provocou prejuízos generalizados, tanto psicológicos quanto físicos, além das perdas de vidas, não sendo a minha família exceção. Isso provocou atrasos diversos, além de outras questões pessoais, e tive pouco tempo para qualificação e defesa. Mais uma vez, ter uma orientadora segura e com amor pelo que faz foi decisivo.

Assim, início os agradecimentos pelo professor Moresi, por ter me apresentado à professor Kira e ter viabilizado essa minha caminhada acadêmica no doutorado.

Agradeço à professora Kira por ter confiado em mim, aceitando-me como orientando e tendo desvelado as primeiras trilhas a seguir pela senda da Ciência da Informação. Terreno este, a princípio, que não me era familiar, eu que sou oriundo da engenharia.

Agradeço à professora Sely por ter acedido e confiado em me orientar numa mudança durante o curso, o que normalmente é tomado como temerário, pois há sutilezas de ordem administrativa, diferenças de estilo de orientação, linhas de pesquisa e relação de confiança que podem se somar e tornarem-se críticas e comprometer a conclusão do curso.

Agradeço aos professores doutores Lillian Alvares, Eduardo Moresi, Marcio Victorino e Enke Carneiro, integrantes da banca de defesa de doutorado, que avaliaram meu trabalho e me arguiram durante a defesa. Graças às avaliações, contribuições e aperfeiçoamentos sugeridos por esses professores, o trabalho pode tomar sua forma final, de maneira adequada aos padrões científicos e de contribuição para a Ciência da Informação.

Agradeço de modo muito especial à professora Lillian, que me acompanhou desde aluno especial, orientando-me com segurança e domínio de conteúdo, o que conquistou meu respeito, inspirou-me e me ajudou em momentos difíceis e decisivos desse caminho.

Para concluir esses agradecimentos com a devida justiça e fidelidade à verdade, não posso esquecer que somos mais que matéria e mente. Lembrando que isso foi percebido e desde os primórdios do exercício do saber humano, como na vida e morte de Sócrates, nas teorias das formas e das reminiscências de Platão, no primeiro motor imóvel de Aristóteles, nos aperfeiçoamentos que esses colossos receberam de Agostinho e Tomás de Aquino, isso apenas para citar alguns dos principais alicerces e pavimentos ocidentais que prepararam para o estabelecimento do conhecimento científico que seria formalizado depois.

Assim, agradeço a Deus por me conceder e nutrir duas potências da alma tão fundamentais à vida, e, em particular, a esse estudo de doutorado, e assim poder desenvolvê-lo: a inteligência e a força de vontade.

Ao agradecer a Deus por eu poder prover uma pequena contribuição à ciência, vem-me o desejo de citar o que pode ter sido uma das primeiras orientações da aplicação do método científico dada por Ele mesmo, por meio de Jesus (independente se o leitor o toma “apenas” por um homem que fez com que o mundo nunca mais fosse o mesmo ou se pelo próprio *Logos* encarnado). Essa aplicação das etapas básicas do método científico se vê em Mateus, capítulo 11, versículo 3, em que os discípulos de João Batista vão até Jesus e fazem o seguinte questionamento: “Sois vós aquele que deve vir, ou devemos esperar por outro?”. No que Jesus responde: “Ide e contai a João o que ouvistes e o que vistes: os cegos veem, os coxos andam, os leprosos são limpos, os surdos ouvem, os mortos ressuscitam, o Evangelho é anunciado aos pobres...”. Ou seja, Jesus, ao ser questionado, orienta os discípulos de João a observarem os fatos e testemunhos dos fenômenos ocorridos, tanto na sua frequência quanto na sua repetição. Podendo, assim, confrontá-los com as escrituras e responder o questionamento de João, que, em si, continha uma hipótese a ser confirmada ou refutada.

Se você conhecer o inimigo e a si próprio, não haverá dúvida quanto à vitória. Se você conhecer os Céus e conhecer a Terra, sua vitória será completa.

(Sun Tzu, A Arte da Guerra, Cap. 10).

RESUMO

Os ambientes modernos onde as organizações se desenvolvem e evoluem são complexos e estão em constantes mudanças. Para fazer frente as essas mudanças, as organizações devem aprender e evoluir com base no conhecimento, materializando esse aprendizado por meio das ações organizacionais para interagir com o ambiente e dele captar sinais de relevância, cuja assimilação e conscientização renovam o processo de aprendizado e ação. Para potencializar o efeito dessas ações, pode-se lançar mão da teoria sobre o ciclo do conhecimento organizacional, tendo por base três processos que se alternam e influenciam mutuamente: a formação de significado, a criação de conhecimento e a tomada de decisão. Observando-se essas ações no campo da defesa nacional no espaço cibernético, percebe-se a necessidade de aprendizado para as organizações atuantes nesse campo. No entanto, ações no espaço cibernético provocam miríades de efeitos intermediários dos quais a organização deve ter meios de acompanhar, o que demanda uma série de sensores tecnológicos, mas que, em último grau, demandam percepções, compreensão e projeções para decisão de indivíduos humanos, ou seja, consciência situacional em defesa cibernética. Nesse sentido, a presente pesquisa buscou desenvolver um *framework* estratégico de necessidades informacionais que, a partir do ciclo do conhecimento organizacional e de modelos de consciência situacional pudesse dar suporte a comandantes, gerentes ou coordenadores de operações de defesa cibernética na concepção desses processos de modo a potencializar o exercício de consciência situacional de defesa cibernética. Para tal, a pesquisa seguiu um caráter de pesquisa aplicada, fazendo uso de métodos dedutivos, técnicas de pesquisa bibliográfica e documental e observação participante do tipo natural. Para aferir a pertinência do *framework* desenvolvido durante o estudo, foi lançado mão de um conjunto de registros pertencentes ao Ministério da Defesa, mais especificamente ao Exército Brasileiro, contendo 477 Lições Aprendidas (LA) e aproximadamente 500 itens de Análise Pós-Ação (APA), referentes às operações cibernéticas ocorridas no período entre 2012 e 2016. A pesquisa concluiu que: (i) a partir de *frameworks* de segurança e defesa cibernética é possível organizar categorias de necessidades informacionais no campo da defesa cibernética a serem desenvolvidas em um ambiente organizacional por meio do ciclo do conhecimento organizacional; (ii) o estabelecimento de necessidades informacionais de defesa cibernética com base no ciclo de conhecimento organizacional pode potencializar metodicamente a capacidade e o exercício da consciência situacional de defesa cibernética na cadeia de decisores envolvidos nos processos para realização de ações de defesa cibernética; (iii) é possível, no campo da defesa cibernética, a partir de instrumentos de conhecimento explícito do tipo *framework*, irradiar aspectos de conhecimentos tácito e cultural numa organização de defesa cibernética, provocando aprendizados que se reflitam na capacidade de consciência situacional de defesa cibernética dos diversos decisores de cada nível da organização, em níveis diversos até o seu comandante.

Palavras-chave: conhecimento organizacional, consciência situacional, defesa cibernética, *framework*.

ABSTRACT

The modern environments which organizations develop and evolve are complex and constantly changing. To face these changes, organizations must learn and evolve based on knowledge, materializing this learning through organizational actions to interact with the environment and, from it, capture signs of relevance, whose assimilation and awareness renew the process of learning and action. To enhance the impact of these actions, one can draw upon the theory of the organizational knowledge cycle, which is based on three interrelated processes: sense-making, knowledge creating, and decision-making. Observing these actions in the field of national defense in cyberspace, one can see the need for learning for organizations working in this field. However, actions in cyber space cause myriads of intermediate effects that the organization must have the means to monitor, which demands a series of technological sensors, but which, ultimately, demand perceptions, understanding and projections for decision by human individuals, i.e. situational awareness in cyber defense. In this context, the present research aimed to develop a strategic framework for informational needs that, based on the organizational knowledge cycle and models of situational awareness, could provide support to commanders, managers, or coordinators of cyber defense operations in designing these processes in order to enhance the cyber defense situational awareness. To this end, the research followed an applied research character, making use of deductive methods, bibliographic and documentary research techniques and natural participant observation. To assess the relevance of the framework developed during the study, a set of records belonging to the Ministry of Defense, more specifically the Brazilian Army, was used, containing 477 Lessons Learned (LL) and approximately 500 Post-Action Analysis (APA) (PAA) items, referring to cyber operations that took place between 2012 and 2016. The research concluded that: (i) based on cyber security and defense frameworks, it is possible to organize categories of informational needs in the field of cyber defense to be developed in an organizational environment by middle of through the organizational knowledge cycle; (ii) the establishment of cyber defense informational needs based on the organizational knowledge cycle can methodically enhance the capacity and exercise of cyber defense situational awareness in the chain of decision makers involved in the processes for carrying out cyber defense actions; (iii) it is possible, in the field of cyber defense, using explicit knowledge instruments of the framework type, to radiate aspects of tacit and cultural knowledge in a cyber defense organization, causing learning that is reflected in the cyber defense situational awareness capacity of the several decision-makers at each level of the organization, at different levels up to its commander.

Keywords: organizational knowledge, situational awareness, cyber defense, *framework*.

LISTA DE ILUSTRAÇÕES

LISTAS DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BSI	*British Standards Institution*
C2	Comando e Controle
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Cert/CC	*Computer Emergency Response Team/Coordination Center*
CI	Ciência da Informação
CIS	*Center for Internet Security*
COBIT	*Control Objectives for Information and Related Technologies*
CS	*Consciência Cibernética*
CSF	*Cybersecurity Framework*
CSIRT	*Computer Security Incident Response Teams*
CTI	*Cyber Threat Intelligence*
DC	Defesa Cibernética
DP	Dados Pessoais
END	Estratégia Nacional de Defesa
ESG	Escola Superior de Guerra
FIFA	*Fédération Internationale de Football Association*
FIRST	*Forum of Incident Response and Security Teams*
GEOINT	*Geospatial Intelligence*
GSIPR	Gabinete de Segurança Institucional. Presidência da República
HUMINT	*Human intelligence*
IEC	*International Electrotechnical Commission*
IOA	*Indicator of Attack*
IOC	*Indicators of Compromise*
ISA	*International Society of Automation*
ISO	*International Organization for Standardization*

JO	*Jogos Olímpicos*
JPCERT/CC	*Japan Computer Emergency Response Team Coordination Center*
MD	Ministério da Defesa
MITRE ATT&CK	*Adversarial Tactics, Techniques, and Common Knowledge*
NBR	Norma técnica brasileira
NIP-CS-DC	Necessidades informacionais primordiais para consciência situacional de defesa cibernética
NIST	*National Institute of Standards and Technology*
OODA	*Observe, Orient, Decide, Act*
OSINT	*Open source intelligence*
OT	*Operational technology*
OWASP	*Open Web Application Security Project*
PDCA	*Plan-Do-Check-Act*
PMS	*Problemas Militares Simulados*
SANS	*SysAdmin, Audit, Network, and Security*
SIGINT	*Signals Intelligence*
TIC	Tecnologia da Informação e Comunicação
US-CERT	*United States Computer Emergency Readiness Team*

SUMÁRIO

1. INTRODUÇÃO

1.1. CONTEXTUALIZAÇÃO

Em 2008, por meio da publicação da Estratégia Nacional de Defesa (END) (Brasil, 2008), o Brasil estabeleceu três setores de maior prioridade para a Defesa Nacional. Dentre eles, há um ramo do combate moderno que tem evoluído rapidamente nas últimas décadas, o qual foi designado na END como Setor Cibernético. Essa escolha seguiu uma tendência mundial de reconhecer que é essencial à soberania de uma nação tanto defender seus sistemas de informação no espaço cibernético, quanto desenvolver capacidades de atuar nesse mesmo espaço contra eventuais agressores.

Desde meados dos anos 90, uma série de eventos vêm se sucedendo pelo mundo nos quais o espaço cibernético é utilizado para ações criminosas, terroristas, de ativismo, de espionagem e de guerra. Um alvo dessas ações que tem merecido especial atenção são as chamadas infraestruturas críticas. Essas infraestruturas são compostas por instalações e sistemas cujo comprometimento pode atingir severamente um país. Dentre as categorias que abrangem, pode-se citar como exemplos as telecomunicações, os sistemas de energia elétrica e nuclear, os serviços de saúde, os sistemas financeiros, dentre outras. Por meio de ataques cibernéticos, é possível comprometer os sistemas de informação que suportam essas infraestruturas e causar impactos de toda ordem e com potencial destrutivo muito significativo a um país e, como consequência, comprometer sua capacidade de defesa (Brasil, 2009).

O Setor Cibernético não é explicitamente definido pela Estratégia Nacional de Defesa, mas, da sua leitura, é possível depreender que é um conjunto de elementos heterogêneos que abrange sistemas computacionais, as redes utilizadas para interligá-los e todos os processos, tecnologias, metodologias gerenciais, pessoal, normas técnicas, legislação e desenvolvimentos científicos envolvidos para processar, armazenar e transmitir os dados digitais que compõem as informações importantes para o país. O Setor Cibernético foi priorizado pela END para que as ações decorrentes viabilizassem a criação de mecanismos de proteção dos dados digitais considerados críticos para o Brasil e, ao mesmo tempo, fossem desenvolvidos instrumentos de

resguardo da soberania nacional que complementassem os mecanismos tradicionais da Defesa da Nacional.

A priorização desse setor na Defesa Nacional é corroborada pelas lições aprendidas no âmbito internacional dos embates militares. Nesses conflitos, o uso da cibernética possibilita inúmeras formas de degradação ou destruição de sistemas essenciais a um país, como se viu no conflito Rússia e Geórgia, em 2008, quando a capacidade de reação da Geórgia à invasão do seu território pelos russos foi comprometida por um massivo ataque cibernético aos seus sistemas computacionais (Clarke e Knake, 2010, p. 19).

Em 2012, com a publicação do Livro Branco de Defesa (Brasil, 2012a, p.22), ficou claro na conceituação de Defesa Nacional que a sua abrangência engloba tanto a atuação de civis quanto de militares, ainda que, conforme definido na Política de Defesa Nacional (Brasil, 2012b, p.15), a aplicação do conceito seja de ênfase no campo militar. Quando estendido ao domínio cibernético, a Defesa Nacional leva ao extremo a necessidade da ação colaborativa entre a segurança cibernética, desenvolvida pelo pessoal civil e a defesa cibernética, desenvolvida pelos militares, conforme distinção proposta por Mandarino Jr. (2010, p.120). Neste ponto, cabe ressaltar as definições existentes para segurança e defesa cibernéticas.

Entende-se por segurança cibernética, conforme consta na Portaria 45 GSIPR:

> Art. 2º Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (Brasil, 2009, p.2).

Sobre a defesa cibernética, conforme a Doutrina Militar de Defesa Cibernética:

> 2.2.5 Defesa Cibernética - 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 as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (Brasil, 2014, p.18).

Os trabalhos desenvolvidos no âmbito do Ministério da Defesa nos últimos 10 anos para a construção do Setor Cibernético proporcionaram uma série de experiências vividas nas operações militares que ocorreram no período. Dentre essas missões, estão as operações de defesa e segurança cibernética dos grandes eventos ocorridos no Brasil entre 2012 e 2016.

Para cada uma dessas operações, um destacamento de defesa e segurança cibernética foi organizado pelo Exército Brasileiro e, em cooperação com as demais Forças Armadas, realizaram uma ação conjunta com diversos órgãos governamentais e privados com atuação destacada nas áreas de segurança cibernética, inteligência e policial para proteger os ativos de informação que suportavam os eventos em si ou organizações com vínculos importantes com esses eventos. Os grandes eventos foram: a Conferência das Nações Unidas sobre o Desenvolvimento Sustentável, Rio + 20 (Vianna, 2013, p.127); a Copa das Confederações FIFA 2013 (Camelo e Carneiro, 2014, p.149); Copa do Mundo FIFA 2014; os Jogos Olímpicos e Paralímpicos 2016.

Operações de defesa e segurança cibernética, tais como as ocorridas nos grandes eventos, são exemplos de operações que envolvem grande número de informações a serem acompanhadas, as quais devem ser consolidadas na consciência situacional que o comandante da operação deve formar sobre o que ocorre no espaço cibernético de interesse da missão. Para evitar ambiguidades sobre a expressão “consciência situacional”, uma vez que existem diversas definições relacionadas ao termo, a noção central que se adota neste trabalho é a de “saber o que está ocorrendo”, traduzida em três estágios, quais sejam, a percepção de determinados elementos em um dado ambiente, a compreensão do seu significado e a projeção da sua condição no futuro (Endsley, 1995, p.35).

Cabe ressaltar que, em qualquer operação que demande a tomada de consciência situacional, o número de dados a serem processados é enorme, difícil de abranger e consolidar em termos humanamente gerenciáveis. Nos âmbitos tanto da defesa quanto da segurança cibernética, o problema se multiplica por ordens de magnitude, uma vez que os sistemas de informação processam dados críticos em quantidades e velocidades impossíveis para qualquer ser humano lidar. Em consequência, percebe-se que tais dados advindos das fontes envolvidas necessitam ser processados em diversos níveis

até que as informações derivadas possam ser reconhecidas, compreendidas e usadas pelos comandantes ou gestores que estiverem à frente do processo de tomada de consciência situacional de defesa cibernética ou de segurança cibernética.

Para tornar viável este processo de tomada de consciência situacional, é imprescindível ter disponíveis as informações adequadas, saber percebê-las como relevantes, ter a capacidade de recuperá-las, processá-las e utilizá-las para a devida apreensão do que ocorre e a gerar os conhecimentos decorrentes. Nesse sentido, apresenta-se como promissor e pertinente tomar as abordagens providas pela Ciência da Informação relacionadas à gestão da informação e do conhecimento como elementos que possam suportar ou, ao menos, contribuir com o suporte do processo de tomada de consciência situacional como tema de estudo.

Além disso, de modo a facilitar a junção do tema central de estudo, a consciência situacional em defesa e segurança cibernética, ao campo da Defesa Nacional, é recomendável lançar mão de elementos das Ciências Militares que estejam simultaneamente relacionados à gestão da informação e do conhecimento e à consciência situacional. Tal área é conhecida no âmbito dos estudos da doutrina militar como Comando e Controle (C2).

1.2. PROBLEMA DE PESQUISA

A consciência situacional é um tema que por força da necessidade sempre mereceu atenção nos estudos relacionados às ciências militares e, mais recentemente, no campo das disciplinas com interfaces com os estudos organizacionais. Seu desenvolvimento se dá nos ambientes informacionais do campo de batalha ou na gestão dos negócios das organizações. No entanto, a dependência atual que os ambientes informacionais têm da tecnologia da informação implica na necessidade de lidar com uma enorme quantidade de dados, processados de modos diversos, complexos e em rede.

Sendo a consciência situacional um processo que ocorre na mente humana, a partir da percepção e compreensão do que se passa e a projeção de futuros possíveis e prováveis para tomada de decisão, a consecução desse

processo em um ambiente informacional digital requer inúmeras e sucessivas integrações de dados, o que, independentemente do tipo de tecnologia empregada para suportá-las, requer métodos para otimizar todos os estágios da tomada de consciência situacional e na diminuição da ambiguidade que a complexidade do ambiente cibernético envolve. Logo, surge a necessidade de realização de pesquisas científicas que abordem o tema da consciência situacional sobre defesa e segurança cibernéticas de modo a esclarecer suas características, como se realiza, possíveis limitações, dentre outras possibilidades.

No estudo do conceito da consciência situacional aplicada ao espaço cibernético, Barford, Dacier *et al*.(2010, p. 5-6) apontam que os conhecimentos desenvolvidos até o momento não se mostram amadurecidos em três aspectos de relevância: (i) a existência de uma grande lacuna entre a capacidade das ferramentas que propiciam a consciência situacional cibernética e os modelos mentais do analista de cibernética; (ii) a carência no tratamento da incerteza inerente aos dados nas abordagens existentes sobre consciência situacional cibernética; (iii) os modelos existentes não proporcionam capacidades de aprendizado e cognição necessárias à formação de uma consciência situacional de defesa cibernética plena.

Por outro lado, pela perspectiva de gestão, mais particularmente pelas abordagens com foco na informação e no conhecimento, Choo (1998) realizou estudos de modo a estabelecer referências a respeito da teoria envolvida na definição de uma organização de conhecimento. Na sua pesquisa, Choo descreveu processos envolvidos na potencialização da capacidade dos gestores de administrarem a informação, desde sua percepção no ambiente até a tomada de decisão, o que inevitavelmente implica em um processo de consciência situacional.

Ao mesmo tempo, as práticas consagradas pelo mercado de tecnologias de segurança cibernética, sejam tanto os produtos tecnológicos propriamente ditos quanto as metodologias empregadas na gestão da sua aplicação, são baseadas, em geral, em conhecimentos advindos da prática de seu uso e que são conhecidas como “melhores práticas”. Em geral, essas melhores práticas são consolidadas em normativos ou em conjuntos de regras e recomendações

que tomam um aspecto de quadros de referência conhecidos como *frameworks*. A aplicação metodológica desses *frameworks* visa diminuir os riscos de segurança cibernética no processo de proteção de ambientes digitais, quando o *framework* é voltado para proteção das informações, ou de potencializar os resultados de ataques cibernéticos, quando for voltado para ações cibernéticas usadas para ataque a sistemas informacionais.

Na grande maioria das situações de seu emprego, esses *frameworks* são voltados para a segurança e geram metodologias de gestão de segurança cibernética nas organizações por meio de políticas e métodos de aplicação de tecnologia personalizados para o negócio da organização, além de gerar modelos mentais para a tarefa do pessoal empregado na gestão operacional desse setor no ambiente organizacional. Processo análogo ocorre em organizações que abranjam no rol de suas atividades a possibilidade de realização de ataques cibernéticos, os quais devem seguir *frameworks* complexos. Exemplos dessas organizações são as instituições militares, agências de inteligência de estado ou empresas especializadas na prática de testes de invasão em redes computacionais.

Desse modo, tanto no aspecto da segurança cibernética quanto da segurança ativa, expressão esta usada como alternativa à expressão ataque cibernético, o emprego de *frameworks* constitui um exemplo de aplicação tanto da teoria envolvida na definição de uma organização de conhecimento quanto o emprego de elementos-chave nas fases do processo de consciência situacional, conforme descrito por Endsley (1995), como se pretende esclarecer em detalhes por meio da revisão de literatura e do referencial teórico desta tese.

Considerando as possíveis lacunas de conhecimento a serem exploradas nas pesquisas sobre consciência situacional em defesa cibernética, tomando por elemento potencializador as teorias voltadas para organizações do conhecimento, além de fazer uso das ferramentas de *framework* de segurança cibernética e defesa ativa, esta pesquisa tem como elemento central a seguinte questão:

“Como estruturar um framework que, baseado no ciclo de conhecimento organizacional, forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da

consciência situacional em defesa cibernética no contexto da Defesa Nacional Brasileira no seu nível estratégico?"

A escolha de aplicar o foco do *framework* nas necessidades informacionais para a consciência situacional na pesquisa se deu pelo fato de que a consciência situacional propriamente dita é formada em cada indivíduo após uma série de processos cognitivos, emocionais e situacionais, cujo mapeamento completo fugiria do escopo desta pesquisa. Por outro lado, ao observar as necessidades informacionais primordiais, torna-se viável mapear com razoável abrangência elementos essenciais para dar início à formação de consciência situacional de defesa cibernética de modo a direcioná-la com maior probabilidade de sucesso.

A especificidade da adjetivação **primordial** advém do fato de que a tomada de consciência situacional, além de ser individual, depende de cada operação de defesa cibernética específica ou do contexto particular empresarial em que incidentes de segurança de relevância ocorrem e são acompanhados pelo gestor. Em consequência, esse caráter de primordialidade se torna necessário para indicar um ponto de partida e não chegada.

A restrição do questionamento no nível estratégico se faz necessário nesta pesquisa de modo a torná-la viável no que diz respeito ao cronograma a ser aplicado, acesso às fontes de dados, bem como atender à expectativa de que, uma vez estabelecida uma referência de nível superior, outros desdobramentos do mesmo tema, nos níveis tático e operacional, sejam facilitados em pesquisas futuras.

1.3. OBJETIVOS

1.3.1. Objetivo geral

Propor um *framework*, baseado no ciclo de conhecimento organizacional de Choo (1998, p. 240), que forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética, conforme definida por Endsley (1995, p.35), no contexto da Defesa Nacional Brasileira no seu nível estratégico.

1.3.2. Objetivos específicos

a) Identificar *frameworks* consagrados internacionalmente para segurança cibernética, segurança da informação e de ataque cibernético que serão úteis à pesquisa.

b) Identificar e aplicar critérios para seleção de elementos presentes nos *frameworks* escolhidos que sejam compatíveis com os aspectos do ciclo de gestão do conhecimento de Choo (1998, p. 240).

c) Identificar e aplicar critérios para relacionar os elementos de *frameworks* selecionados em relação ao ciclo de gestão do conhecimento de Choo (1998, p. 240) com os estágios de consciência situacional de Endsley (1995, p. 35) para primeira consolidação do *framework* a ser produzido na pesquisa.

d) Aplicar o *framework* consolidado nas documentações regulatórias, doutrinárias do Setor Cibernético da Defesa brasileira, assim como nos planejamentos das operações de defesa cibernética e respectivas Linhas de Ação (LA) e Análise Pós-Ação (APA) ocorridas no período de 2012 a 2016 para identificar as necessidades informacionais de cada evento ocorrido no período.

e) Discutir a pertinência do *framework* proposto por meio do relacionamento entre as necessidades informacionais primordiais de defesa cibernética e os registros das principais categorias de incidentes ocorridos nos grandes eventos do período estudado.

1.4. JUSTIFICATIVA

A conexão desta proposta de pesquisa com a Ciência da Informação (CI) tem pelo menos três pontos de articulação. O primeiro se baseia no fato de que a pergunta central da pesquisa aborda diretamente de necessidade informacionais e de gestão do conhecimento, elementos bem determinados no estudo da Ciência da Informação.

O segundo ponto se refere à consciência situacional, a qual está inserida no campo das ciências cognitivas, também relacionado à Ciência da Informação (Robredo, 2003, p. 148).

Por fim, o terceiro ponto, composto pela defesa e pela segurança cibernética, as quais possuem como principal alicerce a segurança da informação, área definitivamente relacionada à CI (Robredo, 2003, p. 150). Além

disso, o campo em que se desenrolam os processos de defesa e segurança abordados, ou seja, a cibernética, também é tema de estudo da Ciência da Informação (Robredo, 2003, p. 148).

Além dos fatores enunciados para conexão à Ciência da Informação, esta pesquisa justificou-se pelas contribuições dadas ao conhecimento científico por meio: (i) do uso do ciclo de conhecimento organizacional de Choo (1998) numa nova perspectiva como instrumento de sedimentação e aperfeiçoamento das capacidades de tomada de consciência situacional de comandantes e gerentes de ambientes de tecnologia da informação ligados à defesa cibernética; (ii) do uso do modelo de Ensdley (1995) de modo personalizado tanto ao ciclo de conhecimento organizacional quanto aos *frameworks* de melhores práticas de segurança e defesa cibernética; (iii) de potencialmente viabilizar avanços de doutrina no contexto da Defesa Nacional brasileira.

1.5. ESTRUTURA DO TRABALHO

Esta tese de doutorado está estruturada em sete capítulos, ordenados da seguinte forma: capítulo1, Introdução; capítulo 2, Revisão de Literatura; capítulo 3, Referencial Teórico; capítulo 4, Metodologia; capítulo 5, Resultados; capítulo 6, Discussão dos Resultados; capítulo 7, Conclusões.

2. REVISÃO DE LITERATURA

2.1. CONHECIMENTO ORGANIZACIONAL

Neste tópico, são descritas as forças que se conjugam para a formação do conhecimento organizacional por meio do uso e do enriquecimento da informação no ambiente de trabalho, tendo por base o ciclo de conhecimento organizacional proposto por Choo (1998, p. 240).

2.1.1. Organizações do conhecimento

As organizações atuais, das mais simples às mais complexas, não podem prescindir do uso da informação estratégica para sua sobrevivência. Segundo Choo (1998, p.1), tendo por base as teorias organizacionais, há três arenas nas quais a organização deve lidar com a informação para se adaptar e crescer.

A primeira arena é aquela na qual a organização usa a informação para reconhecer o sentido das mudanças do ambiente externo. Em consequência, as corporações, ao observar esse ambiente, podem selecionar o que é relevante, interpretar esses sinais e gerar respostas adequadas conforme seus objetivos. Em curto prazo, o uso da informação aprimora a consciência dos membros da organização sobre o que ela é e o que faz, assim como, a longo prazo, esse uso propicia maiores chances de a instituição prosperar e sobreviver (Choo, 1998, p.2).

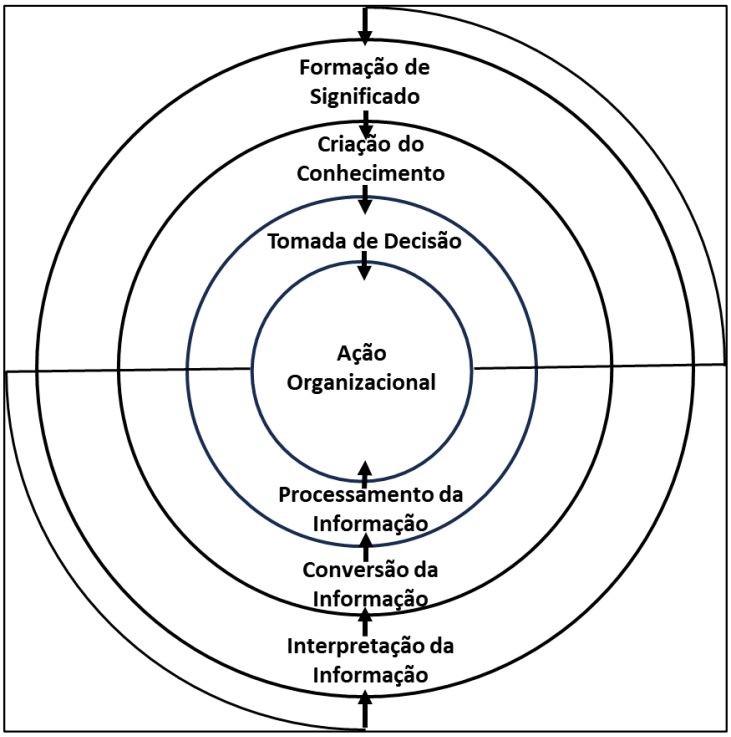
A segunda arena está relacionada ao processo de geração de novos conhecimentos a partir do processamento da informação e por meio do aprendizado (Choo, 1998, p.2). Nessa arena, os membros da organização devem estar sensibilizados para, sistematicamente, localizar, compartilhar, revisar e reintegrar o conhecimento entre si, e, guiados pelos objetivos da organização, promoverem sua evolução.

Na terceira arena, o foco está na tomada de decisão por meio do uso estratégico da informação guiada pelos objetivos institucionais. Essa arena tem por uma das suas características a tensão entre o processo ideal de tomada de

decisão, no qual se faz uso da racionalidade e de técnicas de escolha da melhor estratégia, e os diversos elementos subjetivos dos integrantes da instituição, os quais podem envolver interesses particulares ou de grupos, barganhas, lacunas de informações, dentre outros (Choo, 1998, p.2).

Essas três arenas são designadas, respectivamente, por três aspectos de uso da informação, quais sejam, formação de significado (*sensemaking*), criação do conhecimento (*knowledge creation*) e tomada de decisão (*decision making*). Essas arenas devem ser consideradas como processos que interagem mutuamente (Choo, 1998, p.3). Essa interação pode ser visualizada por meio da Figura 1.

Figura 1- A organização do conhecimento



Fonte: Choo (1998, p. 4), traduzido para o português

Na Figura 1, a formação de significado, a criação do conhecimento e a tomada de decisão representam três camadas concêntricas de comportamentos informacionais, sendo cada camada interna a saída resultante da camada imediatamente exterior a ela. O fluxo da informação segue do exterior para o centro dos círculos de modo a viabilizar a ação organizacional.

O fluxo representado na Figura 1 se desenvolve com a percepção da informação relevante, que, ao ser interpretada, viabiliza a construção social do

significado, sendo este processo sucedido pelo processamento do conhecimento que, inicialmente estando na mente dos integrantes da organização, deve ser amadurecido, compartilhado e reassimilado para que se alcance algum grau de inovação e, por fim, seja viável o uso da informação por meio do seu tratamento e consequente concretização da ação organizacional. A partir desse ponto, há uma realimentação da experiência, levando à organização a se adaptar e gerar um novo ciclo.

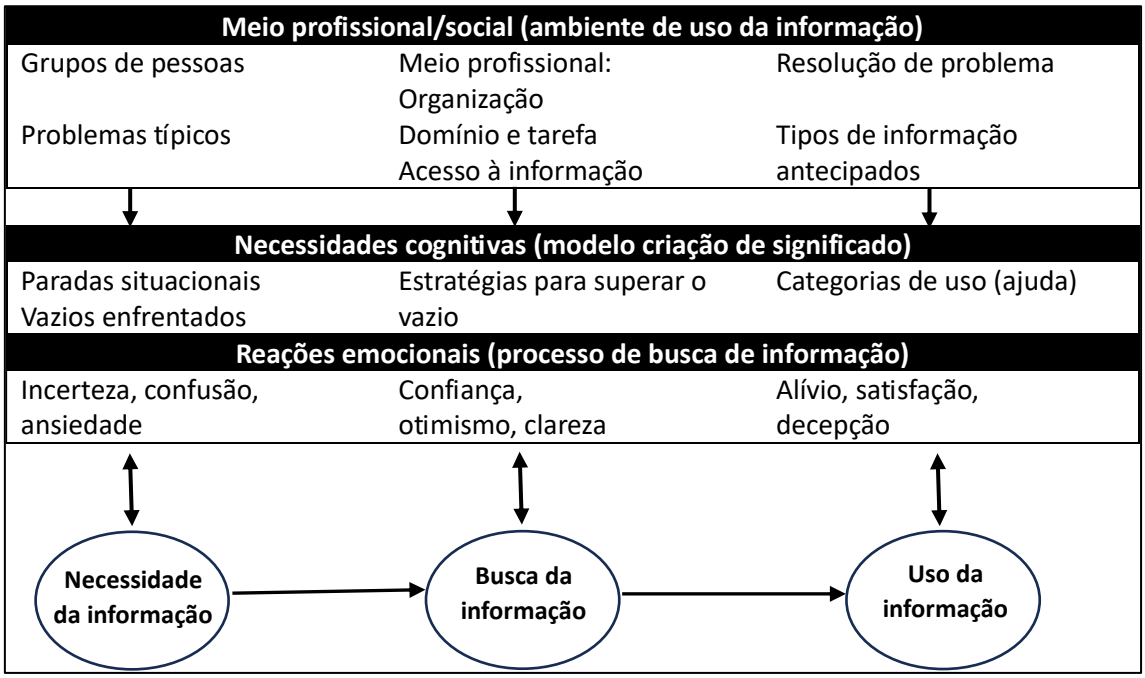
De modo a pavimentar o terreno para apresentação do seu modelo de ciclo de conhecimento organizacional, Choo realizou um levantamento de um grande conjunto de pesquisas sobre necessidades e uso de informação. Entre as fontes utilizadas, está o *Annual Review of Information Science and Technology* (Choo, 1998, p. 32). Dentre os achados da análise desse conjunto de pesquisa, foi constatado o surgimento do que Choo se refere como "elementos definidores de uma análise dos usos e necessidades da informação". Em consequência, afirma o pesquisador, um modelo de uso da informação deve englobar a totalidade da experiência humana: os pensamentos, sentimentos, ações e o ambiente onde eles se manifestam (Choo, 1998, p.40). A partir desses elementos, Choo desenvolve um modelo de busca e uso da informação e, a partir dele, examina cada umas das arenas reconhecidas para uso da informação em um ambiente organizacional.

O modelo de busca e uso da informação se alicerça em três categorias fundamentais: necessidades cognitivas, reações emocionais e ambiente de uso da informação. Os dois primeiros constituem um tipo de ambiente de processamento da informação interno ao indivíduo, enquanto o terceiro elemento constitui o ambiente externo às pessoas, onde a informação é usada (Choo, p.40).

Para a montagem do modelo, foi pressuposto o seguinte: para que um indivíduo se motive e aja na direção da busca e uso da informação, deve haver um evento que deflagra um conjunto de necessidades informacionais. Em suma, um processo de busca e uso da informação possui três etapas bem definidas por comportamentos informacionais, quais sejam: (i) determinação das necessidades informacionais; (ii) busca das informações; (iii) uso da informação. Além disso, o desenrolar de cada comportamento informacional do modelo deve

ser analisado e à luz de cada uma de três categorias, quais sejam, necessidades cognitivas, reações emocionais e ambiente de uso da informação. Esta concepção está representada na Figura 2 e tem sua origem em um trabalho de Taylor (1991).

Figura 2 - Modelo geral de busca e uso da informação



Fonte: Taylor (1991), traduzido para o português.

A partir do modelo geral de uso da informação e fazendo uso dos comportamentos informacionais de referência e dos estágios emocionais, cognitivos e ambientais, é possível analisar cada uma das arenas de uso da informação em um ambiente organizacional, ou seja, formação de significado (Choo, 1998, p.65), criação do conhecimento (Choo, 1998, p. 105) e tomada de decisão (Choo, 1989, p. 155).

2.1.2. Formação de significado (*sense making*)

Na arena de formação de significado, os membros da organização, uma vez submetidos às mensagens do ambiente, devem ser capazes de reduzir as ambiguidades a elas associadas e gerar significado que seja útil do ponto de vista coletivo e, a partir daí viabilizar ações comuns e possivelmente atuações organizacionais. Os processos básicos da formação de significado são (Choo,

1998, p.73): (i) captação (*enactment*); (ii) seleção (*selection*); (iii) retenção (*retention*).

O processo de captação é realizado a partir de uma modificação no fluxo de acontecimentos usuais. Essas mudanças no fluxo informacional são percebidas e ações são realizadas no ambiente observado, podendo resultar delas a extração de dados de relevância para análise mais detalhada, com a possibilidade desses dados sofrerem algum nível de categorização. Além dessa extração, uma intervenção para fins de modificação no ambiente pode também ocorrer.

O processo de seleção tenta responder à pergunta “o que está acontecendo aqui?” por meio da superposição de estruturas de relacionamentos consideradas plausíveis entre os dados coletados no processo de captação. (Choo, 1998, p.6). Essas estruturas, por sua vez, em geral, já devem ter sido testadas em situações similares e foram consideradas úteis para essa função. O processo de seleção deve considerar o histórico do contexto para apoiar o processo de interpretação dos dados.

O processo de retenção tem por objetivo o armazenamento das saídas do processo de formação de significado para futuros usos. A Figura 3 resume esses processos e escolha, seleção e retenção.

Figura 3 - Formação de significado

	Entradas	Processos	Saídas
Captação(C)	Dados brutos do ambiente	- Isolar os dados brutos - Agir ou criar aspectos do ambiente que serão acompanhados	Dados ambíguos como matéria-prima para a criação de significado
Seleção (S)	- Dados ambíguos oriundos do processo de captação - Interpretações vindas de dados captados que já funcionaram antes	Selecionar e estabelecer significados ou interpretações para os dados ambíguos	Ambiente interpretado ou significativo
Retenção (R)	Ambiente captado no processo de seleção	Armazenar o ambiente determinado como produto da criação de significado bem-sucedida	Captações selecionadas para serem usadas em futuras sequências de CSR

Fonte: Choo (1998, p.73), traduzido para o português.

Partindo do modelo geral de uso da informação, Choo (1998, p.89) relaciona o desenvolvimento da formação de significado com os comportamentos informacionais (necessidades, busca e uso informacionais), o estágio de processamento interno (necessidades cognitivas e reações afetivas) e o estágio de processamento externo da informação (dimensões situacionais). Esse relacionamento está sintetizado na Figura 4.

Figura 4 - Necessidades, busca e uso da informação na formação de significado

	Necessidades de informação	Busca da informação	Uso da informação
Criação de significado	- Necessidades obscuras - "O que está acontecendo aqui?" - "Que interpretação escolher?"	- Sonda o ambiente - Nota informações significativas e confiáveis. - Desenvolve interpretações por meio do discurso verbal	- Reduz, mas não elimina, a ambiguidade. - Constrói consenso ou significados comuns para a ação coletiva.
Necessidades cognitivas	- Redes de referência - Interpretações Plausíveis - Informação para escolher valores, prioridades	- Clareza e qualidade da informação - Recuperação na memória organizacional	- Reduz a ambiguidade - Usa esquemas para processar a informação - Prefere informações que confirmem as expectativas
Reações emocionais	- Interrupções provocam reações emocionais - Emoções positivas e negativas - Incerteza, dúvida, tensão, estresse	- Emoções ajudam a memória - Comunicação não verbal por meios de informação ricos - Estados emocionais	- Tensão entre crenças pessoais e consenso de grupo - Confiança na informação - Percepção de ameaça ou desafio
Dimensões situacionais	- Incerteza ambiental percebida - Problemas mal Estruturados - Objetivos obscuros	- Análise ambiental e intromissão organizacionais como - Acesso à informação: sistemas, estruturas, pessoas, valores, experiências	- Culturas organizacionais como sistemas de significado - Compromisso com ações visíveis - Ambientes captados

Fonte: Choo (1998, p.89), traduzido para o português.

Conforme Weick (1995, p.17), a formação do significado pode ser baseada tanto em crenças quanto ações. No caso da formação do significado baseada em crenças, as pessoas utilizam crenças como elemento aglutinador de informações para análises cada vez mais complexas. Na formação do significado baseada em ações, o núcleo aglutinador de significado são as ações dos indivíduos.

2.1.3. Criação do conhecimento (*knowledge creation*)

Na arena da criação do conhecimento, a organização tem suas capacidades ampliadas por meio do aprendizado dos seus membros, seja esse aprendizado oriundo de processos internos ou de interações pessoais externas.

No âmbito interno, de modo a viabilizar a criação do conhecimento, deve-se promover: (i) o compartilhamento da informação; (ii) as conversões envolvendo o conhecimento tácito; (III) a vivência das experiências viabilizadas pelos novos conhecimentos, tais como em realizações iniciais simplificadas em forma de protótipos; (iv) a migração do conhecimento no âmbito interno da organização (Choo, 1998, p.153).

No âmbito externo, o conhecimento pode advir majoritariamente de duas origens: (i) da monitoração da tecnologia, o que deve contar com a capacidade interna para assimilação dos novos conceitos; (ii) da observação do mercado, processo no qual se busca compreender as necessidades dos usuários.

Cabe ressaltar que os modos de criação de conhecimento internos e externo se consumam numa perspectiva em que sejam considerados: (i) a sua análise em relação aos objetivos da organização; (ii) a apreciação das capacidades centrais da organização; (iii) as avaliações dos potenciais tecnológico e de mercado; (iv) o reconhecimento que inovações operacionais requerem ser suportadas por novos sistemas tanto de informação quanto sociais (Choo, 1998, p.153). Outro destaque de relevância é que as tarefas principais envolvidas na construção do conhecimento, tanto no âmbito interno quanto no âmbito externo, estão presentes nos três comportamentos informacionais de necessidades, busca e uso da informação.

No desenvolvimento de sua teoria, Choo busca sempre analisar cada arena à luz do seu modelo geral da informação. Assim, o pesquisador apresenta o desenvolvimento da criação do conhecimento em relação aos comportamentos informacionais (necessidades, busca e uso da informação) e aos estágios de processamento interno (necessidades cognitivas e reações afetivas) e externo da informação (dimensões situacionais). A Figura 5 apresenta a síntese desses elementos.

Figura 5 - Necessidades, busca e uso da informação na criação do conhecimento

	Necessidades de informação	Busca da informação	Uso da informação
Criação do conhecimento	- Falhas de identidade nas capacidades cognitivas existentes - Critérios para criar e avaliar novos conhecimentos - Informações sobre fontes de conhecimento, capacidades	- Intensa partilha e busca da informação - Ampla gama de fontes e mecanismos de busca da informação	- Movimentação do conhecimento interno - Exploração do conhecimento externo - Uso do conhecimento como processo social
Necessidades cognitivas	- Definição e estruturação do problema - Inovações como sistemas sociais - Localização e nível do conhecimento	- Fronteiras flexíveis para disseminação da informação - Proteção e ampliação das fronteiras - Custo da aderência da informação	- Capacidade de absorção - Diversidade cognitiva - Capacitação combinatória
Reações emocionais	- Incerteza, dúvida, tensão, estresse - Uso da intuição para criar um foco ou tornar uma ideia plausível	- Apego emocional às habilidades pessoais - Informação redundante ou exclusiva - Resistência a ideias novas	- Síndrome do "não-foi-inventado-aqui" - Conhecimento emocional - Atrito criativo, caos criativo
Dimensões situacionais	- Criação *versus* descoberta - Problemas complexos com objetivos amorfos - Situação de novos produtos: tecnologia e fatores mercadológicos	- Políticas de informação - Novos e antigos mercados e tecnologias - Acesso a fontes externas de conhecimento	- Propósito organizacional - Utopia tecnológica - Estágios iniciais do processo de inovação

Fonte: Choo (1998, p.140), traduzido para o português.

Cabe destacar que, no desenvolvimento da teoria sobre organizações do conhecimento, Choo adota a classificação de Boisot (Choo, 1998, p. 111) para conhecimento nas organizações como sendo: (i) tácito; (ii) explícito; (iii) cultural.

O conhecimento tácito é utilizado pelas pessoas para desempenhar suas funções na organização e dar sentido ao seu mundo. O conhecimento explícito é aquele que pode ser comunicado no ambiente organizacional por estar registrado conforme as regras para tal na instituição. O conhecimento cultural é constituído de estruturas afetivas e cognitivas que servem para os membros da

organização se servirem para perceber, explicar, avaliar e induzir mudanças na realidade (Choo, 1998, p.112).

2.1.4. Tomada de decisão

Na arena de tomada de decisão, o processo que envolve os comportamentos de necessidade, busca e uso informacionais levam ao comprometimento com um determinado curso de ações. Essas ações são eventos tão frequentes e fundamentais no ambiente organizacional que Choo (Choo, 1998, p. 204) afirma que organizações são redes de decisões, decisores e tomada de decisão.

O caminho da decisão deve estar orientado aos objetivos institucionais e se manter coerente com as estratégias vigentes. A experiência mostra que os decisores têm de encarar situações complexas e variados graus de incerteza ao lidar com uma questão a decidir, levando-os a identificar as alternativas viáveis, avaliar os possíveis resultados e tendo, ainda, que buscar esclarecer e ordenar preferências (Choo, 1998, p.24).

Em consequência da não trivialidade de tal processo, sua execução tende a ser complexa. No entanto, de modo a viabilizar a decisão em termos humanos, as organizações buscam formas de simplificação e regramento do processo, tomando o cuidado de não comprometer requisitos organizacionais de um modo geral.

Há três paradoxos a serem enfrentados na tomada de decisão. O primeiro advém de valores, uniformidade e consistência adquiridos com o tempo e da aplicação de processos, assim como de regras e premissas que estruturam as sistemáticas de tomada de decisão usadas. Observa-se que esses valores podem provocar um estreitamento ou filtragem indevida de informações vitais aos decisores. O segundo paradoxo advém das lições aprendidas de experiências anteriores que, uma vez se tornando inerentes ao processo decisório, podem provocar empecilhos à inovação. O terceiro paradoxo se relaciona ao fato de existirem fatores não racionais que influenciam as decisões, como coalisões ou barganhas, o que pode comprometer escolhas de alternativas que, em tese, seriam mais meritórias.

De modo análogo ao apresentado em relação às duas arenas anteriores, Choo mantém a uniformidade da abordagem, ao estabelecer os critérios para tomada de decisão, relacionando este processo aos comportamentos informacionais (necessidades, busca e uso informacionais) e aos estágios de processamento interno (necessidades cognitivas e reações afetivas) e externo da informação (dimensões situacionais), conforme se pode ver sintetizado na Figura 6.

Figura 6 - Necessidades, busca e uso da informação na tomada de decisão

	Necessidades de informação	Busca da informação	Uso da informação
Tomada de decisões	- Determinar a estrutura e os limites do problema - Esclarecer preferências e adequação da regra - Informações sobre alternativas, resultados, preferências	- Guiada por princípios heurísticos e hábitos - Busca motivada por problemas - Critérios para uma solução satisfatória	- Limitações no processamento da informação - Estruturado por rotinas e regras - Muitos problemas competem por atenção
Necessidades cognitivas	- Fases do processo decisório: inteligência, criação, escolha, revisão - Identificação e desenvolvimento das necessidades	- Múltiplas regras para gerenciamento das decisões - Alta velocidade na tomada de decisões	- Simplificações e Tendências cognitivas - Processamento seletivo da informação
Reações emocionais	- Estresse devido à complexidade, ao risco, aos múltiplos interesses e aspirações - Fatores emocionais na formulação do problema	- Modelo conflituoso de tomada de decisões: aderência ou mudança não conflituosa. Evitação defensiva, hipervigilância, vigilância	- Pressão para aderir ao pensamento do grupo - Excesso de compromisso em situações de crescimento
Dimensões situacionais	- Decisões programadas e não programadas - Táticas para elaborar problemas	- Tipos de processos decisórios: esporádico, fluido e reprimido - Estrutura, incentivos e acesso à informação	- Regras para lidar com a informação: regras de percurso e regras de filtragem - Absorção da incerteza

Fonte: Choo (1998, p.190), traduzido para o português.

2.1.5. Ciclo do conhecimento organizacional

O conhecimento organizacional, segundo Choo (1998, p. 220), apoia-se nas três arenas de uso da informação, ou seja, formação de significado, criação de conhecimento e tomada de decisão. Ao perfazer seu trajeto por essas arenas, a teoria desenvolvida permite reconhecer que, em cada uma delas, os comportamentos de necessidade, busca e uso informacional são realizados. Por

sua vez, cada um desses comportamentos é realizado sob os aspectos emocionais, cognitivos e situacionais. Essas relações foram sintetizadas para cada arena nas Figuras 4, 5 e 6.

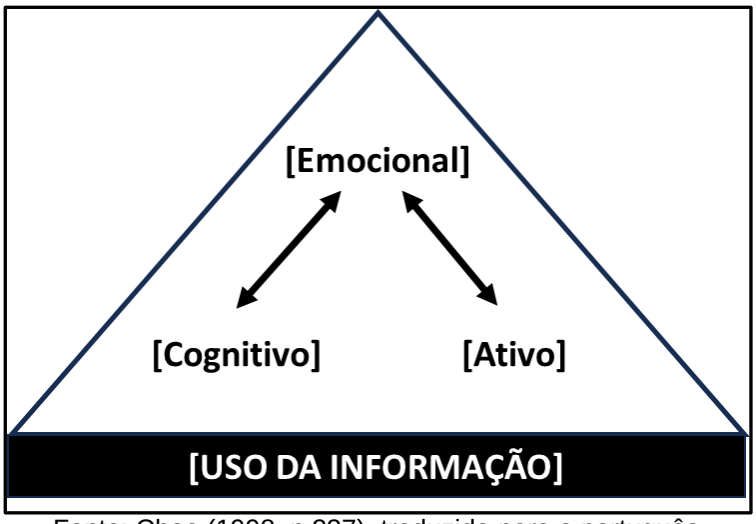
A Figura 7 apresenta uma outra síntese para as três arenas, os comportamentos informacionais e os aspectos simultaneamente. A Figura 8 destaca de modo genérico as Figuras menores retratadas de modo mais específico na quarta coluna da Figura 7.

Figura 7 - Comparação entre formação de significado, criação de conhecimento e tomada de decisão

Modelo	Processo	Modos	Interações / Recursos
Formação de significado	- Mudança no ambiente -> Captação, seleção, retenção -> Interpretações representadas - Olhar para trás: criação de significado retrospectiva	- Processos orientados por crenças - Processos orientados por ações	
Criação do conhecimento	- Lacuna de conhecimento -> Conhecimento tácito, explícito, cultural -> Conversão, construção, conexão do conhecimento -> Novo conhecimento - Observar em muitos níveis: aprender com indivíduos, grupos e organizações de vários níveis	- Conversão do conhecimento - Construção do conhecimento - Conexão do conhecimento	
Tomada de decisões	- Situação de escolha -> Alternativas, resultados, preferências -> Regras, rotinas -> Decisões - Olhar para a frente: visão orientada para o futuro, para os objetivos	- Racional - Processual - Político - Anárquico	

Fonte: Choo (1998, p. 232), traduzido para o português.

Figura 8 - Aspectos afetivos, cognitivos e situacionais no uso da informação



Fonte: Choo (1998, p.237), traduzido para o português.

Para a apresentação do ciclo de conhecimento organizacional, é necessário definir quatro conceitos: teoria da ação organizacional, teoria adotada, teoria em uso e cultura organizacional.

Teoria de ação da organização: segundo Argyris e Shön (1978, apud Choo, 1998, p.220), a teoria de ação de uma organização é aquela que inclui normas para desempenho corporativo, estratégias para cumprimento de normas e pressupostos que mantém unidos normas e estratégias.

Da aplicação do conceito de teoria de ação organizacional, é possível desdobrar dois outros conceitos: **teoria adotada** e **teoria em uso**. A teoria adotada engloba seus organogramas, políticas estabelecidas, descrição de funções e arquivos, os quais a organização projeta para o ambiente externo e seus membros. A teoria em uso abrange conjuntos de regras e pressupostos assumidos pelos integrantes da organização e que pauta seus reais comportamentos. A teoria em uso é de natureza tácita e, em geral, não coincide com a teoria adotada (Choo, 1998, p. 221).

Cultura organizacional: é um conceito que possui diversas definições, mas de modo sintético, pode ser descrito como sendo o aprendizado e a validação de uma série de pressupostos comuns aos integrantes de um ambiente organizacional e que provê um quadro de referência para respostas cognitivas, comportamentais e afetivas. Por meio do uso desse quadro de

referência, os membros da organização podem reconhecer sentido e se adaptar ao ambiente externo, assim como sustentar os relacionamentos internos (Choo, 1998, p.86).

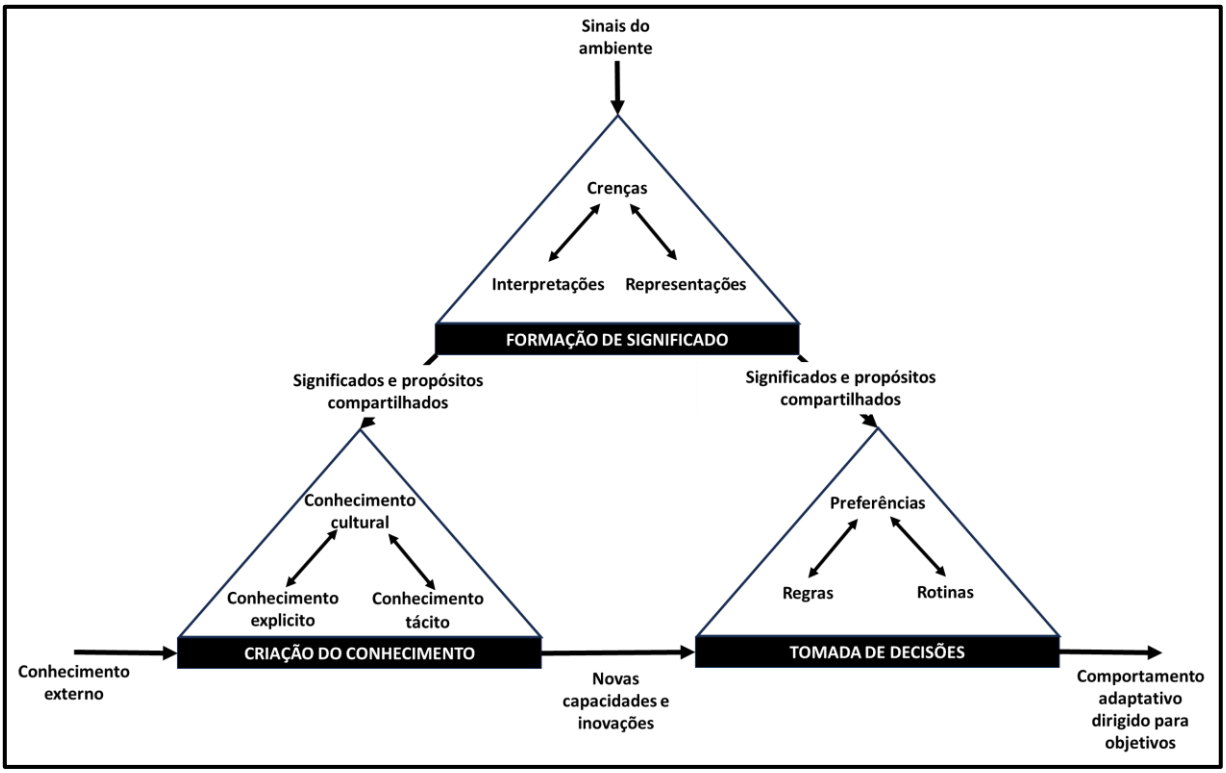
Por fim, neste ponto, é possível apresentar o ciclo do conhecimento organizacional. O ciclo de conhecimento organizacional deve ser interpretado a partir dos sinais do ambiente externo. A informação percorre as três arenas de comportamento informacional, sendo processada internamente em cada arena e gerando resultados que podem seguir as possibilidades de sequenciamento indicadas na Figura 9. Em cada arena, o processamento ocorrido envolve os comportamentos de necessidades, busca e uso da informação, sob a luz dos aspectos cognitivos, emocionais e situacionais (Choo, 1998, p. 241).

A partir da análise da Figura 9 e do esquema da Figura 8, pode-se reconhecer que os elementos internos de cada arena podem ser relacionados a três categorias de elementos pertencentes à constituição de uma organização do conhecimento: cultura organizacional, teoria da ação adotada e teoria da ação em uso.

A cultura organizacional abrange os elementos afetivos (parte superior dos triângulos), ou seja, na arena da formação de significado, tem-se as crenças, na arena da criação do conhecimento, tem-se o conhecimento cultural, e na arena da tomada de decisão se tem as preferências (Choo, 1998, p. 238). A Figura 10 resume essa descrição.

A teoria da organização adotada abrange os elementos cognitivos (parte inferior esquerda de cada triângulo), ou seja, na arena da formação de significado, tem-se as interpretações, na arena da criação do conhecimento, tem-se o conhecimento explícito, e, na arena da tomada de decisão, tem-se as regras (Choo, 1998, p. 239). A Figura 11 representa esses elementos.

Figura 9 - Ciclo do conhecimento organizacional



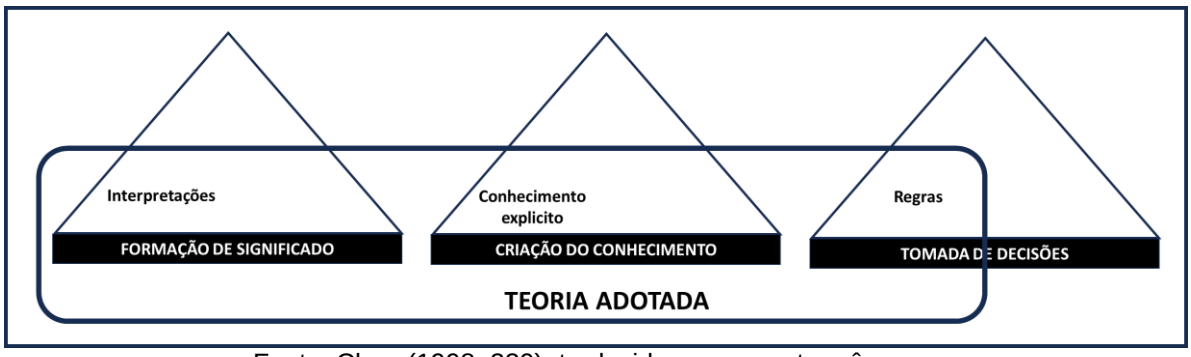
Fonte: Choo (1998, 241), traduzido para o português.

A teoria da organização em uso abrange os elementos situacionais (parte inferior direita de cada triângulo), ou seja, na arena da formação de significado, tem-se os elementos captados, na arena da criação do conhecimento, tem-se o conhecimento tácito, e, na arena da tomada de decisão, tem-se as rotinas (Choo, 1998, p. 239). Na Figura 12 são realçados esses aspectos.

Figura 10 - Cultura organizacional no uso da informação

Fonte: Choo (1998, 238), traduzido para o português.

Figura 11 - Teoria Adotada no uso da informação



Fonte: Choo (1998, 239), traduzido para o português.

Figura 12 - Teoria em Uso no uso da informação

Fonte: Choo (1998, 239), traduzido para o português.

2.2. GESTÃO DA INFORMAÇÃO NAS ESFERAS MILITAR E DE INTELIGÊNCIA

O item 2.1 aborda a teoria do conhecimento organizacional aplicado a uma organização qualquer, o que, por conseguinte, abrange as organizações militares. No entanto, o modelo de Choo não faz parte de modo explícito e sistemático de um processo aplicado no dia a dia das organizações militares. Por outro lado, há um processo de gestão da informação nas Forças Armadas, não só brasileiras, mas de diversos países, que é de uso consagrado que deve ser explanado para fins de suporte a esta pesquisa. Esse processo é conhecido, na sua forma básica e comum a maioria das forças armadas no mundo, por comando e controle (C2).

No exercício da defesa de um estado-nação, a arte da guerra ensina que os conflitos são centrados na ordem e condução do combate. Ao mesmo tempo,

os combates se conjugam em diversas ações denominadas recontros ou engajamentos (batalhas). Conforme se pode constatar na obra de Clausewitz, publicada pela primeira vez em 1832, e traduzidas em diversas línguas e edições desde então, a atividade de ordenar e dirigir os recontros se denominou tática e coordená-los entre si vem a ser a estratégia (CLAUSEWITZ, 1979, p.138). O autor acrescenta que a estratégia “estabelece o plano da guerra e, em função do objetivo em questão, determina uma série de ações que a ele conduzem” (CLAUSEWITZ, 1979, p. 199).

Desse modo, no emprego da estratégia, é fundamental destacar o seu papel coordenador de diversas variantes do combate que atuam de forma conjugada. Por sua vez, esta coordenação é exercida tendo por foco o objetivo maior do conflito e estará sempre se adaptando às mudanças observadas no ambiente das operações.

Tomando por elemento de referência o ciclo de conhecimento organizacional, pode-se estabelecer um paralelo da aplicação desse ciclo com a observação da evolução do teatro de operações com fins de coordenar a aplicação da estratégia e respectivas táticas, por meio de processos que: (i) formem significado a respeito da ação do opositor; (ii) criem conhecimento a respeito das combinações das táticas observadas em execução, sejam elas conhecidas ou não; (iii) levem à tomada de decisão do comandante, por meio das escolhas sobre opções levantadas. As ações decorrentes provocarão novos estímulos ambientais no combate. No meio militar, esse ciclo que gere a informação no campo de batalha, buscando-a e a usando é designado **ciclo de comando e controle**.

2.2.1. Ciclo de Comando e Controle

No âmbito militar, em termos operacionais, ou seja, no que diz respeito ao aspecto central e fim do emprego das Forças Armadas, a gestão da informação ocorre por meio do processo de Comando e Controle (C2). Considerando que a expressão possui diversas interpretações, este estudo adotou a definição doutrinária que guia a Defesa brasileira, o qual consta no Glossário das Forças Armadas:

> COMANDO E CONTROLE - 1. Ciência e arte que trata do funcionamento de uma cadeia de comando. Nesta concepção, envolve, basicamente, três componentes: a autoridade legitimamente investida, apoiada por uma organização, da qual emanam as decisões que materializam o exercício do comando e para onde fluem as informações necessárias ao exercício do controle; a sistemática de um processo decisório que permite a formulação de ordens, estabelece o fluxo de informações e assegura mecanismos destinados à garantia do cumprimento pleno das ordens; e a estrutura, incluindo pessoal, equipamento, doutrina e tecnologia necessários para a autoridade acompanhar o desenvolvimento das operações. 2. Constitui-se no exercício da autoridade e da direção que um comandante tem sobre as forças sob o próprio comando, para o cumprimento da missão designada. Viabiliza a coordenação entre a emissão de ordens e diretrizes e a obtenção de informações sobre a evolução da situação e das ações desencadeadas. 3. Ver SISTEMA DE COMANDO E CONTROLE (Brasil, 2015, p. 65).

...

> SISTEMA DE COMANDO E CONTROLE - Conjunto de instalações, equipamentos, comunicações, doutrina, procedimentos e pessoal essenciais para o comandante planejar, dirigir e controlar as ações de sua organização para que se atinja uma determinada finalidade. Ver COMANDO E CONTROLE (Brasil, 2015, p. 254).

O modo de execução desse ciclo segue padrões doutrinários e variam conforme a força armada que o emprega. Um dos modos mais comuns é o modelo OODA, o qual é explanado no subtítulo 2.2.2.

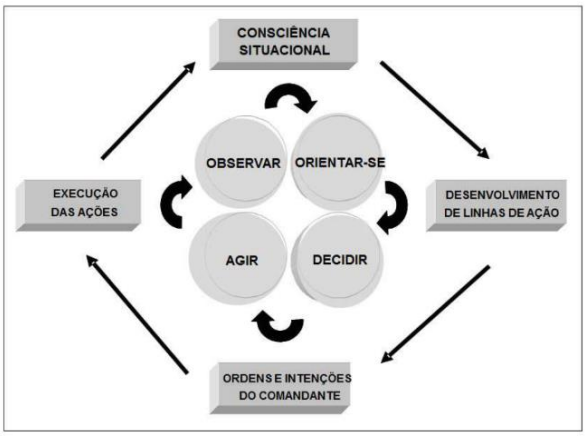
2.2.2. Modelo OODA

O exercício das funções de comando e controle na guerra requer metodologia própria que garanta aos comandantes e seu estado-maior o entendimento e a identificação de todos os processos necessários para realizar o ciclo decisório e superar as incertezas e pressões decorrentes das informações incompletas e do tempo. A rapidez, a complexidade e a quantidade de eventos que ocorrem num teatro de operações, para serem bem gerenciados, necessitam não só das qualidades individuais, da experiência e da intuição, mas, também de metodologia apropriada.

Um dos modelos mais conhecidos e utilizados para realizar o ciclo de Comando e Controle é o modelo OODA (Boyd, 2018). Por intermédio do ciclo OODA, é possível identificar alguns elementos que poderiam ser utilizados para relacionamento com os elementos do ciclo de conhecimento organizacional.

O ciclo de comando e controle OODA é caracterizado pelas fases: observar, orientar, decidir e agir. O ciclo OODA é representado na Figura 13.

Figura 13 - Ciclo de C2 OODA – Observar, Orientar, Decidir e Agir



Fonte: Brasil (2015g, p.2-7).

2.2.2.1. Observar

A fase observar caracteriza-se por perceber o cenário no qual se deseja atuar e se está inserido (Brasil, 2015, p.2-6). Observar consiste em buscar ou coletar dados por meio de diversas fontes. Basicamente, essa coleta é composta pelo levantamento de informações, tais como: o inimigo; o estado das forças amigas; da meteorologia e geografia da área de operações. A ação de observar permite, em primeiro lugar, perceber o que ocorre e, por conseguinte, formar significado sobre os eventos observados.

2.2.2.2. Orientar

Na fase de orientação, as percepções coletadas na fase anterior são consolidadas, compreendidas e analisadas em um contexto global, a fim de delinear um cenário atualizado da situação, com base no qual serão identificadas ameaças possíveis ou concretizadas, os riscos e suas consequências (Brasil, 2015, p.2-6). Orientar é o desenvolvimento de opções das quais, após a

aplicação de processos decisórios, será escolhida aquela que resultará em uma ação.

A orientação será baseada na análise das informações disponíveis, sendo fundamental a sua compreensão e projeção de futuros plausíveis. Assim, a ação de orientar requer a combinação dos significados apreendidos e interpretados de modo que os conhecimentos acumulados da doutrina e as lições aprendidas, que formam parte da teoria adotada, postos à luz do objetivo do combate, possam gerar hipóteses plausíveis sobre as ações a tomar.

2.2.2.3. Decidir

Decidir é quando o comandante toma decisões, baseado no cenário formado na fase anterior e nas possíveis linhas de ação (hipóteses a serem consideradas como possibilidades de escolha), emitindo as ordens aos escalões subordinados (Brasil, 2015, p.2-6). Em outras palavras, é selecionar a opção, ou opções, desenvolvidas dentre as hipóteses de projeção futura na fase anterior. Dessa forma, é decidido o curso das ações, e, em consequência, é preparada a distribuição de ordens. Desse modo, ao decidir, o comandante põe em prática as regras envolvidas no mecanismo de decisão, faz uso de suas próprias idiossincrasias a respeito das rotinas adotadas e suas preferências.

2.2.2.4. Agir

Agir consiste em executar e avaliar as ações, promovendo a realimentação do ciclo. Assim, os comandantes de escalões subordinados transformam as ordens superiores em ações específicas, alterando a situação do ambiente operacional e exigindo atualização de informações e, consequentemente, iniciando um novo ciclo de C2 (Brasil, 2015, p.2-6).

O ciclo OODA de C2 permite que sejam entendidos com clareza os processos relativos às funções gerenciais de Comando e Controle e os identificar. Desta forma, torna-se mais fácil definir o que é necessário fazer.

Cabe ressaltar que a forma de aplicação do ciclo de C2 está ligada ao nível de decisão envolvido. Logo, para uma mesma questão a ser submetida ao

ciclo, aplicando-a em níveis decisórios distintos, a pertinência ou não de certas informações será diferente. Como exemplo, seja considerado a seguinte questão: o emprego militar em uma situação de conflito é necessário? Se o nível decisório for o do comandante supremo, ou seja, no caso brasileiro, do Presidente da República, uma informação meteorológica não será relevante, no entanto, para o comandante da tropa a ser empregada, pode ser essencial.

Um dos principais suportes ao processo de C2 é o processo realizado pelo ciclo de inteligência militar ou de estado. Esse ciclo é sinteticamente explanado no subtítulo 2.2.3 a seguir.

2.2.3. Ciclo de Inteligência Militar ou de Estado

Dentre os principais mecanismos de busca de informações para fins estratégicos de defesa nacional que todas as forças armadas e serviços de inteligência do mundo utilizam está o ciclo de inteligência. O ciclo de inteligência militar, também conhecido como ciclo de inteligência de estado, é um processo contínuo e iterativo que envolve a coleta, análise e disseminação de informações relevantes para apoiar as atividades de segurança e tomada de decisões de um governo ou organização militar ou, em situações mais operacionais, durante operações militares. Embora os detalhes específicos do ciclo possam variar de acordo com a estrutura e as políticas de cada país ou organização, geralmente segue as etapas fundamentais descritas por Jonhson (2007, p.366), conforme sintetizado nos subtítulos 2.2.3.1 a 2.2.3.8.

2.2.3.1. Coleta de informações

A primeira etapa do ciclo envolve a coleta de informações brutas de várias fontes, como inteligência humana (HUMINT), inteligência de sinais (SIGINT), inteligência geoespacial (GEOINT) e inteligência de código aberto (OSINT). Essas informações podem ser obtidas por meio de vigilância, espionagem, monitoramento de comunicações, observação de satélites, entre outros métodos.

2.2.3.2. Processamento e exploração

As informações coletadas são processadas e analisadas para extrair conhecimento útil. Nessa etapa, os analistas de inteligência avaliam a credibilidade, a veracidade e a relevância das informações, além de relacioná-las com conhecimentos pré-existentes e outras fontes de inteligência. As técnicas de processamento de dados, como mineração e análise de padrões, podem ser aplicadas para inferir informações não explícitas na observação dos dados brutos da fonte.

2.2.3.3. Análise e avaliação

Nesta fase, os analistas de inteligência examinam cuidadosamente os dados processados e explorados para identificar padrões, tendências, ameaças emergentes e outros elementos significativos. A análise é feita com base em métodos e modelos analíticos estabelecidos, bem como na experiência e conhecimento especializado dos analistas. O objetivo é compreender a situação atual, prever desenvolvimentos futuros e avaliar o impacto potencial nas decisões políticas e militares.

2.2.3.4. Produção de inteligência

Os resultados da análise e avaliação são transformados em produtos de inteligência, como relatórios, avaliações, reuniões de orientação e planejamento (*briefings*) e recomendações. Esses produtos são adaptados às necessidades específicas dos tomadores de decisão e apresentados de maneira clara e concisa. A produção de inteligência envolve a comunicação efetiva das inferências e descobertas aos destinatários apropriados, garantindo que as informações sejam transmitidas de maneira oportuna e compreensível.

2.2.3.5. Disseminação e compartilhamento

As informações e os produtos de inteligência são compartilhados com os tomadores de decisão e outros usuários relevantes. Isso pode ocorrer em várias formas, como reuniões de orientação, relatórios escritos, bancos de dados

de inteligência ou sistemas de compartilhamento seguro. A disseminação eficaz da inteligência é crucial para garantir que as informações cheguem às pessoas certas no momento certo, permitindo que tomem decisões informadas.

2.2.3.6. Utilização e tomada de decisões

Nesta fase, os tomadores de decisão utilizam os produtos de inteligência para apoiar a formulação de políticas, estratégias e planos de ação. Com base nas informações e análises fornecidas, as decisões são tomadas em relação às operações militares, segurança nacional, defesa, política externa e outras áreas pertinentes. A inteligência militar ou de estado desempenha um papel crucial na identificação de ameaças, na compreensão das intenções e capacidades de adversários potenciais, na avaliação de riscos e na orientação das ações a serem tomadas.

2.2.3.7. Implementação

Uma vez que as decisões são tomadas, inicia-se a fase de implementação. Isso envolve a tradução das decisões em ações práticas e estratégias operacionais. As informações de inteligência são compartilhadas com as unidades militares relevantes, agências de segurança e outros atores envolvidos na execução das políticas e operações. A implementação também pode incluir o monitoramento contínuo da situação e a atualização das estratégias conforme necessário.

2.2.3.8. Avaliação e retroalimentação

Após a implementação, é importante realizar uma avaliação contínua para analisar a eficácia das ações tomadas e dos processos de inteligência utilizados. A coleta de avaliações críticas e a análise de resultados ajudam a identificar lições aprendidas, lacunas nas informações ou nas capacidades de inteligência e oportunidades de melhoria. Essa avaliação contínua é essencial para aprimorar o ciclo de inteligência militar ou de estado, garantindo que ele seja adaptado às necessidades em constante evolução.

2.2.4. Conceitos de Guerra da Informação

A guerra da informação envolve um ciclo complexo de gestão da informação e de conhecimento que é cada mais aplicado na esfera militar, conforme os conflitos se tornam profundamente tecnológicos e não tão de embate humano direto. Neste tópico é apresentado um resumo das definições de Alberts *et al*. (2004) que modela o espaço informacional para obtenção de vantagens em um conflito.

Alberts *et al*. (2004, p.9) estabelece uma série de conceitos, que ele se refere como “primitivas” para apoiar a construção teórica a respeito do desenvolvimento da chamada “guerra da informação”, na qual o objetivo central é o da superioridade informacional. Esses conceitos são estabelecidos para diminuir a ambiguidade associada ao termo “informação” e dar uma utilidade prática para sua aplicação no campo militar.

2.2.4.1. Domínios

Para o desenvolvimento dos aspectos teóricos propostos por Alberts *et al*. (2004, p.10), o autor estrutura o campo de batalha em três ambientes: físico, informacional e cognitivo.

O **domínio físico** é aquele no qual as ações militares são realizadas e provocam consequências físicas na terra, no mar, no ar e no espaço. São os ambientes considerados no meio militar como “tradicionais”, onde as mensurações e indicadores de efeitos das ações são mais diretos.

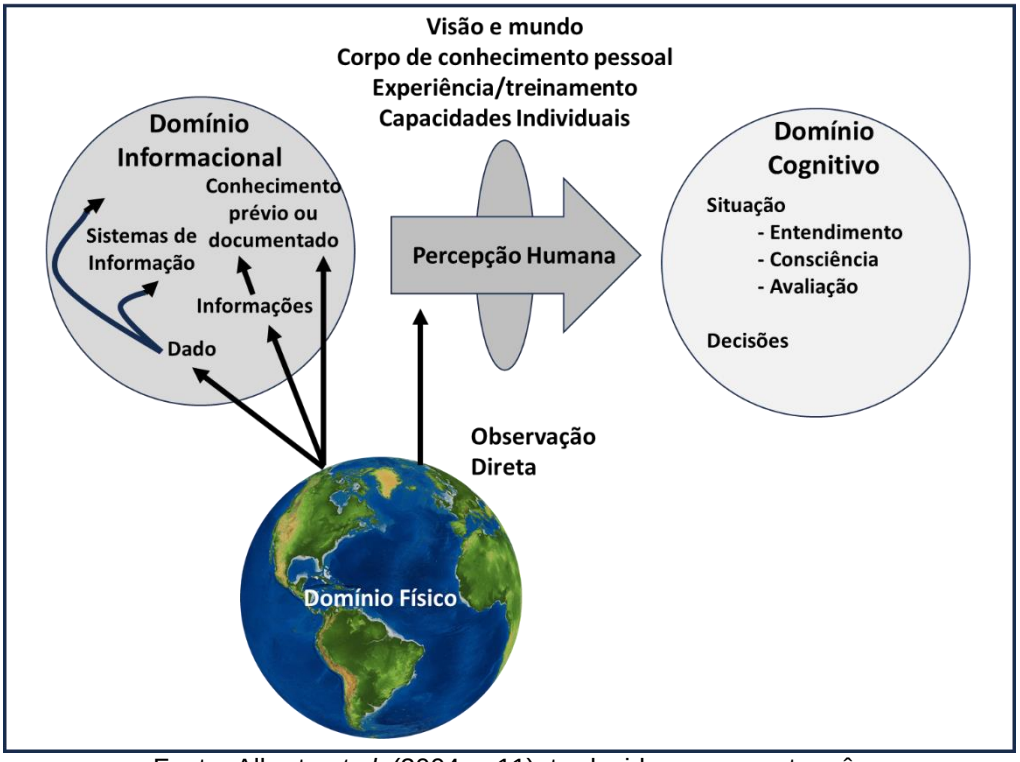
O **domínio informacional** é aquele no qual a informação é criada, manipulada e compartilhada (Alberts *et al*., 2004, p.12). Por meio deste domínio é que se viabilizada comunicação entre os indivíduos que perfazem o combate e no qual reside a geração de força para empregar os meios da batalha. É o domínio considerado “nível zero” para se obter a superioridade informacional em batalha (Alberts *et al*., 2004, p.13). Em parte pelo grande avanço das redes sociais, há abordagens que consideram este um outro domínio, no entanto, para fins da presente pesquisa, as redes sociais são consideradas no domínio informacional.

O **domínio cognitivo** está na mente dos participantes e é o espaço onde a percepções, consciência, entendimento, crenças e valores residem e onde a formação de significado (*sensemaking*) e a tomada de decisão ocorrem. Além disso, seus atributos são difíceis de medir e, considerando cada mente humana como um subdomínio, cada um desses subdomínios é único (Alberts *et al*., 2004, p.13). Ainda sobre o domínio cognitivo:

> ... o conteúdo do domínio cognitivo passa por um filtro ou lente que chamamos de percepção humana. Este filtro consiste na visão de mundo do indivíduo, no conjunto de conhecimentos pessoais que a pessoa traz para a situação, na sua experiência, treinamento, valores e nas capacidades individuais (inteligência, estilo pessoal, capacidades perceptivas etc.). Como esses planos de percepção humana são únicos para cada indivíduo, sabemos que a cognição individual (compreensão etc.) também é única (Alberts *et al*., 2004, p.13).[1]

A Figura 14 representa os domínios físico, informacional e cognitivo em perspectiva.

Figura 14 - Domínios físico, informacional e cognitivo



Fonte: Alberts *et al.* (2004, p.11), traduzido para o português.

[1] *... the contents of the cognitive domain pass through a filter or lens we have labeled human perception. This filter consists of the individual's worldview, the body of personal knowledge the person brings to the situation, their experience, training, values, and the individuals capabilities (intelligence, personal style, perceptual capabilities, etc.) Since these human perception plans are unique to each individual, we know that individual cognition (understandings, etc.) are also unique (ALBERTS et al., 2004, p.13).*

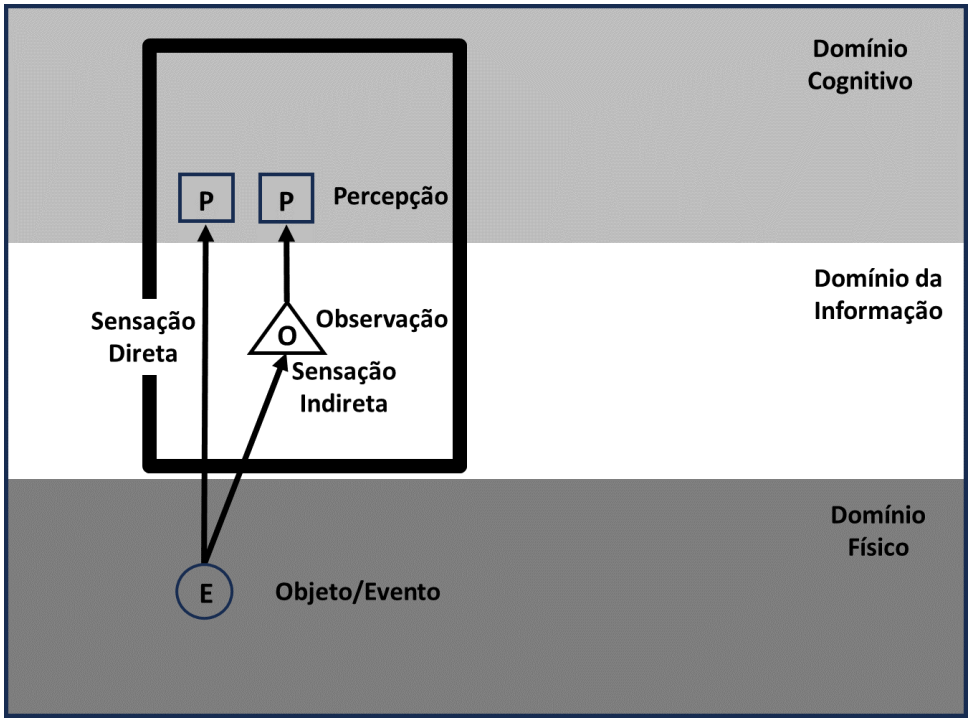
2.2.4.2. Primitivas

Alberts *et al*., (2004, p.14) estabelece onze conceitos, os quais ele designa como primitivas, para a descrição e facilitação da mensuração dos elementos dos domínios informacional e cognitivo. São elas: sensação (*sensing*), observações (*observations*), informação (*information*), conhecimento (*knowlegde*), consciência (*awareness*), entendimento (*understanding*), decisões (*decisions*), ações (*actions*), compartilhamento (*sharing*), colaboração (*collaboration*), sincronização (*synchronization*).

2.2.4.2.1. Sensação (*sensing*)

O conceito de sensação é definido pela detecção de algo no mundo real por meio dos sentidos. Pode ser de dois tipos: direta e indireta. A sensação direta é aquela que se realiza por um dos cinco sentidos humanos no domínio físico. A sensação indireta é aquela que se concretiza pela captação de um evento do domínio físico por meio de um sensor construído pelo homem e que facilita ou intermedia o processo direto (Alberts *et al*., 2004, p.14).

Figura 15 - Sensação e suas relações nos domínios



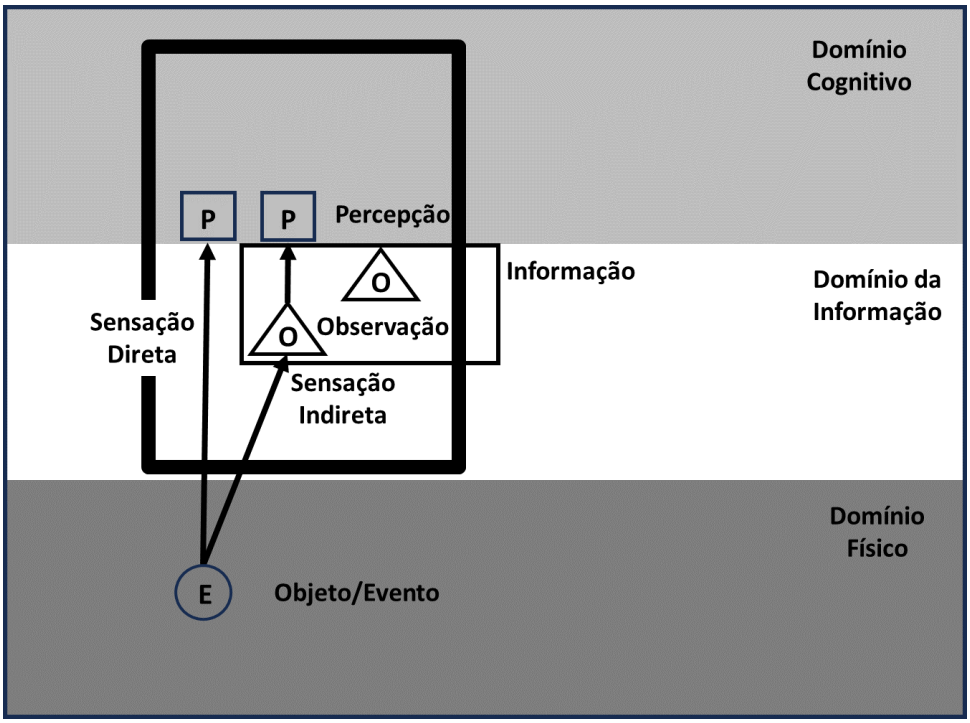
Fonte: Alberts *et al*. (2004, p.15), traduzido para o português.

Os sensores para a sensação indireta facilitam a captação dos eventos e podem ser encarados como mecanismos para reduzir a incerteza sobre o que está ocorrendo no ambiente físico de modo virtualmente invisível à sensação direta (Alberts at al, 2004, p.15). A Figura 15 representa a relação entre os domínios e o conceito de sensação.

2.2.4.2.2. Observações e Informação

Em seu desenvolvimento teórico, Alberts *et al*. (2004, p.16), conceitua a informação como uma estruturação de um conjunto de observações (dados) em um contexto significativo. Nesse contexto, dados são definidos como representações de fatos, conceitos ou instruções que sejam úteis para comunicação, interpretação ou processamento por indivíduos humanos. Cabe ressaltar que dados podem ser perdidos, deixados de lado ou filtrados pelas "lentes" de percepção dos indivíduos. A Figura 16 representa a relação dados e informação com os domínios.

Figura 16 - Informação e suas relações nos domínios

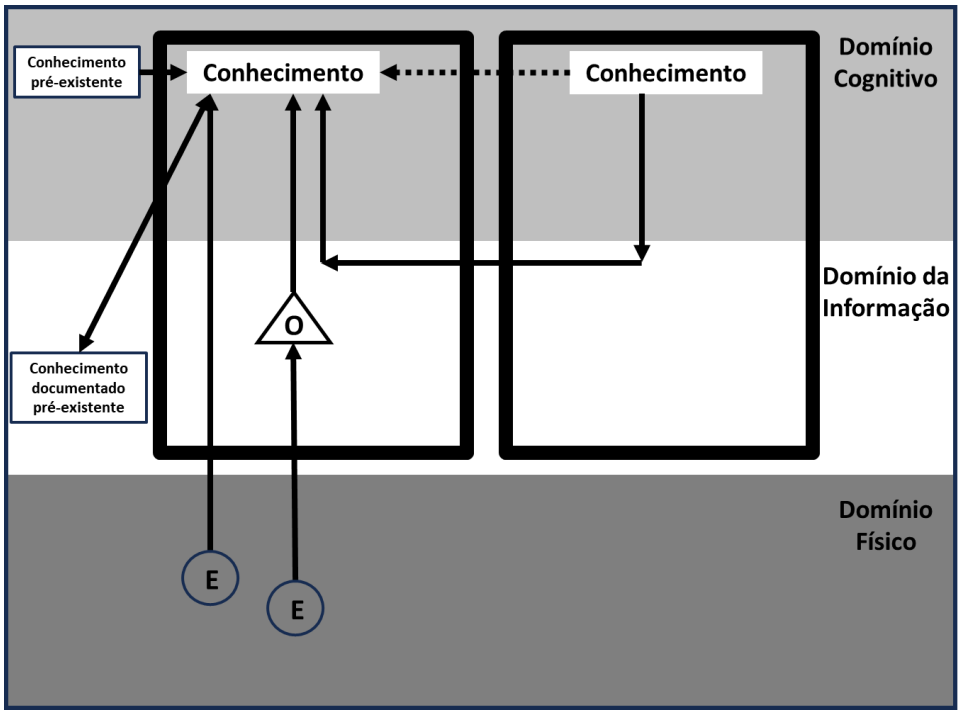


Fonte: Alberts at al (2004, p.16), traduzido para o português.

2.2.4.2.3. Conhecimento

Para Alberts *et al*. (2004, p.17), o conhecimento envolve as conclusões que se chega a partir de padrões sugeridos pelas informações obtidas. Pode estar tanto no domínio cognitivo como no domínio informacional, por exemplo, considerando este último, na forma de lições aprendidas. Numa dada situação, pode-se reconhecer o conhecimento na forma preexistente no domínio cognitivo como, por exemplo, na forma de doutrina. Dentre as possibilidades de inserção de conhecimento no domínio cognitivo de um indivíduo, pode-se ter: (i) educação prévia, treinamento ou experiência; (ii) experiência direta com o domínio físico; (iii) interação com outros humanos; (iv) interação com o domínio informacional. A síntese dos elementos envolvidos está na Figura 17.

Figura 17 - Conhecimento e suas relação nos domínios



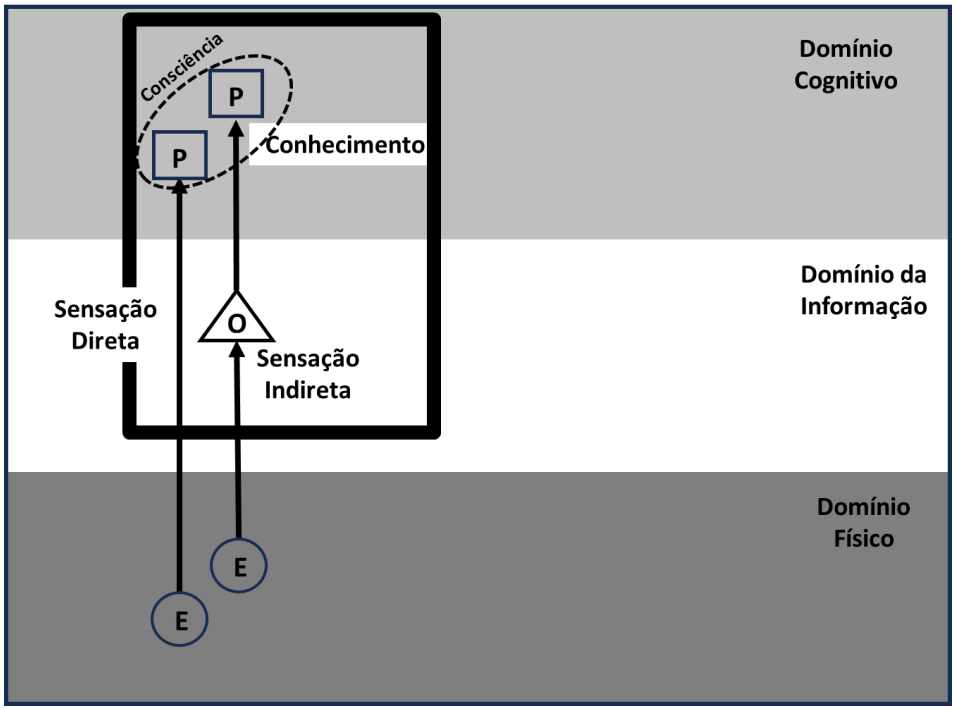
Fonte: Alberts at al (2004, p.17), traduzido para o português.

2.2.4.2.4. Consciência

A consciência é o resultado da interação entre o conhecimento prévio e a percepção da realidade corrente e é única para cada indivíduo para uma dada situação de combate. Por meio de treinamentos e educação é possível

provocar consciências similares em indivíduos diferentes diante de situações com os mesmos dados e informações. A consciência pertence ao domínio cognitivo (Alberts *et al*., 2004, p.18), conforme Figura 18.

Figura 18 - Consciência e suas relação nos domínios



Fonte: Alberts *et al*. (2004, p.19), traduzido para o português.

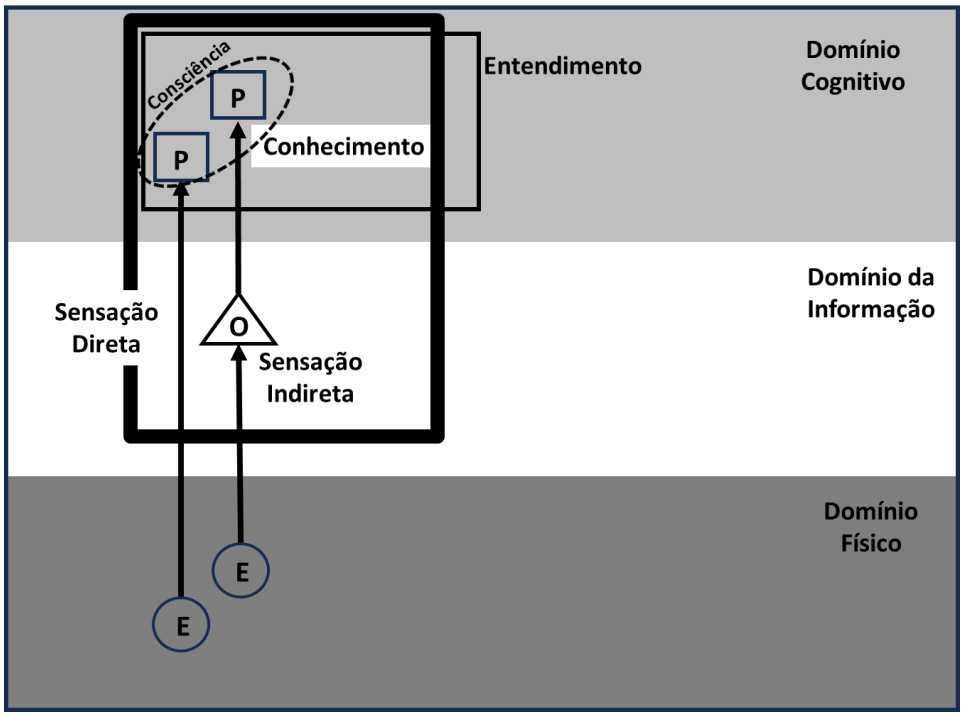
2.2.4.2.5. Entendimento

O entendimento, segundo Alberts *et al*. (2004, p.19) consiste em se ter suficiente conhecimento para ser capaz de inferir as possíveis consequências de uma situação. A Figura 19 busca sintetizar essa definição.

2.2.4.2.6. Decisões

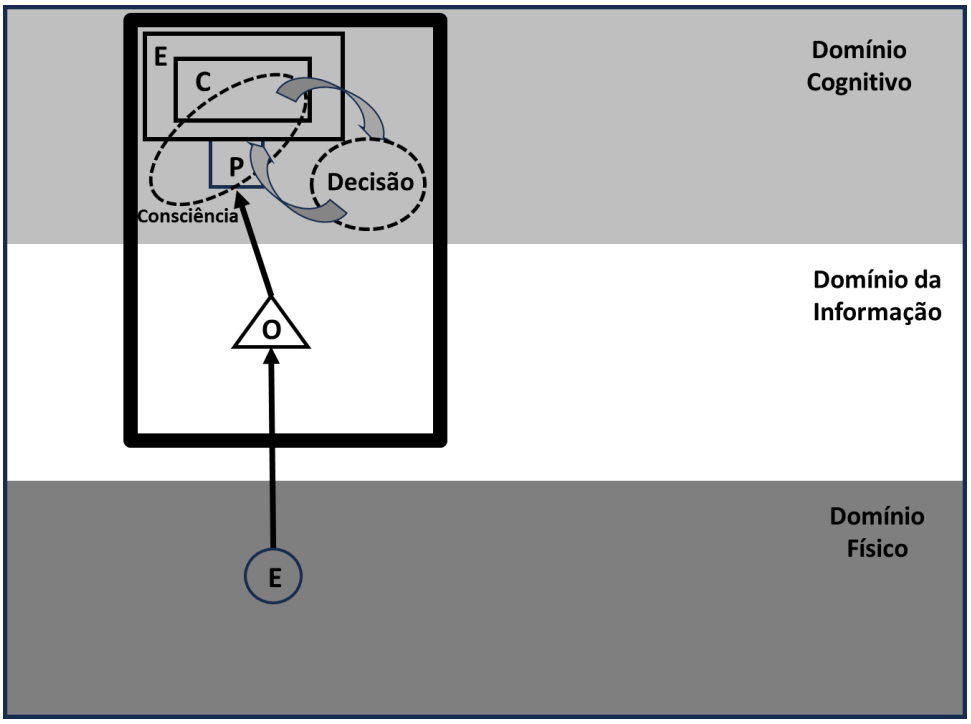
As decisões são escolhas sobre o que fazer (Alberts *et al*., 2004, p.20). As decisões fluem pelo domínio informacional e provocam efeitos no domínio físico. Num campo de batalha, as decisões são propagadas por todas as organizações envolvidas, provocando outras decisões em níveis diferentes de comando e controle, conforme representado na Figura 20.

Figura 19 - Entendimento e suas relação nos domínios



Fonte: Alberts *et al*. (2004, p.20), traduzido para o português.

Figura 20 - Decisões e suas relação nos domínios

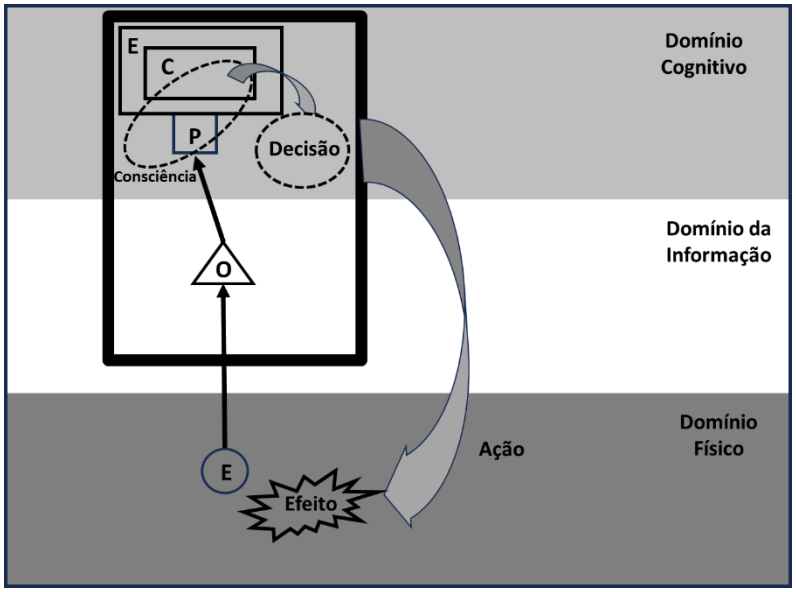


Fonte: Alberts *et al*. (2004, p.21), traduzido para o português.

2.2.4.2.7. Ações

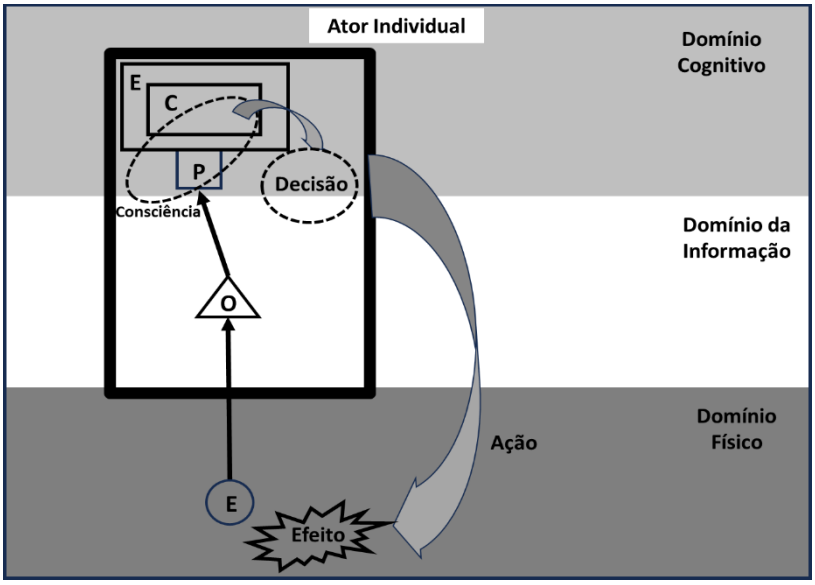
Ações são efetuadas no domínio físico a partir das decisões tomadas no domínio cognitivo e transportadas pelo domínio informacional. Esse processo é desencadeado a partir da tomada de consciência de algum evento e seu entendimento, como se pode ver representado na Figura 21. Já a Figura 22 aplica os conceitos conhecimento, consciência, entendimento, decisão e ação para retratar um ciclo OODA (Alberts *et al*., 2004, p.23).

Figura 21 - Ações e suas relação nos domínios



Fonte: Alberts *et al*. (2004, p.22), traduzido para o português.

Figura 22 - Ciclo OODA



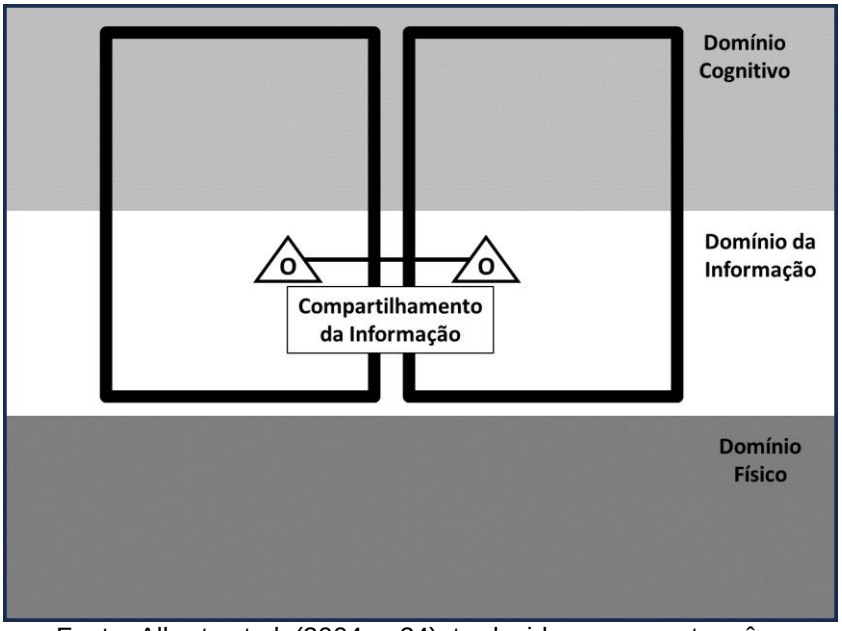
Fonte: Alberts *et al*. (2004, p.23), traduzido para o português.

2.2.4.2.8. Compartilhamento

Na sua estruturação teórica, Alberts *et al*. (2004, p.24) discorre sobre três tipos de compartilhamento: compartilhamento da informação, compartilhamento de conhecimento e compartilhamento de consciência.

O compartilhamento da informação se dá quando ao menos duas entidades interagem no domínio informacional. Essas entidades podem ser indivíduos humanos, bases de dados ou programas de computadores. A Figura 23 fornece uma representação esquemática desse compartilhamento.

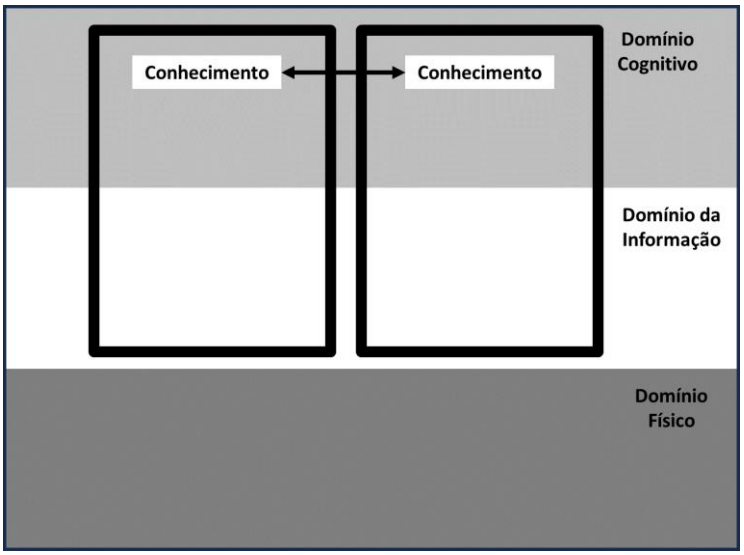
Figura 23 - Compartilhamento do conhecimento e suas relações nos domínios



Fonte: Alberts et al. (2004, p.24), traduzido para o português.

O compartilhamento do conhecimento nas organizações de defesa, seja explícito ou tácito, é um elemento de vital importância, pois a doutrina, os planejamentos, as lições aprendidas e outros elementos de conhecimento devem estar adequadamente compartilhados para viabilizar ações coordenadas de unidades independentes numa manobra de combate (Alberts *et al*., 2004, p.25). Esse compartilhamento influencia diretamente a efetividade do processo de comando e controle. A Figura 24 fornece uma representação do compartilhamento de conhecimento.

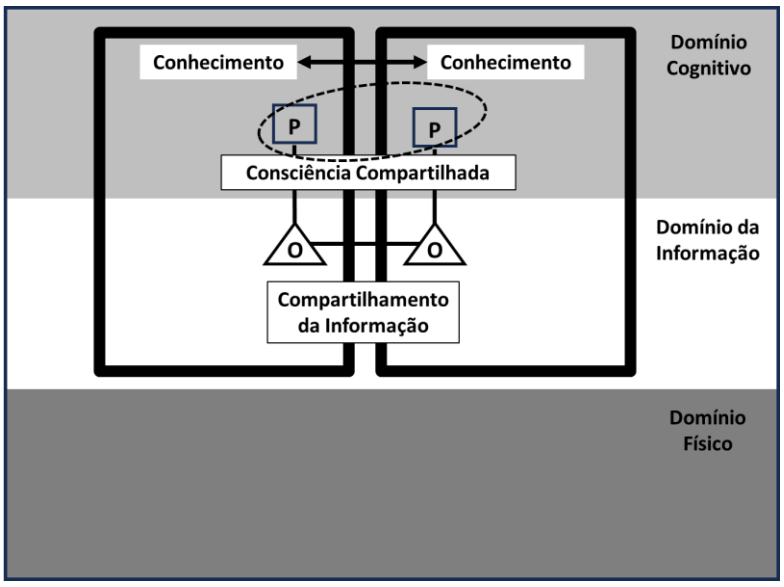
Figura 24 - Compartilhamento da informação e suas relações nos domínios



Fonte: Alberts *et al*. (2004, p.26), traduzido para o português.

O compartilhamento da consciência ocorre quando ao menos duas entidades são capazes de desenvolver consciências similares a respeito de uma situação. O nível de similaridade dependerá do grau de colaboração e de sincronização requerido na operação (Alberts *et al*., 2004, p.26). Cabe ressaltar que múltiplos fatores influenciam no estado da consciência compartilhada, a começar pelos compartilhamentos da informação e conhecimento, além de elementos tais como visão de mundo, cultura, linguagem e interesse. A Figura 25 representa o compartilhamento de consciência.

Figura 25 - Compartilhamento de consciência e suas relações nos domínios

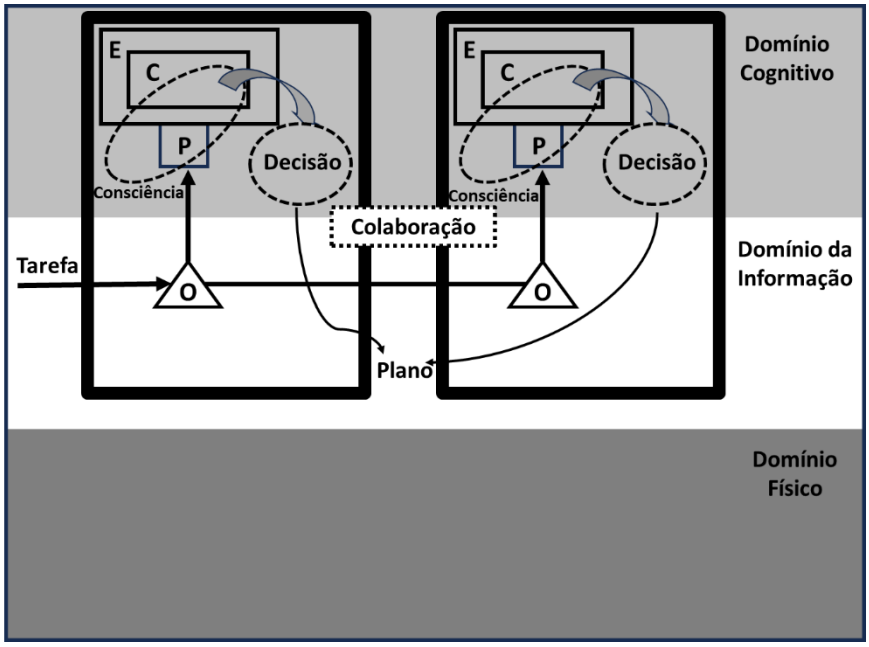


Fonte: Alberts *et al*. (2004, p.27), traduzido para o português.

2.2.4.2.9. Colaboração

A colaboração é o trabalho conjunto por um propósito comum envolvendo duas ou mais entidades. Esse processo se desenvolve no domínio cognitivo, envolve graus de compartilhamento de consciência e conhecimento e, por fim, levando à produção e ao compartilhamento de informação necessários para a ação comum (Alberts *et al*., 2004, p.27). A colaboração à distância, juntamente com o compartilhamento da informação, é uma característica-chave de ambientes centrados em redes. A Figura 26 representa o processo de colaboração.

Figura 26 - Colaboração e suas relação nos domínios



Fonte: Alberts *et al*. (2004, p.28), traduzido para o português.

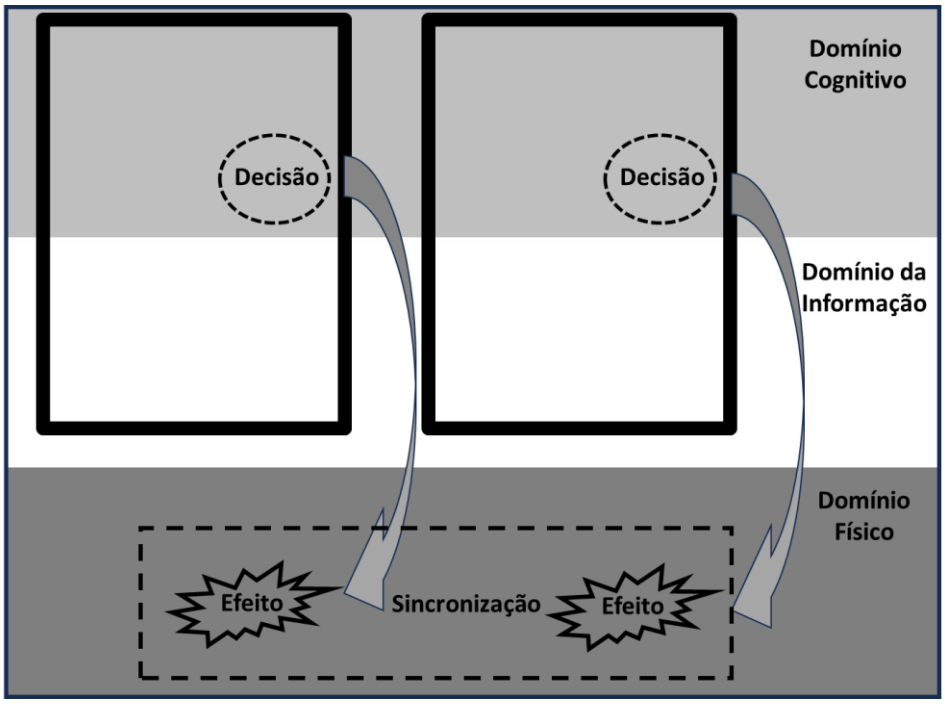
2.2.4.2.10. Sincronização

Alberts *et al*. (2004, p.28) define sincronização como um arranjo de coisas ou efeitos no tempo e no espaço voltados para um propósito. A sincronização pode resultar de planejamento e coordenação consciente ou mesmo de consciência situacional compartilhada num evento espontâneo. A Figura 27 representa o processo de sincronização.

A explanação sobre os processos de gestão da informação apresentados neste tópico teve por objetivo exemplificar a necessidades da esfera militar no tratamento da informação em seu ciclo de vida e como isso

alicerça as modalidades mais modernas de conflito, tais como defesa cibernética, como será abordado no tópico 2.3 a seguir.

Figura 27 - Sincronização e suas relação nos domínios



Fonte: Alberts *et al*. (2004, p.29), traduzido para o português.

2.3. DEFESA E SEGURANÇA CIBERNÉTICA

2.3.1. Contexto Geral

Considerando a perspectiva das estruturas de defesa das diversas nações que empregam a cibernética como uma das formas de sua defesa, o termo “defesa cibernética” tem acepções diversas de acordo com o país que o emprega. O conceito pode abranger desde significados predominantemente voltados para a salvaguarda das informações contidas no espaço cibernético, sendo esta acepção mais conhecida como segurança cibernética, até interpretações calcadas em ações ofensivas. Situações há em que a expressão defesa cibernética até é evitada, dando lugar a expressões que denotem um caráter de não agressão.

Dada a especificidade do trabalho de pesquisa, o qual está voltado para o caso brasileiro, optou-se por se discorrer diretamente o caso nacional, apresentando-se um breve histórico e as nuances principais da doutrina militar brasileira sobre defesa cibernética.

2.3.2. Defesa Cibernética no Brasil

De modo a sustentar as análises realizadas nesta pesquisa, uma breve explanação do conceito de defesa cibernética é apresentada neste ponto. O objetivo é estabelecer sua abrangência, limites e significação. A definição de defesa cibernética consta do manual de defesa cibernética publicado pelo Ministério da Defesa. No documento emitido pelo Ministério da Defesa MD31-M-07 – Doutrina Militar de Defesa Cibernética consta o seguinte:

> 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 as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (Brasil, 2014, p.18)

Essa definição destaca quatro partes principais do conceito: (i) defesa cibernética é um conjunto de ações; (ii) as ações se realizam no espaço cibernético; (iii) as ações são desenvolvidas sob um processo de planejamento militar; (iv) defesa cibernética tem por objeto de ação sistemas de informação de interesse da defesa, ou seja, proteção dos próprios sistemas e comprometimento de sistemas dos oponentes.

De modo complementar, podem-se citar outras menções referentes ao conceito que, embora não sejam de ampla aplicação, foram geradas para servir como primeiros conhecimentos estabelecidos e relacionados ao âmbito das aplicações da defesa cibernética no Brasil. Na obra “Desafios Estratégicos para a Segurança e Defesa Cibernética”, publicada em 2011 pela Secretaria de Assuntos Estratégicos da Presidência da República, há coletânea de artigos que buscavam gerar conhecimentos sobre o assunto. No artigo “Reflexões sobre Segurança e Defesa Cibernética”, Mandarino Junior (2011) afirma:

> Aplicando os conceitos de segurança e defesa ao espaço cibernético, surgem os conceitos de segurança e de defesa cibernética. Entende-se, portanto, que segurança incorpora as ações de prevenção (incidentes) e repressão enquanto a defesa cibernética abrange ações ofensivas e defensivas.

Nessa definição, embora compacta, fica clara a possibilidade de a cibernética ser usada ofensivamente e em autodefesa, como uma extensão do conceito tradicional de defesa, entendendo-se como “tradicional” a aplicação do termo como originalmente cunhado para defesa do país e antes da defesa cibernética surgir. Cabe observar a distinção entre defesa cibernética e segurança cibernética, sendo que esta última visa prevenir ataques cibernéticos e reprimi-los, ou seja, neutralizar suas consequências no menor prazo possível e, conforme o caso, tratar como questão policial e jurídica a identificação e punição dos autores.

No Guia de Defesa Cibernética na América do Sul de 2016/17, Oliveira *et al*. (2017), encontra-se no glossário a seguinte definição para defesa cibernética:

> Ato de defender o sistema crítico das tecnologias de informação e comunicações (TIC) de um Estado. Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país. (Oliveira *et al*. 2017).

Nessa definição, chama-se indiretamente a atenção para aplicação da defesa cibernética na proteção das infraestruturas críticas do país. Importante notar que foi utilizado o termo “defender” e não “segurar” ou “prover segurança” ao sistema crítico de TIC de um Estado.

Nos trabalhos internos do Centro de Defesa Cibernética (CDCiber), foi proposto que a Defesa Cibernética poderia ser vista como “extensão da missão constitucional das Forças Armadas no espaço cibernético”. Esta abordagem da defesa cibernética foi repetidamente explorada em apresentações públicas nacionais e internacionais durante os anos de 2015 e 2016, como, por exemplo, na abertura do IV Seminário Internacional de Defesa Cibernética, realizado na cidade de Foz de Iguaçu, em 2015[2].

Logo, conforme o artigo 142 da Constituição da República Federativa do Brasil (Brasil,1988), pode-se depreender que o exercício da defesa cibernética

[2] https://www.defesanet.com.br/cyberwar/seminario-internacional-de-defesa-cibernetica/

tomará parte do esforço de defender a pátria, garantir os poderes constitucionais e, por iniciativa destes, da Lei e da Ordem, no âmbito do espaço cibernético.

Fernandes (2021, p.538) enuncia a defesa cibernética nacional como sendo:

> defesa cibernética nacional é o conjunto de mobilizações das expressões de poder cibernético nacional conduzida pelo Estado, sob a coordenação da expressão militar, para a defesa do território, da soberania e dos interesses nacionais, contra ameaças preponderantemente externas, potenciais e manifestas.

Nessa definição, cabe ressaltar dois elementos. O primeiro, é o termo poder cibernético, o qual diz respeito às possibilidades de ação no campo cibernético que uma nação pode ter e que não necessariamente se restringe ao campo da tecnologia da informação, mas em outras categorias que podem ser influenciadas ou atingidas por meio da quebra da segurança das estruturas cibernéticas que as sustentam, como, por exemplo o campo econômico.

A segunda, por sua vez, diz respeito à definição propriamente dita de defesa cibernética, para a qual se tomou por base a definição de defesa nacional da Escola Superior de Guerra (ESG)[3], e indicando uma transição para o campo cibernético por meio da adaptação das expressões tanto de defesa quanto do poder nacional.

2.3.3. Ações de defesa cibernética segundo a doutrina militar de defesa cibernética brasileira

As ações cibernéticas podem ser de três naturezas. Segundo a Doutrina Militar de Defesa Cibernética, essas ações são designadas como: proteção cibernética; exploração cibernética; ataque cibernético. (Brasil, 2014, p. 23).

Primeiramente, têm-se as ações de proteção cibernética. Essas ações preservam os dados digitais de interesse da defesa nacional, os respectivos sistemas que os processam e as redes por onde trafegam.

[3] Defesa Nacional é o conjunto de atitudes, medidas e ações do Estado, com ênfase na Expressão Militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais e manifestas. (ESCOLA SUPERIOR DE GUERRA, 2009, p. 64).

Em segundo lugar, as ações de exploração cibernética buscam no espaço cibernético obter informações de toda sorte, mas úteis para preponderância no combate. De natureza especialmente importante são informações sobre vulnerabilidades de sistemas informacionais existentes no espaço cibernético pertencentes ou utilizados por agentes que ameacem a soberania nacional. Essas informações dão suporte à tomada de decisão de um comandante de uma operação militar.

Por fim, tem-se a ação de ataque cibernético, a qual é de natureza ofensiva tendo por alvo sistemas digitais localizados no espaço cibernético e cujo comprometimento neutralizaria ou degradaria a capacidade ofensiva de um agente ameaçador à soberania nacional.

A aplicação de ações cibernéticas desencadeia efeitos cibernéticos. Esses efeitos dizem respeito aos impactos causados em sistemas de informações pertencentes ou utilizados por oponentes, por meio das ações de ataque cibernético, causando a sua degradação ou neutralização direta ou de estruturas por eles suportadas. Por “oponente”, neste contexto, entende-se um ente hostil ao país e que leve às entidades que garantem a Defesa Nacional a agir em legítima defesa da pátria contra ataques à soberania nacional.

2.3.4. Segurança da Informação e Cibernética

A segurança da informação é um conceito que se consolidou na década de 90 mundialmente por meio da disseminação de uma série de normas elaboradas para a proteção das informações no ambiente organizacional. Embora diversos padrões tenham sido publicados e utilizados, um em especial despontou como referência para aplicação em nível mundial de segurança da informação. Esse padrão se consolidou como a atual série 27000 de normas ISO/IEC, partindo, originalmente, de normas britânicas do *British Standards Institution* (BSI)[4] que foram adotadas como padrão internacional. Esse padrão

[4] *BSI, the British Standards Institution, is a nonprofit organization that develops and publishes standards that oversee virtually every aspect of modern society. Headquartered in London, United Kingdom, BSI is the United Kingdom's national standards organization and its representative in the European CEN and the international ISO and IEC. The pioneer of standards for management systems, BSI is now the world's largest certification body.* Texto retirado em 5/11/2023 do endereço eletrônico:

foi totalmente erigido sobre a noção de que para se obter a segurança da informação era necessário preservar três de seus atributos: (i) confidencialidade; (ii) disponibilidade; (iii) integridade (ABNT, 2013, p.1).

Com a tecnologia da informação ocupando um percentual que cada vez mais se aproxima dos 100% para conter na forma digital as informações relevantes de toda e qualquer organização, a aplicação da segurança da informação passou a ser majoritariamente no campo do ambiente digital das organizações, o que ganhou a denominação de segurança cibernética.

A definição relativa à segurança cibernética na série 27000, mais especificamente contidas na versão brasileira ISO/IEC NBR 27032 (ABNT, 2015), remete-se integralmente à definição da segurança da informação, ou seja, a segurança cibernética é a preservação da confidencialidade, da disponibilidade e da integridade das informações no espaço cibernético (ABNT, 2015, p.5).

A segurança cibernética passou a ser largamente usada para as melhores práticas de segurança de dados digitais, cobrindo desde as regulações internas das organizações até a legislação de diversos países, inclusive no Brasil. Por conta da Internet e outras redes digitais globais, o campo onde se dá a realização da aplicação da segurança cibernética mereceu uma nova designação, sendo denominado espaço cibernético.

O espaço cibernético abrange redes de dados digitais, em todas as modalidades de processamento, armazenamento ou transmissão dessas informações ou ainda em dispositivos computacionais isolados. Há diversas definições do conceito que, em geral, figuram em documentos normativos e doutrinários militares. Por exemplo, segundo as normas 27032, da ABNT, o espaço cibernético é definido como sendo o ambiente complexo resultante da interação de pessoas, software e serviços na Internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe em qualquer forma física (ABNT, 2015, p. 2).

Pela sua aplicação e experimentação, as boas práticas de segurança da informação, conforme se constata a partir da primeira década dos anos 2000,

---

https://webstore.ansi.org/SDO/BSI?gclid=Cj0KCQjw-pyqBhDmARIsAKd9XINKW4JGKD6rfRdyccVMJjeetjgSq5oKNgj70EM2K2OxmVNGRrBQ0dkaAszIEALw_wcB

voltam a se fragmentar tanto na especialização cada vez maior da série ISO/IEC 27000 quanto no surgimento de padrões internacionais como, por exemplo, a série de controles CIS *Controls & Resources* (*Center for Internet Security*)[5], Normas do *National Institute of Standards and Technology* (NIST)[6], o *framework* para gestão e governança de tecnologia da informação *Control Objectives for Information and Related Technologies* (COBIT)[7], além de outros, cabendo ressaltar que a segurança cibernética passa a ser totalmente integrada a esses quadros de referência, pois é derivada da segurança da informação. Essa fragmentação é fruto tanto da especialização técnica quanto da necessidade gerencial em níveis distintos, além de outros fatores mais específicos conforme o caso.

Devido à sua abrangência, a segurança cibernética se tornou uma referência importante para a defesa cibernética, pois compõe o aspecto de proteção, ou da ação de proteção cibernética, conforme doutrina de defesa cibernética brasileira (Brasil, 2014, p. 23).

2.3.5. *Frameworks* e Normas de Segurança da Informação e Cibernética

De um modo geral, os *frameworks* são instrumentos de gestão que funcionam como quadros de referência para as áreas para as quais foram concebidos. Segundo Taherdoost (2022, p. 3), *frameworks* são guias que cobrem uma ampla gama de domínios, com objetivos gerais, mas sem os passos específicos para atingir esses objetivos. O mesmo autor acrescenta que são usados como padrão de qualidade para o que deve ser alcançado no contexto de sua aplicação, descrevendo escopo e sumarizando entradas e saídas.

Especificamente sobre *frameworks* de segurança da informação e cibernética, Taherdoost (2022, p. 8) informa que são estruturas que uma organização necessita para se tornar protegida de ataques cibernéticos, enquanto Syafrizal *at al* (2020, p. 419) afirma que o principal objetivo *frameworks* de segurança cibernética é reduzir os riscos, incluindo a prevenção e mitigação

[5] https://www.cisecurity.org/controls, acesso em 05/011/2023.
[6] https://www.nist.gov/, acesso em 05/11/2023.
[7] https://www.isaca.org/resources/cobit, acesso em 05/11/2023.

de ataques cibernéticos. Syafrizal *at al* (2020, p. 419) destaca a maior parte dos elementos de um *framework* de segurança cibernética são as melhores práticas do setor.

Nesse sentido, ou seja, sendo os *frameworks* de segurança da informação e cibernética reflexos das melhores práticas do setor, observa-se da sua aplicação uma ampla abrangência de áreas não só de tecnologia da informação, mas também de normatização, gestão de recursos humanos, segurança física, além de outros elementos. Isso leva a aplicação desse tipo de *framework* como um instrumento de sensibilização e aculturamento do pessoal em segurança, disciplinamento de ações estratégicas pelos documentos normativos gerados e geração de procedimentos operacionais específicos requeridos pelos ativos onde as ações estratégicas têm reflexos.

Os *frameworks* de segurança cibernética têm suas próprias especificidades e subdividem em categorias a segurança da informação ou cibernética, conforme o quadro de referência considerado. Por exemplo, as normas ISO 27002 (ABNT, 2022) categorizam a segurança da informação em 93 controles diferentes organizados em quatro categorias diferentes. O *framework* CIS em dezoito, enquanto o *Framework for Improving Critical Infrastructure Cybersecurity* ou *NIST Cybersecurity Framework* - NIST CSF (NIST, 2018), compacta 108 controles em subcategorias, categorias e, finalmente, cinco funções principais. Nesta revisão bibliográfica foram destacados aspectos da segurança cibernética e da informação de maior relevância para o exercício da ação de proteção da defesa cibernética, o que está exposto a partir do subtítulo 2.3.6, o que se designa no jargão técnico da segurança cibernética de “melhores práticas”.

2.3.6. Melhores Práticas em Segurança da Informação e Cibernética (normas técnicas e *frameworks*)

2.3.6.1. Série de Normas ISO/IEC 27000

A série de normas ISO/IEC 27000 fornece um conjunto de diretrizes e melhores práticas para estabelecer, implementar, monitorar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). A

série é extensa, abrangendo até mesmo diretrizes para segurança na área de saúde, porém, em coerência com o escopo desta pesquisa é dado destaque as mais utilizadas na segurança da informação e cibernética, ou seja, as normas NBR ISO/IEC 27001 (ABNT, 2020), 27002 (ABNT, 2022), 27005 (ABNT, 2023) e 27032 (ABNT, 2022).

A norma NBR ISO/IEC 27001 (ABNT, 2020) especifica os requisitos para estabelecer, implementar, manter e melhorar um SGSI em uma organização. Ela fornece uma abordagem abrangente para identificar os riscos à segurança da informação e implementar controles apropriados para mitigar esses riscos. A norma NBR 27001 é baseada na abordagem de melhoria contínua conhecida como PDCA (*Plan-Do-Check-Act*), fornecendo uma estrutura sólida para a implementação de um SGSI.

A norma NBR ISO/IEC 27002 (ABNT, 2022), fornece diretrizes detalhadas para a seleção e implementação de controles de segurança da informação. Ela descreve um conjunto abrangente de controles organizacionais, físicos, de pessoal e técnicos que podem ser aplicados para atender aos requisitos de segurança da informação de uma organização específica. A norma NBR ISO/IEC 27002 é projetada para ser utilizada em conjunto com a norma 27001, auxiliando as organizações na implementação de controles apropriados para proteger seus ativos de informação.

A norma NBR ISO/IEC 27002 (ABNT, 2022), fornece um conjunto de controles de segurança da informação, sendo 37 organizacionais, oito de pessoas, 14 físicos e 34 tecnológicos. A lista a seguir fornece as categorias dos controles, sendo a numeração que precede cada designação corresponde aos subtítulos dos capítulos 5 (controles organizacionais), 6 (pessoal), 7 (físico) e 8 (tecnológicos):

- 5. **Controles organizacionais**
- 5.1 Políticas de segurança da informação;
- 5.2 Papéis e responsabilidades pela segurança da informação;
- 5.3 Segregação de funções;
- 5.4 Responsabilidades da direção;
- 5.5 Contato com autoridades;

- 5.6 Contato com grupos de interesse especial;
- 5.7 Inteligência de ameaças;
- 5.8 Segurança da informação no gerenciamento de projetos;
- 5.9 Inventário de informações e outros ativos associados;
- 5.10 Uso aceitável de informações e outros ativos associados;
- 5.11 Devolução de ativos;
- 5.12 Classificação das informações;
- 5.13 Rotulagem de informações;
- 5.14 Transferência de informações;
- 5.15 Controle de acesso;
- 5.16 Gestão de identidade;
- 5.17 Informações de autenticação;
- 5.18 Direitos de acesso;
- 5.19 Segurança da informação nas relações com fornecedores;
- 5.20 Abordagem da segurança da informação nos contratos de fornecedores;
- 5.21Gestão da segurança da informação na cadeia de fornecimento de TIC;
- 5.22 Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores;
- 5.23 Segurança da informação para uso de serviços em nuvem;
- 5.24 Planejamento e preparação da gestão de incidentes de segurança da informação;
- 5.25 Avaliação e decisão sobre eventos de segurança da informação;
- 5.26 Resposta a incidentes de segurança da informação;
- 5.27 Aprendizado com incidentes de segurança da informação;
- 5.28 Coleta de evidências;
- 5.29 Segurança da informação durante a disrupção;
- 5.30 Prontidão de TIC para continuidade de negócios;
- 5.31 Requisitos legais, estatutários, regulamentares e contratuais;
- 5.32 Direitos de propriedade intelectual;
- 5.33 Proteção de registros;

- 5.34 Privacidade e proteção de DP;
- 5.35 Análise crítica independente da segurança da informação;
- 5.36 Conformidade com políticas, regras e normas para segurança da informação;
- 5.37 Documentação dos procedimentos de operação.
- 6 **Controles de pessoas**
- 6.1 Seleção;
- 6.2 Termos e condições de contratação;
- 6.3 Conscientização, educação e treinamento em segurança da informação;
- 6.4 Processo disciplinar;
- 6.5 Responsabilidades após encerramento ou mudança da contratação;
- 6.6 Acordos de confidencialidade ou não divulgação;
- 6.7 Trabalho remoto;
- 6.8 Relato de eventos de segurança da informação.
- 7 **Controles físicos**
- 7.1 Perímetros de segurança física;
- 7.2 Entrada física;
- 7.3 Segurança de escritórios, salas e instalações;
- 7.4 Monitoramento de segurança física;
- 7.5 Proteção contra ameaças físicas e ambientais;
- 7.6 Trabalho em áreas seguras;
- 7.7 Mesa limpa e tela limpa;
- 7.8 Localização e proteção de equipamentos;
- 7.9 Segurança de ativos fora das instalações da organização;
- 7.10 Mídia de armazenamento;
- 7.11 Serviços de infraestrutura;
- 7.12 Segurança do cabeamento;
- 7.13 Manutenção de equipamentos;
- 7.14 Descarte seguro ou reutilização de equipamentos;
- 8 **Controles tecnológicos**

- 8.1 Dispositivos *endpoint* do usuário;
- 8.2 Direitos de acessos privilegiados;
- 8.3 Restrição de acesso à informação;
- 8.4 Acesso ao código-fonte;
- 8.5 Autenticação segura;
- 8.7 Proteção contra malware;
- 8.8 Gestão de vulnerabilidades técnicas;
- 8.9 Gestão de configuração;
- 8.10 Exclusão de informações;
- 8.11 Mascaramento de dados;
- 8.12 Prevenção de vazamento de dados;
- 8.13 Backup das informações;
- 8.14 Redundância dos recursos de tratamento de informações;
- 8.15 *Log*;
- 8.16 Atividades de monitoramento;
- 8.17 Sincronização do relógio;
- 8.18 Uso de programas utilitários privilegiados;
- 8.19 Instalação de software em sistemas operacionais;
- 8.20 Segurança de redes;
- 8.21 Segurança dos serviços de rede;
- 8.22 Segregação de redes;
- 8.23 Filtragem da web;
- 8.24 Uso de criptografa;
- 8.25 Ciclo de vida de desenvolvimento seguro;
- 8.26 Requisitos de segurança da aplicação;
- 8.27 Princípios de arquitetura e engenharia de sistemas seguros;
- 8.28 Codificação segura;
- 8.29 Testes de segurança em desenvolvimento e aceitação;
- 8.30 Desenvolvimento terceirizado;
- 8.31 Separação dos ambientes de desenvolvimento, teste e produção;
- 8.32 Gestão de mudanças;

- 8.33 Informações de teste;
- 8.34 Proteção de sistemas de informação durante os testes de auditoria.

A norma NBR ISO/IEC 27005 (ABNT, 2023) fornece orientações para a gestão de riscos de segurança da informação. Ela descreve um processo sistemático para identificar, analisar e avaliar os riscos de segurança da informação, a fim de tomar decisões informadas sobre a implementação de controles de segurança. A norma 27005 é uma ferramenta essencial para ajudar a organização a entender e tratar os riscos relacionados à segurança da informação de forma eficaz.

A norma NBR ISO/IEC 27032 (ABNT, 2022) fornece diretrizes específicas para proteção da informação em ambientes de computação em rede. Seu conteúdo aborda os desafios e riscos relacionados à segurança cibernética e oferece orientações para a implementação de medidas adequadas de segurança cibernética.

2.3.6.2. NIST CSF

O *National Institute of Standards and Technology*, NIST, é uma agência do governo dos Estados Unidos, parte do Departamento de Comércio dos EUA[8]. O NIST é responsável por promover a inovação e a competitividade industrial por meio do avanço da ciência, da tecnologia e da metrologia. A agência é reconhecida internacionalmente por suas contribuições no desenvolvimento de padrões e diretrizes em diversas áreas, incluindo segurança da informação e segurança cibernética.

O NIST emite uma longa série de normativos de segurança da informação e cibernética, sendo de especial importância, dada a sua larga aplicação em organizações governamentais, bancárias, privadas, indústria e em produtos comerciais, tal como o *Framework for Improving Critical Infrastructure Cybersecurity* ou *NIST Cybersecurity Framework* - NIST CSF (NIST, 2018).

[8] https://www.commerce.gov/bureaus-and-offices/nist, acessado em 06/11/2023.

O NIST *Cybersecurity Framework* (NIST CSF) é composto por cinco funções principais, que representam as etapas do ciclo de vida de gerenciamento de riscos cibernéticos. Cada função é subdividida em categorias, 23 no total, que representam as áreas de foco dentro de cada função, e essas categorias, por sua vez, são subdivididas em subcategorias, totalizando 108, que especificam recomendações a serem consideradas para alcançar os objetivos de segurança cibernética. As funções que integram todos os controles são ordenadas nas categorias: identificar, proteger, detectar, responder e recuperar.

2.3.6.3. MITRE

O MITRE ATT&CK® (*Adversarial Tactics, Techniques, and Common Knowledge*)[9] é uma base de conhecimento e uma estrutura de referência amplamente reconhecida para entender e descrever as táticas, técnicas e procedimentos (TTP) usados por agentes de toda ordem (criminosos, ativistas, militares, agentes de inteligência, terroristas, dentre outras possibilidades) que realizam ataques cibernéticos. Foi desenvolvido pela organização sem fins lucrativos MITRE Corporation (MITRE, 2023).

O objetivo do MITRE ATT&CK é fornecer um vocabulário comum e uma estrutura padronizada para descrever as etapas e as técnicas utilizadas em diferentes fases de um ataque cibernético. O comportamento de atacantes cibernéticos é mapeado em várias etapas do ciclo de vida de um ataque, desde a etapa de preparação até o vazamento de dados.

O MITRE ATT&CK organiza as táticas e técnicas em uma matriz, conhecida como Matriz ATT&CK. A matriz é dividida em duas dimensões principais: (i) Táticas (quatorze no total), as quais representam as intenções ou objetivos gerais dos atacantes, incluindo categorias como Reconhecimento, Acesso Inicial, Escalação de Privilégios, Defesa Evasiva, dentre outras; (ii) Técnicas (227 no total, cada qual subdividida em subtécnicas): ações específicas realizadas por atacantes para alcançar suas metas dentro de cada tática. Cada técnica é uma descrição detalhada de uma ação específica executada pelos atacantes. Exemplos de técnicas incluem *phishing* (engenharia social realizadas

[9] https://attack.mitre.org/, acessado em 05/11/2023.

frequentemente por e-mail) e *exploitation* (uso de programas de computador maliciosos que exploram vulnerabilidades específicas de seus alvos), entre outras.

Além disso, o MITRE ATT&CK também categoriza as técnicas em diferentes grupos de atacantes, fornecendo indícios sobre os perfis e comportamentos de autores de ataques.

O MITRE ATT&CK é amplamente utilizado pela comunidade de segurança cibernética, empresas e organizações governamentais para melhor compreender os ataques cibernéticos, desenvolver estratégias de defesa e realizar análises de ameaças. Ele auxilia na detecção e resposta a incidentes de segurança, permitindo que as organizações se preparem e se defendam de forma mais eficaz contra ameaças cibernéticas.

2.3.6.4. CIS

O CIS (*Center for Internet Security*) é uma organização sem fins lucrativos amplamente reconhecida que oferece diretrizes e controles de segurança cibernética para ajudar organizações a protegerem seus sistemas, redes e dados contra ameaças cibernéticas. O padrão CIS é baseado em práticas recomendadas e medidas de segurança atualizadas.

O padrão CIS aborda diversos aspectos da cibersegurança, desde o levantamento de inventário de ativos de *software* e *hardware* até a proteção contra *malware*, gerenciamento de vulnerabilidades e detecção de intrusões. O *framework* é dividido em várias categorias e subcategorias, cada uma com uma série de controles que devem ser implantados para mitigar riscos e fortalecer a postura de segurança.

O padrão CIS possui 18 categorias principais na última versão à época da redação desta tese, quais sejam: (i) Inventário e Controle de Ativos Corporativos; (ii) Inventário e Controle de Ativos de Software; (iii) Proteção de Dados; (iv) Configuração Segura de Ativos Corporativos e Software; (v) Gerenciamento de Contas; (vi) Gerenciamento de Controle de Acesso; (vii) Gerenciamento Contínuo de Vulnerabilidades; (viii) Gerenciamento de Logs de Auditoria; (ix) Proteções de Email e Navegador da Web; (x) Defesas contra

Malwares; (xi) Recuperação de Dados; (xii) Gerenciamento de Infraestrutura de Rede; (xiii) Monitoramento e Defesa de Rede; (xiv) Conscientização e Treinamento em Segurança; (xv) Gerenciamento de Provedores de Serviços; (xvi) Segurança de Software de Aplicação; (xvii) Gerenciamento de Resposta a Incidentes; (xviii) Teste de Penetração.

2.3.6.5. Outros Padrões e *Frameworks*

Os padrões sobre os quais foram discorridas algumas das suas características neste texto estão entre os mais utilizados no Brasil e no mundo atualmente. Existem outros padrões, conjuntos de boas práticas ou *frameworks* de uso corrente que diferem dos apresentados, em geral, por escopos bem mais específicos, porém, mantendo uma forte compatibilidade com os apresentados. Dessa forma, outros padrões ou *frameworks* serão omitidos sem prejuízos para a pesquisa.

Alguns exemplos de relevância são: (i) SANS *Critical Security Controls* (SANS Top 20); (ii) OWASP (*Open Web Application Security Project*); (iii) COBIT (*Control Objectives for Information and Related Technologies* – embora este *framework* não seja de segurança cibernética, envolve fortemente o tema pelo viés da segurança da informação); (iv) *Cyber Kill Chain*, desenvolvido pela *Lockheed Martin*; (v) *Cyber Threat Intelligence* (CTI) *Framework*; além de outros.

Especial atenção deve ser dada aos ambientes industriais. Em geral esses ambientes utilizam equipamentos de comando e controle das linhas de produção de um ambiente industrial ou de plantas de produção, controle de energia, como hidrelétricas, usinas nucleares ou de produção e distribuição de energia elétrica. Essa atenção especial se faz pertinente por dois fatores: (i) em geral, os equipamentos de tecnologia da informação que comandam os equipamentos industriais são simplórios ou muito antigos se comparados aos mais simples computadores pessoais, o que os faz alvos mais fáceis de comprometer; (ii) no caso das plantas industriais consideradas críticas para um país, tais como as de distribuição de energia elétrica, o seu comprometimento pode até mesmo comprometer a segurança nacional, o que as faz ter uma designação especial chamada infraestrutura crítica.

Os *frameworks* já citados são compatíveis com os ambientes industriais, ainda que precisem ser particularizados ou adaptados em alguns controles e dependendo das instalações nas quais são aplicados. Por outro lado, há padrões de segurança específicos para esses ambientes. Um exemplo de referências para segurança cibernética nesses ambientes é a série ISA/IEC 62443[10]. Este é um conjunto de padrões desenvolvido pela Sociedade Internacional de Automação (ISA) e pela Comissão Eletrotécnica Internacional (IEC). O ISA/IEC 62443 fornece uma estrutura abrangente para a segurança de sistemas de automação e controle industrial. Ele define requisitos de segurança, práticas recomendadas e diretrizes para proteger sistemas e redes industriais contra ameaças cibernéticas.

As tecnologias operacionais (*operational technology* - OT), como são conhecidas as tecnologias de plantas industriais, se comparadas às tecnologias da informação, evoluíram pouco em relação à segurança cibernética, apesar de, em muitos casos, serem de altíssima criticidade devido aos reflexos extensos do seu comprometimento. Com o avanço cada vez maior da convergência entre redes de TI e OT, mais vias de ataques a esses ambientes surgem, o que vem possibilitando ataques severos a plantas industriais, tais como o notório caso *stuxnet.* O *Stuxnet* é um *worm* (tipo de software malicioso) usado para comprometer o processo industrial de enriquecimento de urânio no Irã, tendo uma das descrições do ataque e descoberta contida em um dossier da empresa Symantec[11].

2.3.7. Times de Respostas a Incidentes de Rede e Tratamento de Incidentes de redes de computadores

Os times de respostas a incidentes de rede têm especial importância nesta pesquisa uma vez que fornecem processos de detecção, investigação, interpretação e orientação sobre incidentes ocorridos ou tendências de riscos. Além disso, possuem processos de compartilhamento de informação preciosos

[10] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards, acessado em 05/11/2023.

[11] https://web.archive.org/web/20191104195500/https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf, acessado em 05/11/2023.

para diminuir os riscos das redes por eles vigiadas e estatísticas dos principais ataques e ameaças cibernéticas correntes. Esses times são conhecidos pela expressão em inglês *Computer Security Incident Response Teams* (CSIRT).

Um CSIRT é uma equipe responsável por lidar com incidentes de segurança cibernética e mitigar seus impactos. Esses times são compostos por especialistas em segurança da informação e cibernética, cuja função principal é detectar, analisar e responder a incidentes de segurança em sistemas computacionais.

As funções dos CSIRT são variadas conforme a necessidade do contexto em que é implementado, pois podem variar desde pequenas estruturas inseridas em uma organização até times que monitoram países ou regiões ainda mais abrangentes. Apesar desse largo espectro de variedades, há diversas funções comuns entre eles. Alguns exemplos são:

a) Monitoramento e detecção de incidentes de segurança: Os CSIRT empregam técnicas avançadas de monitoramento para identificar atividades maliciosas ou anômalas em sistemas de informação.

b) Resposta a incidentes: Os CSIRT atuam rapidamente para conter e neutralizar os incidentes de segurança, ainda que não seja da competência do CSIRT atuar diretamente no problema, podendo acionar outras equipes ou instituições com tal atribuição, minimizando o impacto nos sistemas e na organização.

c) Análise forense: Os CSIRT conduzem investigações técnicas detalhadas para determinar a origem e a extensão dos incidentes de segurança, coletando evidências para análise posterior.

d) Comunicação e coordenação: Os CSIRT colaboram com partes internas e externas, compartilhando informações relevantes e coordenando esforços de resposta conjunta.

Especial importância tem o processo de tratamento de incidentes de segurança computacional adotado por esses times. O CERT.br [12]provê cursos de capacitação para tratamentos de incidentes, além de outros cursos e eventos

[12] https://cert.br/, acessado em 05/11/2023.

para segurança da informação. O CERT.br é o principal CSIRT brasileiro e segue os padrões do CERT/CC[13] da *Carnegie Mellon University*, primeiro dos CSIRT e referência mundial. Uma descrição adaptada, a partir de publicações do CERT.br, de pontos comuns entre os CSIRT no que diz respeito ao processo e tratamento de incidentes de segurança computacional é a seguinte:

a) **Detecção e Triagem**

O processo começa com a detecção de um incidente de segurança. Isso pode ser feito por meio de sistemas de monitoramento, detecção de intrusões, alertas de segurança, relatos de usuários ou outras fontes de informação. Os incidentes são triados para determinar sua gravidade e prioridade. Para lidar objetivamente com a percepção de eventos de segurança que possam vir a ser considerados incidentes, as melhores práticas de segurança recomendam o uso de parâmetros chamados de indicadores de comprometimento (IOC), na sua forma reativa, e indicadores de ataque (IOA), na sua forma proativa. Em última instância, esses indicadores informam possíveis violações de segurança cibernética por meio da identificação de possíveis comprometimentos ou quebra da integridade, da confidencialidade ou disponibilidade dos dados relevantes para a organização, ou, ainda, da quebra da autenticidade no processo de identificação da entidade que acessa esses dados.

b) **Coleta de Informações**

Após a triagem, o CSIRT coleta informações relevantes sobre o incidente. Isso inclui registros de eventos, *logs* do sistema, dados de tráfego de rede, capturas de tela, arquivos maliciosos ou qualquer outra evidência relacionada ao evento. A coleta de informações é fundamental para entender a natureza e a extensão do incidente.

c) **Análise e Investigação**

Nesta etapa, os especialistas do CSIRT analisam as informações coletadas para compreender a causa raiz do incidente. Eles examinam os padrões de atividade, identificam as vulnerabilidades exploradas, examinam os artefatos maliciosos e realizam investigações forenses digitais, se necessário. A

[13] https://sei.cmu.edu/about/divisions/cert/index.cfm, acessado em 06/11/2023.

análise visa determinar o escopo do incidente, identificar os sistemas afetados e avaliar os riscos envolvidos.

d) **Classificação e Priorização**

Com base nos resultados da análise, os incidentes são classificados e priorizados de acordo com sua gravidade, impacto e urgência. Isso permite que o CSIRT aloque recursos adequados para responder aos incidentes de maneira eficiente, dando prioridade aos incidentes mais críticos ou que afetem sistemas essenciais.

e) **Resposta e Mitigação**

Nesta fase, o CSIRT desenvolve e executa planos de resposta para conter o incidente e mitigar seus efeitos. Isso pode envolver a remoção de *malware*, o isolamento de sistemas comprometidos, a aplicação de *patches* de segurança, a alteração de senhas, a interrupção de atividades maliciosas, entre outras medidas. O objetivo é restaurar a normalidade e minimizar o impacto do incidente.

f) **Documentação e Relatórios**

Durante todo o processo de análise de incidentes, é essencial manter registros detalhados das ações realizadas, das descobertas feitas e das lições aprendidas. Essa documentação é valiosa para fins de análise pós-incidente, para aprimorar os controles de segurança e para fornecer informações úteis em futuros incidentes similares. Também pode ser necessário gerar relatórios para comunicação interna, parceiros de negócios ou autoridades reguladoras, dependendo da natureza do incidente.

Diversos são os CSIRT de relevância internacional, cujo trabalho tem repercussões em todo o globo. Alguns exemplos de grande relevância são:

a) US-CERT[14] (*United States Computer Emergency Readiness Team*): O CSIRT dos Estados Unidos é conhecido por sua expertise e colaboração com organizações públicas e privadas no combate a ameaças cibernéticas.

[14] https://www.cisa.gov/, acessado em 06/11/2023.

b) JPCERT/CC (*Japan Computer Emergency Response Team Coordination Center*): O JPCERT/CC é um dos principais CSIRT asiáticos, focado na resposta a incidentes de segurança cibernética no Japão e na região da Ásia-Pacífico. O centro desempenha um papel crucial na proteção das infraestruturas digitais japonesas, trabalhando em estreita colaboração com organizações governamentais, empresas e outros CSIRT internacionais. O JPCERT/CC[15] também desempenha um papel ativo na pesquisa de ameaças cibernéticas emergentes, fornecendo orientações e melhores práticas de segurança para a comunidade de TI.

Sobre o trabalho conjunto desses times, especial destaca dá-se ao FIRST[16] (*Forum of Incident Response and Security Teams*). Trata-se de uma organização global que reúne CSIRT de diversas partes do mundo, promovendo o compartilhamento de melhores práticas e coordenação em incidentes de segurança.

A atuação dos CSIRT pelo mundo aumenta em muito a consciência do que se passa no espaço cibernético por parte dos administradores do próprios CSIRT ou dos administradores de redes organizacionais ligadas a esses CSIRT. Essa consciência de cada gestor diminui em muito o risco a que essas redes estão submetidas, pois, em particular pelo compartilhamento das informações sobre incidentes entre esses times, os gerentes das redes desse universo podem, proativamente, tomar medidas que tornem imunes os seus ambientes digitais para ataques conhecidos e mantendo assim uma consciência situacional sobre o espaço cibernético mais elevada.

O aspecto da consciência situacional sobre o espaço cibernético é essencial para mitigar as os riscos a que esse espaço está submetido. No subtítulo 2.4, o tema é explorado conforme as necessidades deste trabalho de pesquisa.

[15] https://www.jpcert.or.jp/english/, acessado em 06/11/2023.
[16] https://www.first.org/, acessado em 06/11/2023.

2.4. CONSCIÊNCIA SITUACIONAL

2.4.1. Consciência Situacional em Ambientes Dinâmicos

O entendimento do que ocorre no ambiente no qual se vive sempre foi uma necessidade humana, chegando mesmo, em tempos primordiais, a ser uma exigência da vida diária a ser satisfeita para se garantir a sobrevivência. Da consciência adquirida do que era dado da realidade, passava-se à ação, de acordo com a necessidade específica do momento. Desse modo, desde a mais remota história da humanidade, a consciência do que se passa e o consequente desenvolvimento da capacidade de decidir como reagir conforme as circunstâncias acompanhou o desenvolvimento do ser humano.

As guerras figuram dentre os eventos históricos que sempre requereram uma preparação sistemática para a tomada de consciência sobre o estado e a evolução da situação corrente. Num campo de batalha, os comandantes precisavam estar munidos de conhecimento, lições aprendidas, experiências tanto pessoais quanto de outros comandantes, além de virtudes diversas para que, confrontados a toda sorte de dados advindos da contenda, em particular dos não raros imponderáveis acontecimentos dos combates, fossem capazes de perceber com clareza o que era relevante, conjugar e interpretar essas percepções, conjecturar evoluções possíveis e decidir.

Essa necessidade de formar significado e construir conhecimento a partir dos dados da realidade e de esquemas mentais adquiridos previamente é corroborada por clássicos das artes militares como se vê nas inúmeras transcrições da milenar obra “A Arte da Guerra”, de Sun Tzu, tais como em Cardoso (2005) ou em compilações do livro “Da Guerra”, elaborada no século 19, de Clausewitz (1979).

Em tempos recentes, notadamente a partir do século XX e impulsionados pelos desenvolvimentos tecnológico e das capacidades administrativas para a indústria, várias áreas relacionadas aos processos de percepção e compreensão de eventos correntes passaram a ser objeto de atenção acadêmica, em especial voltadas para a tomada de decisões. Um desses campos, mostrou-se de especial interesse da área militar foi o da Consciência Situacional (CS).

Na documentação doutrinária militar brasileira, o termo “consciência situacional” é definido no Glossário das Forças Armadas como segue:

> CONSCIÊNCIA SITUACIONAL - Percepção precisa dos fatores e condições que afetam a execução da tarefa durante um período determinado de tempo, permitindo ou proporcionando ao seu decisor, estar ciente do que se passa ao seu redor e assim ter condições de focar o pensamento à frente do objetivo. É a perfeita sintonia entre a situação percebida e a situação real. (Brasil, 2015, p. 64).

De especial importância para entendimento do campo da consciência situacional para ambientes dinâmicos e complexos são os trabalhos da pesquisadora Mica Endsley (Endsley,1988, 1990, 1993, 1995 e 2001), em particular um artigo usado como seminal para diversas pesquisas na área (Endsley, 1995, p. 32-64), no qual a cientista provê uma valiosa série de conhecimentos sobre o tema, além de propor um modelo sobre o assunto. Como definição sobre o que é a consciência situacional, Endsley (1995) enuncia o seguinte:

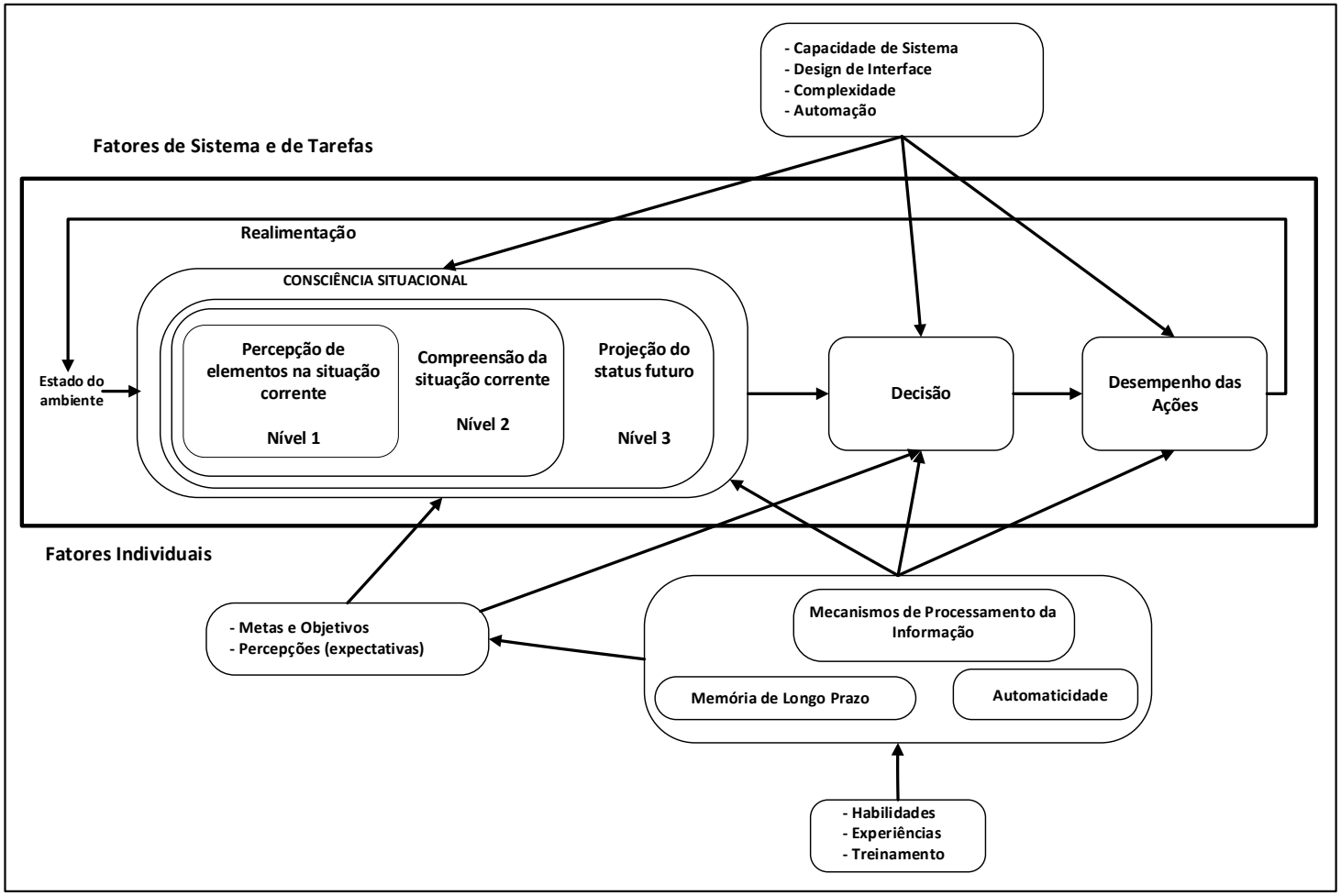
> A consciência situacional é a percepção dos elementos do ambiente durante um certo intervalo de tempo e num determinado espaço, a compreensão de seu significado e a projeção de seu estado no futuro próximo." (Endsley, 1995, p.36)[17]

Endsley propõe o modelo representado na Figura 28 para consciência situacional em ambientes dinâmicos.

De modo esclarecer os elementos fundamentais do modelo, o Quadro 1 resume a terminologia e seu significado.

[17] *Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*. (ENDSLEY, 1995, p.36)

Figura 28 - Modelo de Consciência Situacional para tomada de decisão dinâmica



Fonte: Endsley (1995, p. 35), traduzido para o português.

Quadro 1 - Significado dos termos empregados no modelo de CS de Endsley (1995, p. 35)

TERMO	SIGNIFICADO
FATORES DE SISTEMA OU TAREFA	Conjunto de tarefas e de elementos (fatores) que integram a conjunção entre os processos de Consciência Situacional, Tomada de Decisão e execução das ações.
Capacidade do Sistema	Capacidade para captar e processar os dados necessários à consciência situacional.
Projeto de Interface	Forma de provimento e aspecto da informação que é apresentada ao decisor por sistema automatizado.
Estresse	Fatores que são percebidos como ameaçadores ou perigosos.
Carga de trabalho	Demandas existentes para um operador num contexto para a qual é requerido que ele obtenha consciência situacional
Complexidade	Característica do contexto em relação ao qual se deseja alcançar a consciência situacional, que é diretamente proporcional ao número de elementos existentes, suas relações e dinâmicas.
Automação	Grau que sistemas possam operar sem intervenção humana.
Estado do Ambiente	Coleção de elementos relevantes do ambiente observado e sua dinâmica.
CONSCIÊNCIA SITUACIONAL	Processo por meio do qual se pode perceber e identificar os elementos de interesse e suas dinâmicas no ambiente; compreender como se combinam e se relacionam os elementos identificados; projetar possíveis evoluções da situação desses elementos.
Percepção	Captação do estado, dos atributos e da dinâmica dos elementos de relevância do ambiente observado.
Compreensão	A partir da consideração dos elementos captados durante a percepção, compreender suas relevâncias individuais e em conjunto à luz dos objetivos que envolvem o operador.
Projeção	Exercício da capacidade de conjecturar possíveis evoluções futuras para os quais a situação foi interpretada na fase de compreensão.
Decisão	Escolha de alternativa dentre opções advindas da Consciência Situacional.
Performance de ações	Realização no mundo físico de tarefas que concretizam as decisões.
Feedback	Efeito de aprendizado ou de novos elementos que realimentam o processo de consciência situacional advindos dos efeitos das ações executadas no ambiente físico.
FATORES INDIVIDUAIS	Fatores inerentes à condição humana no que diz respeito a características individuais na área cognitiva, emocional, experiência acumulada e possíveis outros aspectos particulares do operador de quem se espera alcançar a consciência situacional em um contexto.
Metas e Objetivos	Parâmetros estabelecidos *a priori* em relação a uma situação a ser observada.
Preconcepções	Expectativas prévias em relação a um tipo de situação.
Mecanismos de Processamento de Informação	Forma particular de um indivíduo gerir informações a que tem acesso ou busca.

TERMO	SIGNIFICADO
Memórias de longa duração	Conjunto informações, conhecimentos e mecanismos mentais necessários para recuperá-los frente a uma necessidade que um indivíduo pode contar para perceber, compreender e projetar situações.
Automaticidade	Processo automatizado pelo qual se pode executar etapas da consciência situacional de forma imediata ou com menos ou nenhum subprocesso de interpretação a respeito da situação corrente.
Habilidades	Características próprias do operador.
Experiência	Referências de vivências anteriores do operador aplicáveis à situação corrente.
Treinamento	Aprendizado de estratégias previamente organizadas e ensinadas por terceiros e relacionadas às possíveis situações a serem observadas.

Fonte: o autor.

Neste ponto, convém esclarecer alguns pormenores do encadeamento dos elementos que compõem o modelo de Endsley, o qual está centrado nos estágios (níveis) do processo da consciência situacional: a percepção, a compreensão e a projeção.

2.4.2. Percepção

O primeiro estágio da consciência situacional, segundo Endsley (1995, p. 36), é a percepção. Neste contexto, O estágio de Percepção é o ato de notar o estado, os atributos e a dinâmica dos elementos relevantes do ambiente. A capacidade de perceber o que é relevante no ambiente pode ser influenciada por vários fatores. Endsley (1995, p.40-42) destaca o processamento pré-atenção, a Atenção e as Memórias de Trabalho e de Longo Prazo.

O processamento de pré-atenção busca notar no ambiente observado características dos elementos que compõem esse ambiente e que chamam a atenção para eles. Exemplos utilizados nos sistemas de monitoração do espaço cibernético das redes de computadores são das cores dos ícones representativos de equipamentos críticos que se tornam amarelos ou vermelhos indicando imediatamente ao operador uma anomalia que merece a atenção em curto prazo ou mesmo imediata.

A Atenção é um aspecto humano que está presente em praticamente todos os estágios, seja da consciência situacional, seja da tomada de decisão e de ações. Esse aspecto está voltado para a capacidade humana de se focar em

um objeto de interesse e, deste modo, acompanhar a dinâmica desse objeto no tempo. A complexidade de um sistema que é observado, em particular no que diz respeito à variedade de aspectos dos seus elementos, quantidades e dinâmicas é um fator de dispersão para a Atenção. Outros aspectos entrelaçados à Percepção são a Memória de Trabalho e a Memória de Longo Prazo. Por estarem presentes nos outros estágios do processo de consciência situacional, esses aspectos são explorados no subtítulo 2.4.3 a seguir.

2.4.3. Compreensão

A Compreensão da situação corrente está baseada numa síntese formada na mente do operador a partir dos elementos desconexos captados no nível 1, ou seja, na Percepção (Endsley, 1995, p. 37). A compreensão desses elementos se processa sempre à luz dos objetivos da observação.

De forma similar à Atenção, a Memória de Trabalho age em todos os estágios do modelo de Endsley, conforme se pode observar na Figura 28. Esse aspecto da natureza da mente humana deve processar as observações feitas no nível 1, novas informações que se apresentam no decorrer do tempo, conhecimentos aprendidos previamente e evocados conforme a necessidade da situação corrente. Em outras palavras é o aspecto da mente humana que Endsley destaca como sendo o elemento responsável por estruturar um raciocínio lógico entre premissas e inferências sobre desdobramentos que viabilizarão as decisões e ações decorrentes (Endsley, 1995, p. 43).

De modo análogo ao que ocorre à Atenção e à Memória de Trabalho, a Memória de Longo Prazo está presente em todos os estágios representados na Figura 28. A Memória de Longo Prazo, conforme sugere Endsley (1995, p.43) age como um repositório de onde a mente humana pode recuperar conhecimentos dominados os quais desempenham papel fundamental no reconhecimento de padrões, estabelecimento de categorizações, aplicação de regras, técnicas e controles, além de diversos outras possibilidades de consubstanciar o uso de conhecimentos em relação à situação corrente.

Especial destaque Endsley dá a três elementos no contexto da Memória de Longo Prazo: *scripts***,** *schematas* e modelos mentais (Endsley, 1995, p. 43).

Schematas são estruturas de representação sob as quais sistemas de informação, mesmo os complexos, podem ser interpretados e representados de modo simplificado. Na sua descrição desse elemento, Endsley (1995, p.43) utiliza termo da língua inglesa *framework*, que frequentemente é utilizado em português sem ser traduzido, na acepção de um modelo esquemático de referência para se avaliar em algum grau uma dada situação ou orientar ações para lidar de modo mais acertado, conforme o conhecimento embutido no *framework*, com algum contexto a ser conduzido ou gerido.

Uma forma simplificada de s*chemata* é o *script*. Para descrever o s*cript,* Endsley lança mão da definição de Schank e Abelson (1977, apud Endsley, 1995, p. 43) de que s*cripts* proveem sequências de ações apropriadas para diferentes tipos de desempenho de tarefa. *Schematas* e *scripts* facilitam em muito a tomada de consciência situacional, pois diminuem a necessidade de o operador fazer inferências sobre as informações advindas do ambiente e sobre as quais deverá alcançar consciência situacional, decidir e agir.

Na definição de Modelos Mentais, Endsley se vale do que Rouse e Morris (1985, apud Endsley, 1995, p. 43) estabelecem, ou seja, Modelos Mentais são mecanismos por meio dos quais indivíduos são capazes de gerar descrições da forma e do propósito de sistemas, explicações sobre o seu funcionamento e os seus estados observados e, por fim, de predições dos seus estados futuros. Dessa descrição, Endsley infere que modelos mentais podem ser descritos como *Schematas* complexos que são usados para modelar o comportamento de sistemas.

Endsley dedica especial atenção ao uso de modelos mentais no alcance da Consciência Situacional, pois a partir deles, em tese, pode-se obter: (i) conhecimento dos elementos relevantes do sistema que podem ser usados no direcionamento da atenção e na classificação da informação usada durante a Percepção; (ii) meios de integração dos elementos para formar o entendimento do seu significado; (iii) um mecanismos de projeção de estados futuros, tomando por base o estado corrente e sua dinâmica (Endsley, 1995, p. 44).

2.4.4. Projeção

O nível 3 da Consciência Situacional é constituído pela habilidade de projetar as ações dos elementos do ambiente, no mínimo, no curto prazo, e é referido como Projeção. Esse estágio da Consciência Situacional é atingido como consequência direta do conhecimento do estado e da dinâmica dos elementos do ambiente e da compreensão da situação corrente (Endsley, 1995, p.37).

Como aludido nos tópicos sobre Percepção e Compreensão, no estágio da Projeção os aspectos de Atenção, Memória de Trabalho e Memória de Longo Prazo são intensamente evocados. A Figura 29 sintetiza o processo.

2.4.5. Objetivos

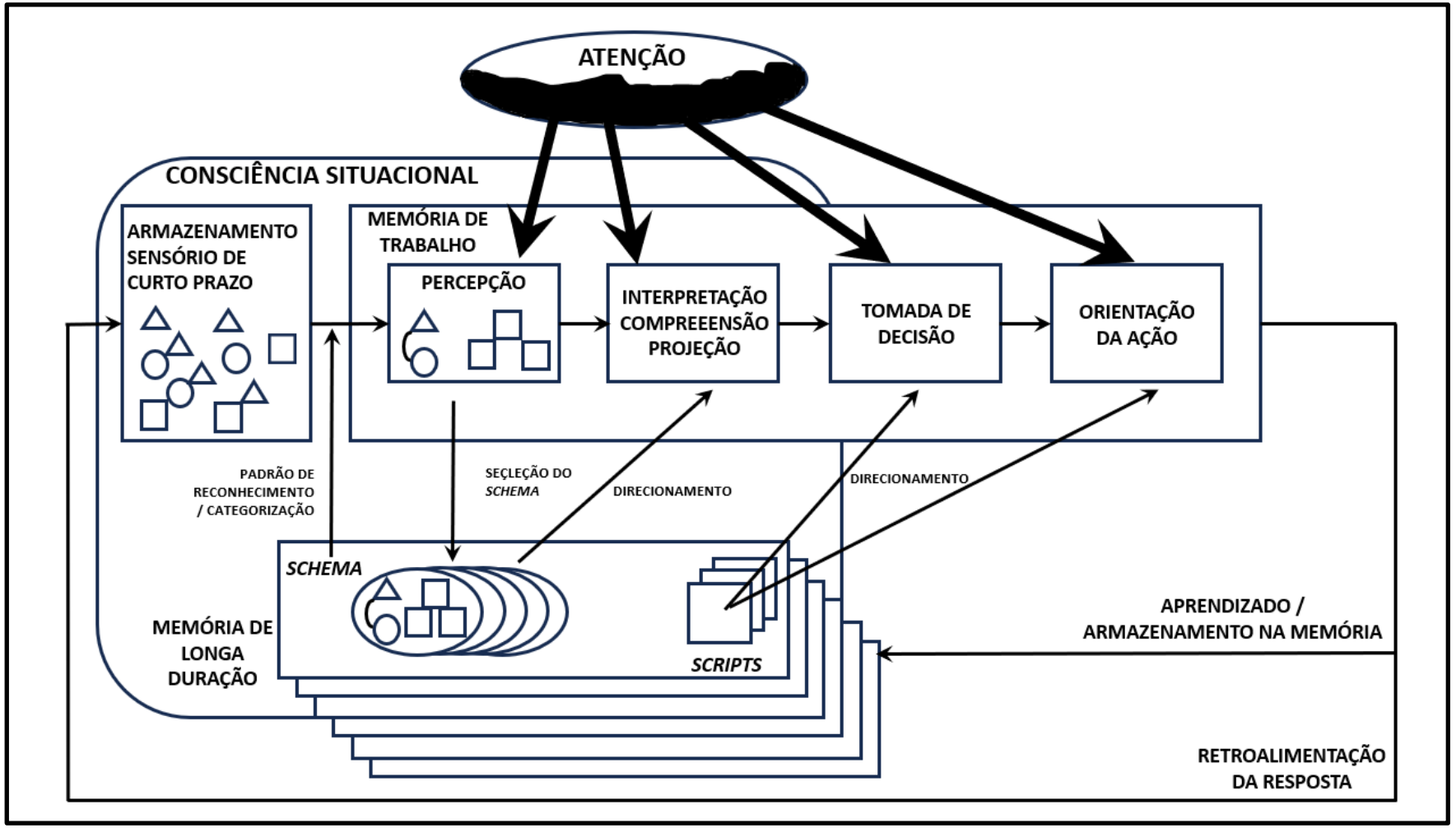
A respeito da aplicação do seu modelo, Endsley enfatiza a importância central dos objetivos a serem alcançados no contexto no qual é necessária a tomada de consciência situacional (Endsley, 1995, p. 47). Em consequência, toda a cadeia de eventos que levam à Consciência Situacional, além da tomada de decisão e realização das ações é influenciado pelos objetivos a serem atingidos.

Toda essa influência dos objetivos pode ocorrer de dois modos diferentes. Um deles constitui uma abordagem *top-down,* enquanto o outro advém de um processo *bottom-up*.

Na possibilidade do processo de ser *top-down*, toda a sequência de eventos para alcançar a consciência situacional são desenvolvidos sob a luz dos objetivos primordiais da tarefa em execução. Aspectos tais como quais modelos mentais devem ser evocados e que *schematas* devem ser empregados são diretamente influenciados.

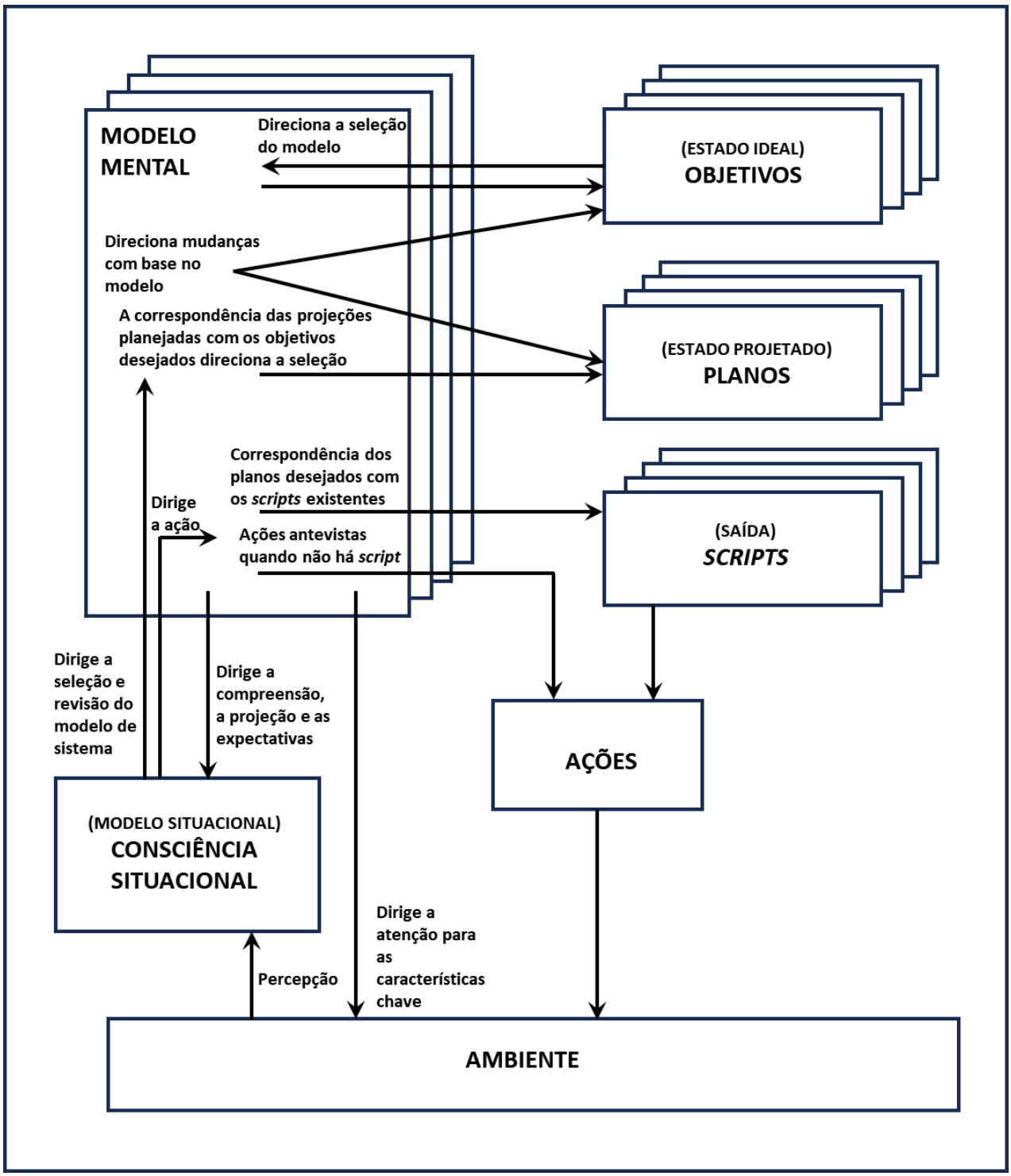
A possibilidade de o processo ser *bottom-up* surge quando o retorno dos resultados das ações sobre a realidade demonstra algum nível de ineficácia, provocando mudanças nos objetivos e planos originais, assim como a alternância de modelos mentais a serem empregados ou s*chematas*. A Figura 30 representa de forma esquemática ambas as possibilidades.

Figura 29 – Mecanismos de Consciência de Situacional



Fonte: Endsley (1995, p. 41), traduzido para o português.

Figura 30 - Modelo de Consciência Situacional



Fonte: Endsley (1995, p. 48), traduzido para o português.

2.4.6. Consciência Situacional em Defesa Cibernética

O conceito de consciência situacional é utilizado em áreas diversas e um desses campos é o espaço cibernético. Embora, em si, se constitua um campo próprio, o espaço cibernético também é plataforma de sustentação para outros espaços. Em consequência, pode-se dizer que o exercício da observação do espaço cibernético para fins de desenvolvimento da consciência situacional a seu respeito está frequentemente condicionado a outros campos que esse espaço sustenta.

Como exemplos muito relevantes para os dias atuais, pode-se destacar o ambiente de negócios e gestão das organizações e o universo das operações militares. Por ser um campo inerentemente dinâmico e sujeito a uma massiva quantidade de dados a observar, o espaço cibernético faz com que os outros campos que suporta se tornem imensamente mais complexos para tomada de consciência situacional a seu respeito.

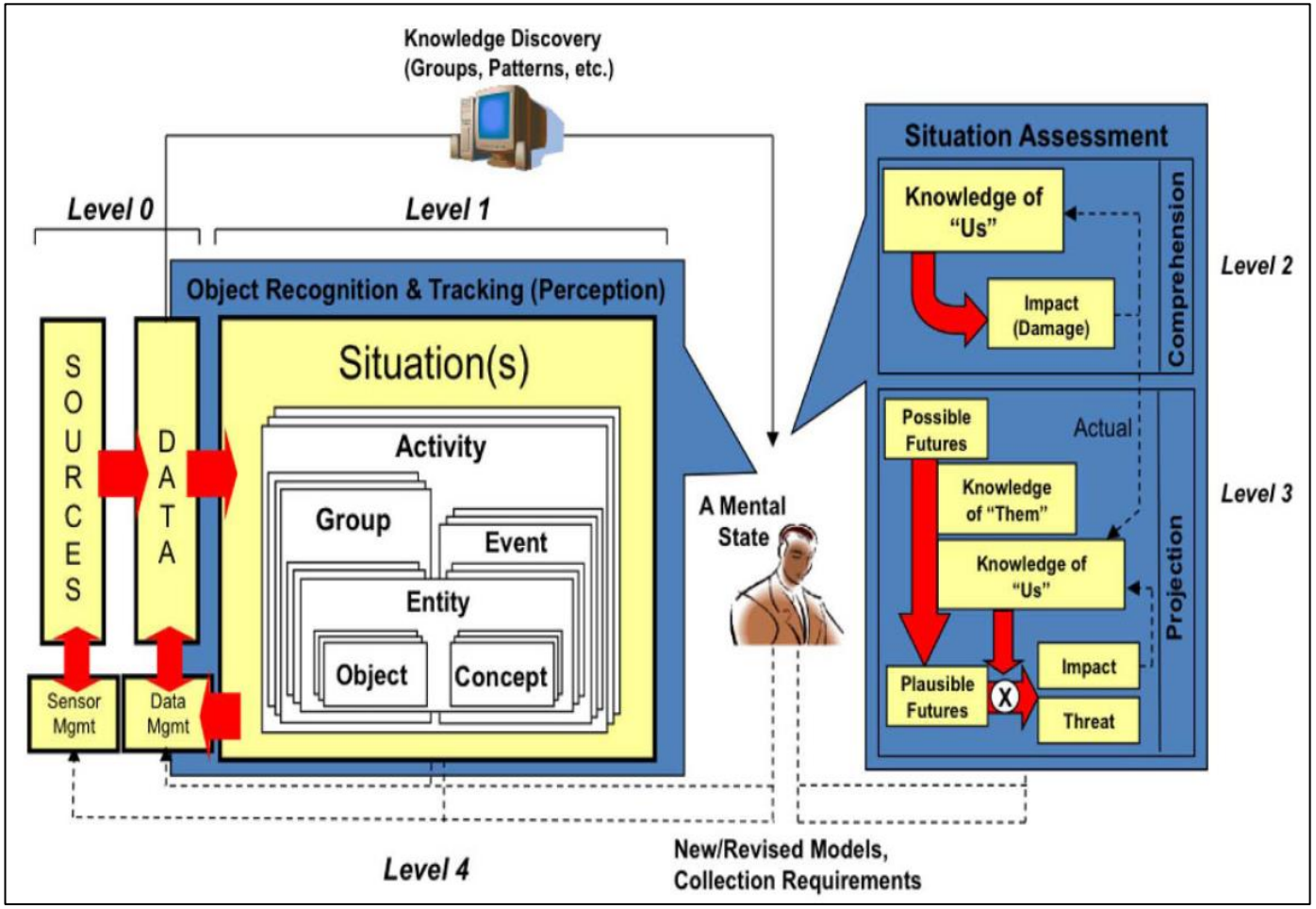
Para seus estudos para aplicação do conceito no contexto da defesa cibernética, Tadda e Salerno (2010, p.17) adaptam sutilmente a definição de Endsley (1995) da seguinte forma:

> Consciência situacional é a percepção dos elementos do ambiente dentro de um espaço e tempo específicos, a compreensão do significado desses elementos e a projeção de seu estado em um futuro próximo para possibilitar a superioridade na tomada de decisões. (Tadda E SALERNO, 2010, p.17)[18]

Assim, ao acrescentar o elemento de “superioridade de decisão”, os autores apontam para a necessidade de aumentar a probabilidade de que as decisões tomadas majoritariamente em dados advindos de sistemas digitais sejam mais precisas que a dos eventuais antagonistas no espaço cibernético. A representação dessa ideia pode ser observada no modelo de referência da Figura 31.

[18] *Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority.”* (TADDA E SALERNO, 2010, p.17)

Figura 31 - Modelo de referência de consciência situacional em defesa cibernética



Fonte: Tadda e Salerno (2010, p.20).

Segundo Barford *et al*. (2010, p. 3-5), a consciência situacional em defesa cibernética está associada a pelo menos sete aspectos: (i) a percepção da ocorrência de um ataque, seu tipo, fonte, alvo etc.; (ii) consciência do nível atual e possível desdobramento do impacto do ataque; (iii) consciência da evolução da situação; (iv) ciência do comportamento do adversário; (v) ciência do porquê e como a situação corrente foi causada; (vi) ciência da qualidade (confiabilidade) das informações coletadas e das decisões de inteligência que foram derivadas dessas informações; (vii) avaliação dos futuros plausíveis da situação corrente.

Esses aspectos podem ser reconhecidos em operações cibernéticas pela análise dos efeitos reais provocados sobre os ativos informacionais e não informacionais, por meio da aplicação das ações cibernéticas (Carneiro, 2012, p.120).

Barford *et al*. (2010, p. 4) ainda distribuem esses aspectos pelos níveis definidos por Endsley (1995) do seguinte modo:

- Percepção dos elementos do ambiente (nível1): aspectos (i) e (vi).
- Compreensão da situação corrente (nível2): aspectos (ii), (iv) e (v).
- Projeção de estados futuros (nível 3): aspectos (iii) e (vii).

Para a interpretação da Figura 31, são necessários definir os conceitos: objeto (*object*), entidade (*entity*), grupo (*group*), evento (*event*), atividade (*activity*), situação (*situation*) e avaliação de situação (*situation assessement*).

Entidade é definida como algo que tenha uma existência distinta e separada, ainda que não necessariamente material (Tadda e SALERNO, 2010, p. 20). Um exemplo de entidade é uma abstração jurídica, a qual, em si, embora não tenha existência material, tem significado aplicável à realidade.

Um **objeto** é uma entidade física, ou seja, algo que esteja ao alcance dos sentidos humanos (Tadda e SALERNO, 2010, p. 20).

Um **grupo** é um conjunto cujos elementos têm relação entre si (Tadda e SALERNO, 2010, p. 20). Por exemplo, grupos em uma organização.

Um **evento** é algo que ocorre num determinado tempo e local (Tadda e SALERNO, 2010, p. 21).

Uma **atividade** é algo realizado tal como uma ação ou movimento. Atividades são compostas por entidades ou grupos relacionados por um ou mais eventos no tempo ou espaço (Tadda e SALERNO, 2010, p. 21).

Uma **situação** é a visão de mundo pessoal de uma coleção de atividades das quais alguém está ciente em um determinado momento (Tadda e SALERNO, 2010, p. 21).

Avaliação de situação é uma avaliação quantitativa relacionada com noções de julgamento, maneiras de apreciação e relevância (BOSSE, ROY e WARK, apud Tadda e SALERNO, 2010, p. 22).

2.5. OBSERVAÇÕES FINAIS SOBRE A REVISÃO DE LITERATURA

Esta revisão de literatura buscou destacar os pontos da literatura técnica e científica que provessem os alicerces necessários à compreensão da tese proposta neste trabalho de pesquisa. As referências-chave foram destacadas no início da revisão, a teoria do conhecimento organizacional (Choo, 1998), e no seu fecho, o modelo de consciência situacional (Endsley, 1995).

De modo a possibilitar a amálgama desses elementos-chave, outros elementos complementares foram explanados, assim como algumas de suas perspectivas especializadas para fins da pesquisa. Assim, foi discorrido sobre gestão da informação e sua aplicação nas áreas de comando e controle militar, inteligência e guerra da informação.

Os conceitos de defesa cibernética e segurança da informação e cibernética foram estabelecidos concomitantemente, dada as suas interfaces. Foram explorados em maiores detalhes os aspectos de *frameworks* e normas, conhecidos como melhores práticas de segurança e os processos de trabalho dos times de resposta a incidentes de rede, uma vez que são, respectivamente, instrumentos de gestão do conhecimento e da informação, indo, portanto, ao encontro dos objetivos da pesquisa.

Por fim, no fecho do elemento-chave da consciência situacional, foi explanado sobre a sua aplicação para o espaço cibernético. Deste modo, buscou-se preparar o terreno do estudo para que sobre esses alicerces fosse

possível construir a plataforma do referencial teórico da tese, sobre a qual a metodologia da pesquisa será desenvolvida para realização do estudo a partir do capítulo seguinte.

3. REFERENCIAL TEÓRICO

O objetivo desta pesquisa visa propor um modelo de *framework* que, baseado na teoria e no processo que fundamentam uma organização do conhecimento (Choo, 1998, p.220), forneça um conjunto de elementos iniciais para a determinação das necessidades informacionais básicas à formação da consciência situacional em defesa cibernética, segundo modelo de Endsley (1995, p.34), adaptado por Barford *et al*. (2010, p. 3-5), aplicado no contexto da Defesa Nacional brasileira no seu nível estratégico.

Desse modo, é mister que os conhecimentos que suportam a pesquisa e que foram descritos no capítulo de revisão da literatura sejam ordenados adequadamente em um referencial teórico, o qual constituirá a ponte entre os conhecimentos que fundamentam a pesquisa, a metodologia de investigação e a construção do resultado do trabalho.

3.1. *FRAMEWORKS* E CICLO DO CONHECIMENTO ORGANIZACIONAL

No capítulo de revisão de literatura, foi feita uma explanação sobre *frameworks* de segurança da informação ou cibernética como sendo instrumentos de melhores práticas pelos quais é possível moldar, em certo grau, o comportamento de indivíduos para colaborar na efetivação dessas modalidades de segurança no ambiente organizacional, diminuindo os riscos inerentes a esses domínios. De modo análogo, a aplicação de *frameworks* viabiliza a realização de ataques cibernéticos de modo sistemático e gerenciável, quando se trata do aspecto ofensivo.

De acordo com o modelo da teoria que fundamenta uma organização do conhecimento utilizado nesta pesquisa, cada arena conta com elementos emocionais, cognitivos e situacionais. No modelo, esses elementos são reunidos respectivamente nas categorias **Cultura Organizacional**, **Teoria Adotada**, e **Teoria em Uso**, conforme Figuras 10, 11 e 12.

Ao mesmo tempo, por definição, os *frameworks* de segurança da informação ou cibernética são criados para: (i) sensibilizar as pessoas da organização a terem comportamentos favoráveis à segurança da informação ou

cibernética, o que, em graus variados, dependendo do nível de maturidade do processo de sensibilização na organização, atuará sobre as crenças, o conhecimento cultural e as preferências do pessoal, ou seja na **cultura organizacional**; (ii) referenciar a geração de normativos, diretrizes, além de outros instrumentos formais de definição de ações para a segurança da informação ou cibernética no nível institucional, o que leva a influenciar as interpretações, os conhecimentos explícitos gerados e as regras para aplicação da segurança, ou seja a **teoria adotada**; (iii) fomentar com que as maneiras operacionais de execução das regras e diretrizes institucionais a respeito da segurança cibernética sejam implementadas na prática de modo alinhado e agregando valor a essas regras e diretrizes, o que leva a se refletir na captação dos elementos informacionais, no conhecimento tácito e nas rotinas empregadas, ou seja, na **teoria em uso**.

Nesse sentido, uma constatação útil à pesquisa é que, nos *frameworks* de melhores práticas em segurança da informação, cibernética e defesa ativa, é possível identificar elementos ou efeitos de sua aplicação que potencializam a cultura organizacional (aspectos emocionais), a teoria adotada (aspectos cognitivos) e a teoria em uso (aspectos situacionais) em um ambiente organizacional voltado para a cibernética ou que dela dependa de forma crítica.

Isso abre a perspectiva de que é possível aplicar os *frameworks* de melhores práticas em segurança da informação, cibernética e defesa ativa como instrumentos que, incidentalmente, facilitam a formação de significado, a criação de conhecimento e a tomada de decisão. Em consequência, é possível rearranjar adequadamente os controles de um ou mais *frameworks* de segurança da informação e cibernética para que, numa nova ordenação, se obtenha um ou mais novos *frameworks* voltados especificamente para provocar a formação de significado, a criação de conhecimento e a tomada de decisão no domínio da cibernética.

3.2. *FRAMEWORKS* E TEORIA ADOTADA

A viabilidade da pesquisa depende da descoberta e realização do relacionamento entre o modelo de Choo (1998) e os *frameworks* de cibernética

selecionados e da ligação do resultado desse relacionamento com o modelo de Endsley (1995, p.35) adaptado para cibernética Tadda e Salerno (2010, p.20). Ademais, o *framework* a ser produzido como resultado da pesquisa deve ser um mecanismo que possa ser utilizado por pesquisadores e executores de operações cibernéticas, em particular na formação desses agentes e manutenção desse conhecimento nas organizações que realizam essas operações. Assim, esse conhecimento se torna útil para diversos indivíduos diferentes e no decorrer do tempo, quando devidamente atualizado.

Ao se verificar a natureza dos elementos que compõem as arenas do ciclo de conhecimento de Choo (1998, p.232), constatam-se as naturezas emocionais, cognitivas e situacionais, conforme Figura 7. A partir dessa constatação, é necessário verificar a compatibilidade entre a natureza do resultado ser alcançado na pesquisa, em forma de *framework*, e essas naturezas emocionais, cognitivas e situacionais. Nesse sentido, ressalta-se dois fatores fundamentais. O primeiro tem a ver com a natureza das estruturas utilizadas em *frameworks* ligados à cibernética e o segundo está relacionado com as interações mútuas entre os elementos que compõem cada arena, conforme constata Choo (1998, p. 241).

Sobre o primeiro fator aludido, como se registrou na revisão de literatura, é direto constatar que os *frameworks* de segurança da informação ou cibernética atuam como indutores de manifestações emocionais, cognitivas e situacionais para as aplicações da cibernética. Ao mesmo tempo, eles, em si, são conhecimentos registrados e passíveis de serem assimilados e aplicados por uma variedade de indivíduos em intervalos de tempo que podem alcançar anos, escala de tempo esta que, em geral, são usadas para atualizações desses *frameworks*.

Assim, em termos de estrutura e aplicação, os *frameworks* são majoritariamente correspondentes aos elementos cognitivos no modelo de Choo (1998, p. 239), pois seus componentes finais são regras e recomendações. Isso leva a suscitar que convém à pesquisa limitar a busca de componentes nos *frameworks* compatíveis com elementos de natureza cognitiva no modelo de Choo (1998, p. 239).

Sobre o segundo fator, é necessário salientar que, mesmo se considerando a busca de componentes dos *frameworks* compatíveis apenas com a teoria adotada da organização (reunião dos elementos cognitivos de cada arena), o *framework* produzido pela pesquisa, ao ser aplicado, se irradiará para os componentes emocionais e situacionais, conforme Choo (1998, p.241) demonstra em seu modelo, o que é corroborado pelos objetivos de concepção e as aplicações práticas desses instrumentos na cibernética.

3.3. ELOS PARA LIGAÇÃO ENTRE *FRAMEWORKS* E TEORIA ADOTADA

Neste estágio do referencial teórico, é necessário elucidar como se espera ser possível na pesquisa fazer o relacionamento entre os elementos da teoria adotada e os componentes dos *frameworks* analisados. Como primeiro passo, deve-se voltar às definições desses elementos, assim como, a partir da conceituação de cada um, estabelecer referências objetivas para reconhecimento do componente de *framework* relacionado. Desse modo, destacam-se as definições dos elementos da teoria adotada, sendo as interpretações advindas da formação de significado, o conhecimento explícito vindo da geração de conhecimento e as regras oriundas da tomada de decisão.

Esses três elementos, coletivamente designados por Choo (1998, p.239) por teoria adota, são parte da face pública da organização, importante para codificação e transferência de experiências aprendidas e pela legitimação da existência e das ações da organização perante seus constituintes internos e externos (Choo, 1998, p. 219). As definições de cada elemento da teoria adotada são as seguintes:

Interpretações: Aspectos selecionados do ambiente onde a organização está inserida que, devidamente articulados, merecem atenção dos gestores e que se provam úteis para utilização futura, sendo armazenados para esse fim (Choo, 1998, p. 233).

Conhecimentos Explícitos: Conhecimento codificado em regras organizacionais, rotinas e procedimentos (Choo, 1998, p. 233), sendo passível de ser testado em modelos ou protótipos (Choo, 1998, p. 234).

Regras: No contexto da tomada de decisão, as regras especificam o comportamento apropriado, a alocação de atenção, participação nas ocasiões de escolha de decisão, assim como no exercício da influência política (Choo, 1998, p. 235).

Dadas as definições estabelecidas especificamente para a aplicação do ciclo do conhecimento (Choo, 1998, p.240), faz-se necessário, para a finalidade deste referencial teórico, buscar uma personalização das conceituações para o escopo da segurança e da defesa cibernética. Para tal, lança-se mão dos aspectos teóricos envolvidos.

3.3.1. Interpretações para defesa cibernética

Considerando que as interpretações, sinteticamente, são elementos armazenados passíveis de compor uma informação de complexidade maior e que se deseja adaptar o conceito para o domínio da cibernética, torna-se necessário reconhecer que tipos de extratos informacionais são relevantes armazenar nesse domínio. Considerando que esta pesquisa não busca resolver um caso específico e sim construir uma tese de aplicação extensa, tal condição ainda se demonstra muito abrangente, pois as possibilidades de tais extratos tende a ser crescente e ilimitada dada as variações e combinações de eventos possíveis no ambiente cibernético.

Para lidar racionalmente com essa variedade e manter a viabilidade da pesquisa, a primeira escolha é elucidar o que no campo da cibernética é equivalente às modificações do ambiente da empresa mencionadas por Choo (1998, p.5). Da literatura relativa ao tratamento e resposta aos incidentes computacionais, é possível constatar que o ente que serve ao propósito dessa equivalência é representado pelo conjunto dos eventos de segurança.

Eventos de segurança da informação ou cibernética são definidos, segundo as normas NBR ABNT 27002, como sendo a ocorrência indicando uma possível violação de segurança da informação ou falha de controles, sendo considerado incidente de segurança da informação quando um ou múltiplos eventos de segurança da informação relacionados e identificados que podem

prejudicar os ativos da organização ou comprometer suas operações (ABNT, 2022, p. 3-4).

Assim, para viabilização da personalização buscada, deve-se optar por trabalhar com categorias gerais de informações de interesse para os gestores de cibernética, utilizando como ponto de partida o tipo de modificação ambiental que é fundamental nesse campo: os eventos de segurança. Uma vez que os eventos de segurança são circunstâncias que indicam anomalias com possíveis consequências no estado da segurança das informações do ambiente ou espaço cibernético, as práticas de segurança estabelecidas no campo da cibernética estabelecem que é necessária a caracterização do evento com procedimentos padronizados, tais como, identificar se há ou não uma ameaça, categorizar o tipo de violação que constitui a ameaça, estimar o grau de risco do evento, identificar outros eventos relacionados, além de outros.

Para fins da presente pesquisa, a adaptação da definição do conceito de interpretações requer o uso de conceitos de segurança cibernética que estejam relacionados à percepção de anomalias no espaço cibernético. Essas anomalias são tão relevantes quanto haja indícios ou confirmação de violação de segurança cibernética, sendo uma forma objetiva de lidar com sua identificação, conforme abordado no tópico da revisão de literatura sobre CSIRT, é o uso de indicadores de comprometimento (IOC), na sua forma reativa, e indicadores de ataque (IOA), na sua forma proativa.

De modo a complementar a noção de anomalia, cabe ressaltar que esse conceito para fins desse referencial teórico se constitui de um construto. A necessidade desse construto se dá pela razão de que o evento de segurança cibernética, particularmente se confirmado como incidente, é o ápice de uma cadeia de elementos informacionais que vão desde o ativo informacional envolvido até a violação de segurança propriamente dita. Logo, para uso do conceito nesse referencial teórico, por anomalia ou evento anômalo, toma-se o seguinte significado: evento ocorrido no espaço cibernético que seja ou possa se tornar, ou ainda viabilizar uma violação de segurança cibernética. São exemplos de eventos anômalos de interesse neste estudo: incidente de segurança, vulnerabilidades e ameaças aos ativos de informação, riscos a outros ativos de interesse da defesa cibernética que sejam detectados no espaço

cibernético ameaças, riscos de segurança da informação, incluindo os aspectos de pessoas e instalações físicas que possam gerar violação de segurança cibernética.

Logo, uma readaptação possível e que foi adotada para o referencial teórico da pesquisa é a seguinte:

Interpretações para defesa cibernética: Anomalias do espaço cibernético que envolvam eventos de segurança cibernética que mereçam atenção e análise dos gestores da organização e que se provem úteis para utilização futura, sendo registrados e armazenados para esse fim.

3.3.2. Conhecimento explícito para defesa cibernética

Considerando que os conhecimentos explícitos são conhecimentos codificados e passíveis de modelagem ou produção no mundo real, a busca da personalização do conceito para o contexto da cibernética é mais simples que no caso desenvolvido para o conceito de interpretações. No contexto da cibernética, há diversas necessidades de produção, registro e aplicação de conhecimentos codificados que são decisivos no sucesso dos processos de aplicação da segurança e defesa cibernéticas.

Alguns exemplos específicos desses conhecimentos codificados são as políticas de segurança da informação ou cibernética, os relatórios de gestão de riscos, os planos de continuidade do negócio, os processos de gestão de incidentes, as categorias de ataques cibernéticos, os registros de lições aprendidas, os casos descritivos de ataques cibernéticos reais, as melhores práticas de segurança da informação ou cibernética, os sistemas de gestão de segurança etc.

Logo, é simples estabelecer uma adaptação para o conceito de conhecimento explícito a ser utilizado na pesquisa como segue:

Conhecimentos Explícitos para defesa cibernética: Conhecimento codificado em políticas, normativos, planos, relatórios técnicos, processos, lições aprendidas, metodologias, técnicas, categorias e estatísticas de ataque ou

quaisquer outros conhecimentos codificados similares e passíveis de implementação e transmissão no contexto da defesa cibernética.

3.3.3. Regras para defesa cibernética

Considerando que a pesquisa tem por foco a tomada de consciência situacional de defesa cibernética, baseada no modelo de Endsley (1995, p. 35), e o produto pretendido é de um *framework* para as necessidades primordiais para essa tomada de consciência situacional, a adaptação do conceito de **regras** pode ser, até certo ponto, simplificada, pois, no modelo de Endsley (1995, p. 35), a tomada de decisão propriamente dita vem após o estágio de projeção, ou seja, após a tomada de consciência cibernética.

Ao mesmo tempo, pelo estudo do modelo de Choo (1998, p.240), o desenvolvimento do conceito de **regras** abrange o estágio de projeções de possíveis saídas do processo decisório (Choo, 1998, p. 235). Dos métodos analisados por Choo para uso em seu modelo, o que mantém compatibilidade maior com as melhores práticas de segurança e defesa cibernética são os modelos de decisão racional e de processo (Choo, 1998, p. 172, p.176).

No modelo racional, tem-se quatro elementos basilares: *quasi*-resolução de conflito, prevenção de incerteza, busca de problemática e aprendizado organizacional (Choo, 1998, p. 174). No modelo de processo, tem-se três fases: identificação, desenvolvimento e seleção (Choo, 1998, p. 176)

Dentre as melhores práticas de segurança ou defesa cibernética, é possível identificar quatro processos ligados à projeção de futuros possíveis para subsidiar a tomada de decisão, além de serem compatíveis com os modelos racional e de processo, em particular com este último. São eles:

(i) gestão de riscos: processo eminentemente voltado para antever e prevenir riscos de violação de segurança, que, uma vez diagnosticados são ordenados por prioridade de grau de risco, estabelecendo-se formas de tratamento para cada um, as quais são aplicadas conforme a precedência de cada um, podendo haver mudanças de prioridade caso eventos de segurança forcem uma reavaliação;

(ii) registros das respostas a eventos de segurança passados ou métodos de ataque conhecidos: registros de eventos passados já tratados que funcionam como subsídios para escolher alternativas adequadas para projetar possíveis respostas a eventos em andamento em processos de gestão de incidentes;

(iii) análises de inteligência de ameaças cibernética: processos de busca no espaço cibernético de ameaças à organização para que, de modo antecipado, seja possível haver uma preparação para lidar com a sua concretização ou até mesmo realizar a sua neutralização, provendo, deste modo informações sobre ações iminentes ou prováveis de atacantes cibernéticos, o que dá suporte a projeções para decisão;

(iv) processo de continuidade do negócio e gestão de crises cibernéticas: planejamentos de ações e procedimentos de contenção de potenciais estados de crise gerados por ataques cibernéticos severos, sendo esses planejamentos projetados sobre cenários fictícios de crise prováveis.

Desse modo, pode-se adaptar o conceito de regras, para fins deste referencial teórico, da seguinte forma:

Regras para defesa cibernética: regras que especificam o comportamento apropriado, a alocação de atenção, participação nas ocasiões de escolha de decisão para lidar com eventos de segurança cibernética, sendo baseadas em subsídios advindos de gestão de riscos, registros de incidentes, inteligência cibernética e cenários de incidentes cibernéticos.

Uma vez feita as definições de interpretações, conhecimento explícito e regras para defesa cibernética, torna-se possível analisar os *frameworks* de segurança da informação, cibernética e de ataque cibernético utilizados na pesquisa, de modo a identificar os controles desses *frameworks* relacionados a cada elemento da teoria adotada adaptado para defesa cibernética.

3.4. RELACIONAMENTO ENTRE TEORIA ADOTADA PARA CIBERNÉTICA E MODELO DE ENDSLEY

Tomando as definições de interpretações, conhecimento explícito e regras adaptadas para defesa cibernética, conforme explanado nos subtítulos 3.3.1 a 3.3.3, define-se, para fins desta pesquisa, o conceito de **teoria adotada para defesa cibernética** como sendo a reunião dos elementos de interpretações, conhecimento explícito e regras adaptados para esse domínio.

A relação utilizada neste referencial teórico entre o modelo de Endsley (1995, p.34) e a teoria adotada para defesa cibernética é obtida em duas etapas. A primeira, é realizada a partir da seleção dos elementos integrantes dos estágios da consciência situacional (Endsley, 1995, p.34), ou seja, perceber, compreender e projetar, que apresentam comportamento informacional de interpretações ou conhecimentos explícitos ou regras para cibernética.

Uma vez selecionados os aspectos da consciência situacional, a segunda etapa de relação é realizada por meio do reconhecimento de quais controles obtidos dos *frameworks* analisados e organizados por cada elemento da teoria adotada para defesa cibernética estão ligados aos aspectos selecionados na primeira etapa. Para tal, como critérios para esse reconhecimento, foram elaboradas perguntas sobre as necessidades informacionais primordiais buscadas na pesquisa.

3.4.1. Relação à Percepção

O estágio da percepção, conforme visto na revisão de literatura, dá-se por meio do processamento da pré-atenção, da atenção e das memórias de trabalho e de longo prazo. Dentre esses elementos do estágio da percepção, para fins desse referencial teórico, será dado o foco principal à pré-atenção. Essa escolha se deu pelo fato de que a pré-atenção pode ser diretamente relacionada à teoria adotada, pois se vale de registros significativos e conhecimentos explícitos como critérios para ser realizada.

Embora as memórias de trabalho e de longo prazo se valham dos mesmos elementos, esses aspectos são abordados no tópico relativo à compreensão, pois, ainda que essas memórias estejam presentes em todas as

etapas da consciência situacional, Endsley (1995, p.45) se refere a elas com maior ênfase nesse estágio. Portanto, para este estudo de doutorado, essas memórias foram abordadas no estágio de compreensão.

Por fim, o aspecto da atenção não foi incluído por ser uma capacidade humana de manutenção de foco no objeto de interesse. Relembrando que esse interesse é despertado na pré-atenção, a qual é já é reconhecida como elemento de análise de pesquisa.

Dentre os possíveis insumos para que a pré-atenção possa acontecer, estão os conhecimentos codificáveis que explicitam elementos de relevância que constituem possibilidades para as quais, caso concretizadas, tornam-se prioritárias à percepção, conforme se pode constatar da análise das Figuras 28 a 30, com destaque para os elementos de metas, *schematas* e *scripts*.

Assim, para aplicação neste referencial teórico, o estágio da percepção será relacionado à teoria adotada para defesa cibernética por meio do conceito de pré-atenção. Para efetuar a relação com os controles selecionados dos *frameworks* usados na pesquisa, deve ser utilizado o seguinte de questionamento:

Que necessidades informacionais primordiais podem ser derivadas dos controles do framework de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo schematas, as quais viabilizam ou realizam a pré-atenção necessária para identificação de eventos de segurança cibernética no espaço cibernético de interesse da operação cibernética?

3.4.2. Relação à Compreensão

O estágio de compreensão está baseado numa síntese formada na mente do operador a partir dos elementos desconexos captados no nível 1, à luz dos objetivos da operação. Para tal, a memória de trabalho age como um mecanismo de processamento da informação, enquanto a memória de longo prazo age como um repositório a suprir com dados e informações esses processamentos, conforme indicado nas Figuras 28 e 29.

Desta forma, uma vez que a construção deste referencial teórico está baseada nos aspectos cognitivos da teoria do conhecimento organizacional de Choo (1998, p. 239), a memória de trabalho não é o aspecto da compreensão a ser usado na pesquisa, uma vez que essa memória se processa como um encadeamento de premissas providas pela memória de longo prazo, chegando a algumas inferências, conforme juízo de valor do indivíduo que está tomando a consciência situacional.

Por outro lado, a memória de longo prazo faz uso de elementos cognitivos, conforme se pode constatar da Figura 29 e do conteúdo do item 2.4.3 (Compreensão) do capítulo sobre revisão de literatura. Foi explanado que a memória de longo prazo, segundo esquematizado por Endsley (1995, p. 43), serve-se de um conjunto de informações que geralmente são originalmente codificadas em conhecimentos explícitos. Em consequência, para fins desse referencial, o foco majoritário no estágio de compreensão será dado à memória de longo prazo.

Por sua vez, em relação aos insumos à memória de longo prazo destacados por Endsley (1995, p. 43) na Figura 29, ou seja, *schematas*, *scripts* e modelos mentais, os *schematas* serão focalizados neste referencial teórico, pois dão origem tanto aos *scripts* (formas mais simples de *schematas*) quanto aos modelos mentais, estes últimos, sendo *schematas* mais complexos de formação particular de cada indivíduo.

Sendo os *schematas* estruturas de representação sob as quais sistemas de informação podem ser interpretados e representados de modo simplificado, tal qual um modelo esquemático de referência para se avaliar em algum grau uma dada situação, Endsley considera esses esquemas como *frameworks* (Endsley, 1995, p.43).

Assim, para aplicação neste referencial teórico, o estágio da compreensão será relacionado à teoria adotada por meio do conceito de *schemata*. Logo, de modo análogo ao que foi estabelecido para o estágio da percepção, por meio do conceito de *schemata* como instrumento do relacionamento da **teoria adotada para cibernética** com o estágio de compreensão da consciência situacional, será utilizado o seguinte de questionamento para revelar a relação com os controles selecionados dos *frameworks* da pesquisa:

Que necessidades informacionais primordiais podem ser derivadas dos controles do framework de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo schematas para a memória de longo prazo necessários à compreensão de eventos de segurança cibernética?

3.4.3. Relação à projeção

O estágio de projeção é constituído pela habilidade de projetar as ações dos elementos do ambiente como consequência direta do conhecimento do estado e da dinâmica desses elementos e da compreensão da situação corrente. Novamente, Endsley (1995, p.37) enfatiza as memórias de longo prazo e de trabalho. Em consequência, novamente a ênfase para fins desta pesquisa será dada aos *schematas,* tendo as mesmas justificativas explanadas no estágio da Compreensão, apenas destacando que, neste estágio, os *schematas* são voltados para a projeção de possibilidades.

Assim, a aplicação do conceito de *schemata* como instrumento de relacionamento da teoria adotada para cibernética com o estágio de projeção da consciência situacional, será utilizado o seguinte de questionamento para obter a relação com os controles do *framework* da pesquisa:

Que necessidades informacionais primordiais podem ser derivadas dos controles do framework de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo schematas para a memória de longo prazo necessários à projeção dos desdobramentos de eventos de segurança cibernética?

3.4.4. Metas, Objetivos e Perspectivas

Por fim, Endsley (1995, p. 47) enfatiza que os objetivos a serem alcançados no contexto em que se desenrola a tomadas de consciência situacional influencia decisivamente o processo. Assim, toda e qualquer aplicação do *framework* buscado nesta pesquisa para situações específicas deverá estar intrinsecamente ligada ao objetivo a ser alcançado de tal aplicação.

Em relação a esses aspectos ligados à finalidade de uma operação de defesa cibernética, a seguinte pergunta será utilizada como guia para identificação de necessidade informacionais primordiais:

Que necessidades informacionais primordiais podem ser derivadas dos controles do framework de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo schematas de pré-atenção ou memória de longo prazo para parâmetros estabelecidos a priori em relação a operação cibernética?

3.5. CRITÉRIOS PARA AVALIAÇÃO PRELIMINAR DO *FRAMEWORK*

Como elemento final do referencial teórico a ser definido para a abordagem a ser seguida na pesquisa, faz-se necessário o estabelecimento das referências teóricas a serem usadas de modo a viabilizar a consecução dos objetivos finais do trabalho, os quais visam avaliar a pertinência do *framework* produzido. Nesse sentido, utilizou-se a adaptação do modelo de Endsley, conforme proposta por Barford *et al*. (2010, p. 3-5), para o campo da cibernética, consoante ao exposto na revisão de literatura e retomado neste tópico.

Na adaptação realizada por Barford *et al*. (2010, p. 3-5), sete aspectos são estabelecidos para serem aplicados em cada estágio da consciência situacional:

(i) a percepção da ocorrência de um ataque, seu tipo, fonte, alvo etc.;
(ii) consciência do nível atual e possível desdobramento do impacto do ataque;
(iii) consciência da evolução da situação;
(iv) ciência do comportamento do adversário;
(v) ciência do porquê e como a situação corrente foi causada;
(vi) ciência da qualidade (confiabilidade) das informações coletadas e das decisões de inteligência que foram derivadas dessas informações;
(vii) avaliação dos futuros plausíveis da situação corrente.

A relação desses aspectos com os estágios Perceber, Compreender e Projetar são as seguintes Barford *et al*. (2010, p. 4)

- Percepção dos elementos do ambiente (nível 1): aspectos (i) e (vi).
- Compreensão da situação corrente (nível 2): aspectos (ii), (iv) e (v).
- Projeção de estados futuros (nível 3): aspectos (iii) e (vii).

Esses aspectos serviram como guias para verificar se as necessidades de informação primordiais obtidas da relação das fases da consciência situacional e o *framework* produzido no estágio anterior da pesquisa seriam efetivos se aplicados aos eventos reais objetos da pesquisa. Para facilitação dessa verificação, esses aspectos da consciência situacional foram utilizados em forma de questionamento e buscando evidenciar o uso de *schematas*. Por exemplo, para o aspecto (i), foi aplicado desta forma: *Quantos schematas de pré-atenção foram usados para a percepção da ocorrência de uma anomalia no espaço cibernético?* Assim, as perguntas foram formuladas conforme Quadro nr 2. Essa verificação deve ser baseada nos eventos anômalos ocorridos em cada operação cibernética, assim como as lições aprendidas e eventos de APA registrados, em contraposição às preparações realizadas para cada operação, com base nas necessidades informacionais de cada uma, sendo estas derivas das necessidades primordiais.

Cabe ressaltar que a avaliação proposta é de caráter preliminar, pois uma verificação completa deve se dar numa operação rela futura.

Quadro 2 - Questionamentos para teste do *framework* da pesquisa

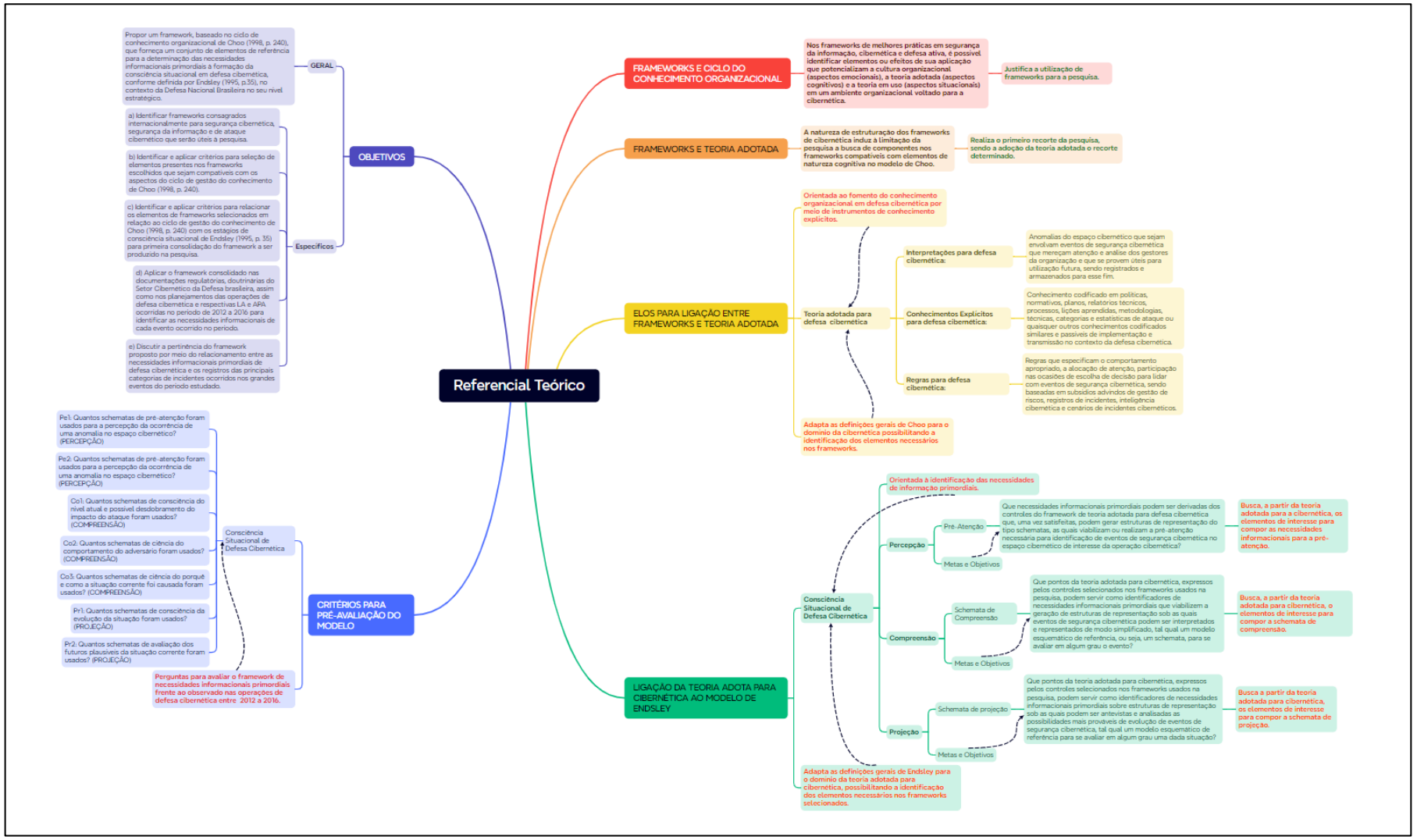
Questão	**Estágio da Consciência Situacional**
Pe1: Quantos *schematas* de pré-atenção foram usados para a percepção da ocorrência de uma anomalia no espaço cibernético?	**Percepção**
Pe2: Quantos *schematas* de pré-atenção foram usados para a percepção da ocorrência de uma anomalia no espaço cibernético?	**Percepção**
Co1: Quantos *schematas* de consciência do nível atual e possível desdobramento do impacto do ataque foram usados?	**Compreensão**
Co2: Quantos *schematas* de ciência do comportamento do adversário foram usados?	**Compreensão**
Co3: Quantos *schematas* de ciência do porquê e como a situação corrente foi causada foram usados?	**Compreensão**
Pr1: Quantos *schematas* de consciência da evolução da situação foram usados?	**Projeção**
Pr2: Quantos *schematas* de avaliação dos futuros plausíveis da situação corrente foram usados?	**Projeção**

Fonte: Autor

3.6. REPRESENTAÇÃO GRÁFICA DO REFERENCIAL TEÓRICO

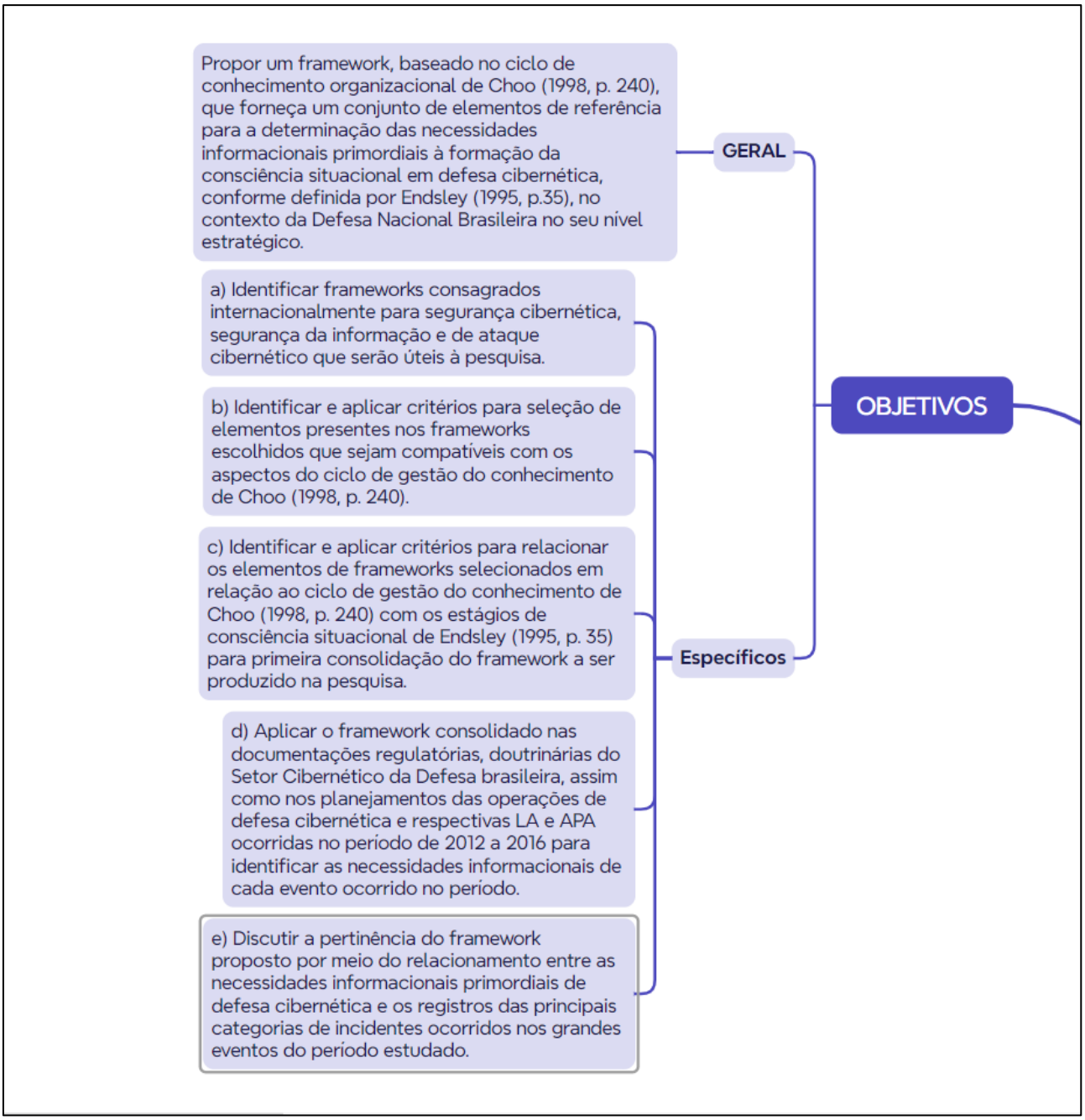
Como síntese gráfica da ordenação estabelecida pelas definições e recortes para a abordagem da pesquisa provida pelo referencial teórico, as Figuras 32 a 37 mostram o mapa mental correspondente.

Figura 32 - Representação completa do referencial teórico em mapa mental



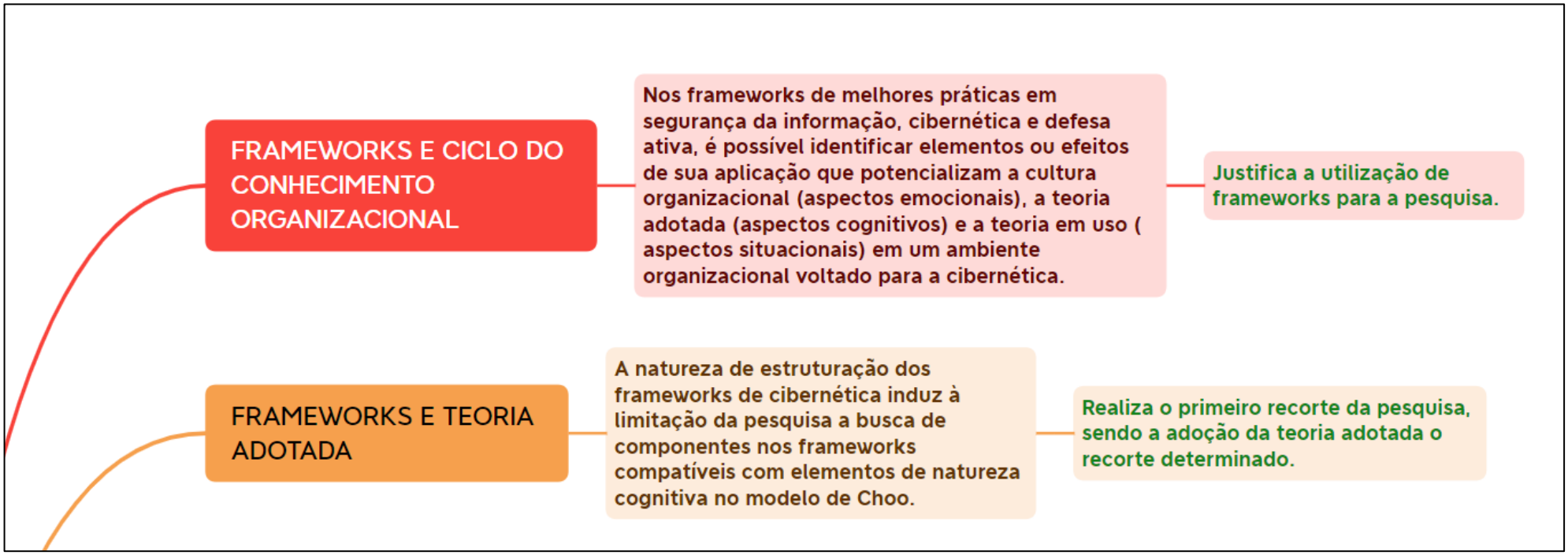
Fonte: Autor.

Figura 33 - Representação parcial do referencial teórico: objetivos da pesquisa



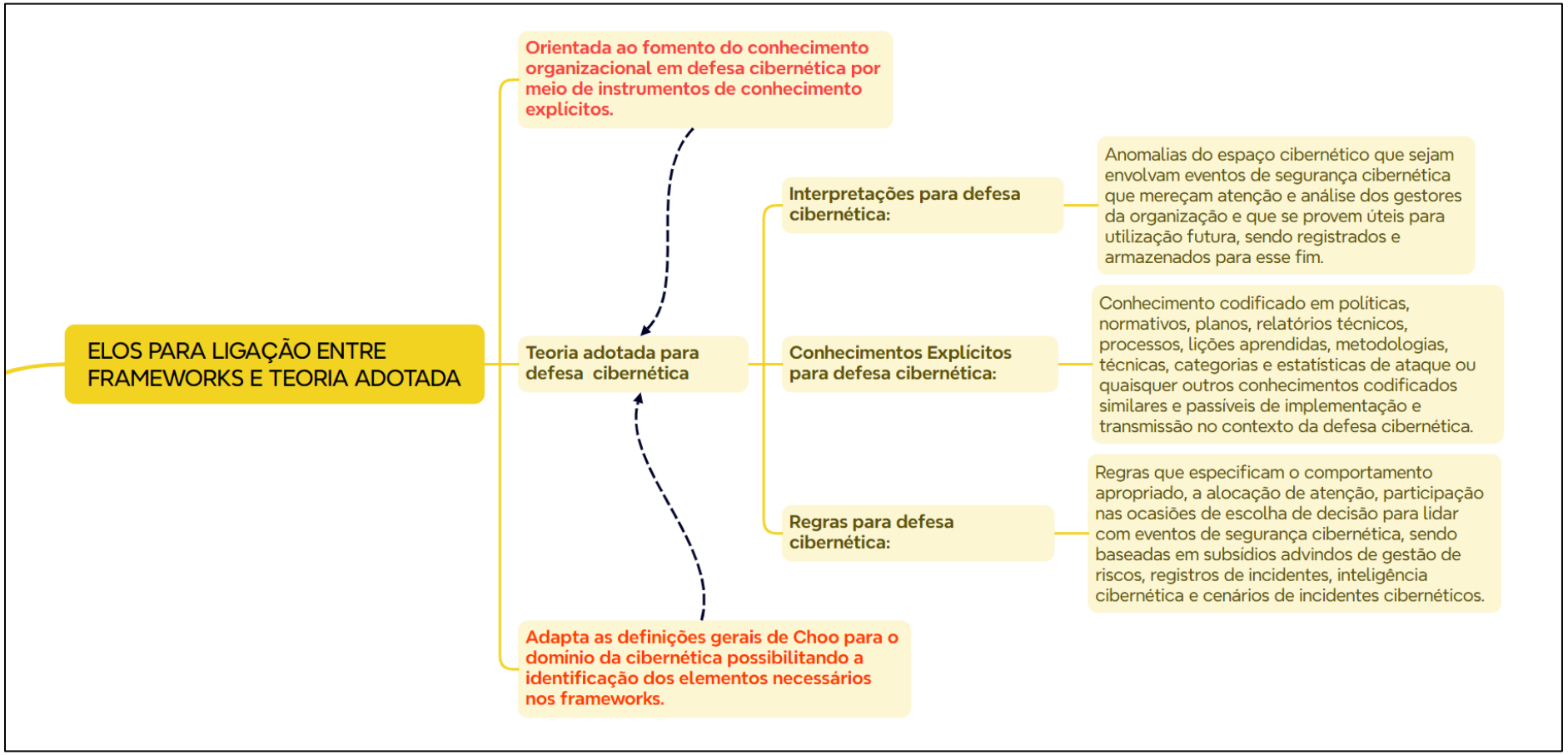
Fonte: Autor.

Figura 34 - Representação parcial do referencial teórico em mapa mental: sobre o uso do conceito de *frameworks*



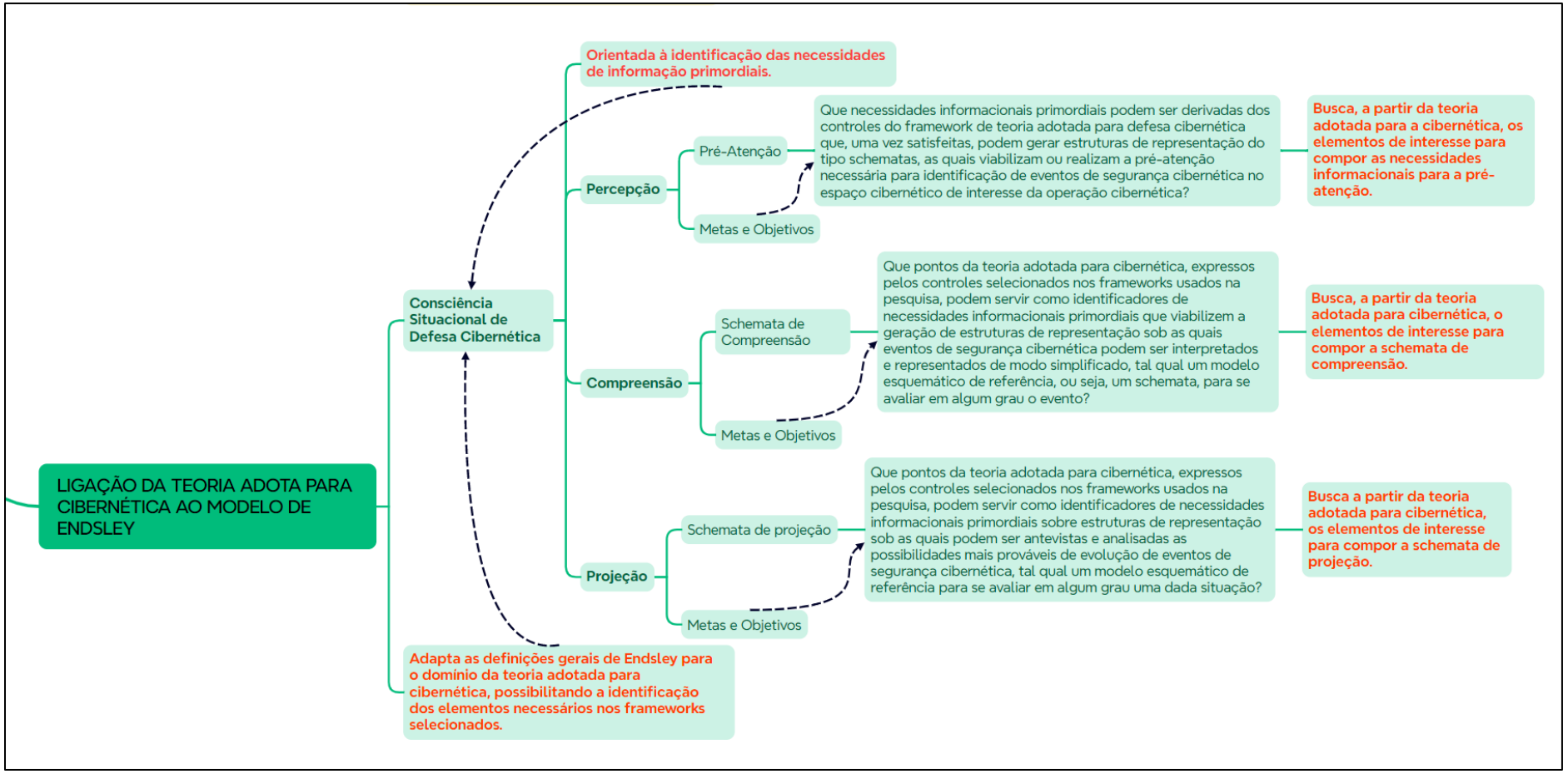
Fonte: Autor.

Figura 35 - Representação parcial do referencial teórico em mapa mental: elos entre *frameworks* e teoria adotada



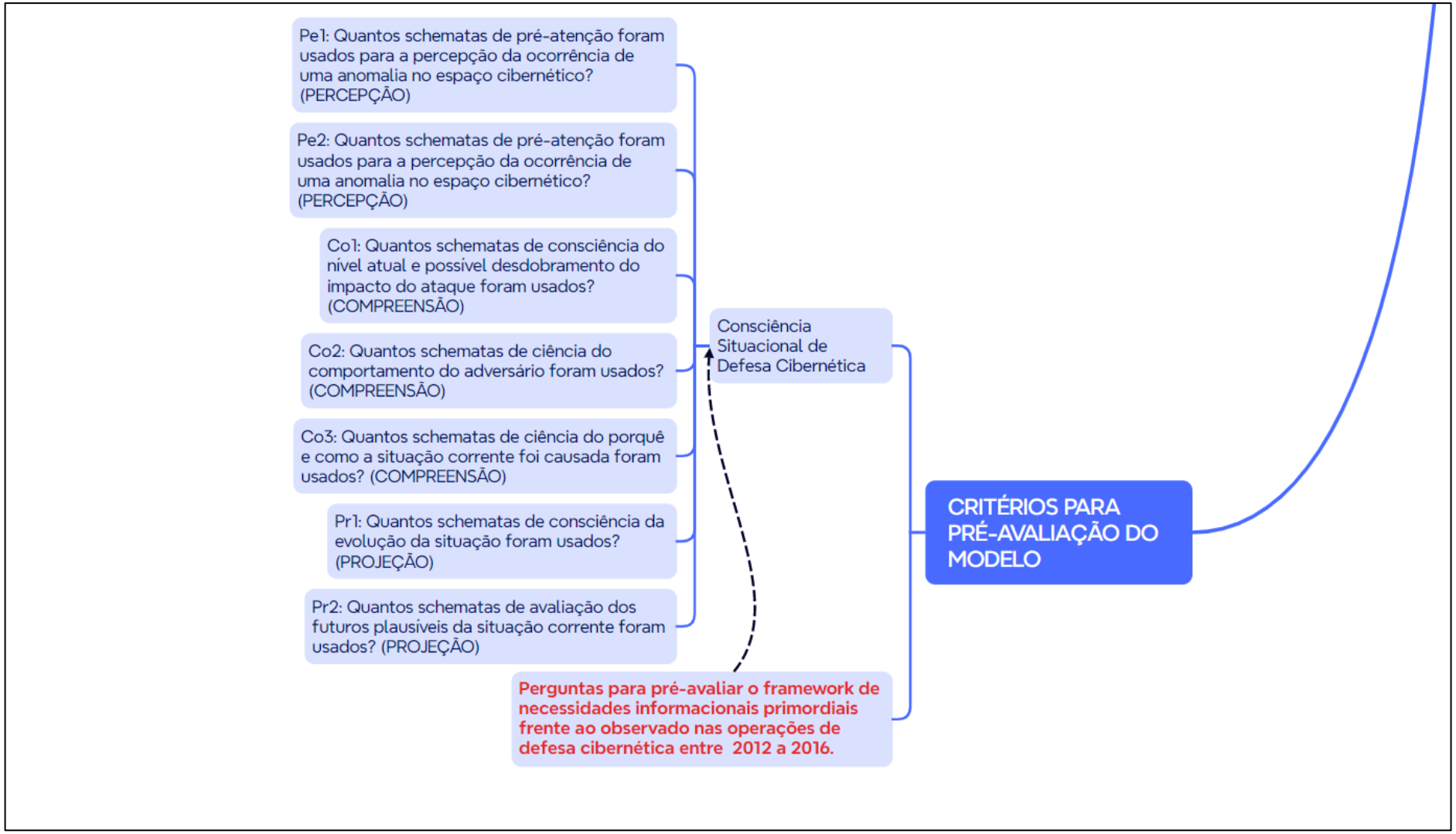
Fonte: Autor.

Figura 36 - Representação parcial do referencial teórico: ligação entre teoria adotada para cibernética e o modelo de Endsley



Fonte: Autor.

Figura 37 - Representação parcial do referencial teórico em mapa mental: critérios de avaliação do modelo



Fonte: Autor.

Neste capítulo, buscou-se ordenar os conhecimentos de base para a pesquisa de modo a viabilizar a consecução dos objetivos da tese, de acordo com o recorte feito no contexto da realidade estudada. Para isso, foram realizadas adaptações e encadeamentos lógicos entre esses conhecimentos, gerando assim critérios de especificidade e singularidade requeridos para um estudo de doutoramento. Em consequência, foi gerado o referencial teórico apresentado, a partir do qual se estabeleceu os requisitos para elaboração e execução dos procedimentos metodológicos, conforme disposto nos capítulos restantes deste documento.

4. METODOLOGIA

4.1. CATEGORIZAÇÃO DA PESQUISA

A presente pesquisa tem por objetivo geral propor um *framework* que, baseado no ciclo de conhecimento organizacional, forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética no contexto da Defesa Nacional Brasileira no seu nível estratégico. Em consequência, a pesquisa busca gerar um conhecimento explícito útil à preparação de gestores e comandantes que precisem liderar uma operação de defesa cibernética seja no contexto militar ou civil.

Desse modo, o desenvolvimento da investigação tomou um caráter de pesquisa aplicada, uma vez que, a partir de modelos teóricos já consolidados, visa aplicar a composição desses modelos para verificar sua efetividade real (Oliveira, 2001, p. 123).

Além disso, a pesquisa tem por características essenciais ser estudo descritivo, que fez uso de técnicas de pesquisa bibliográfica, documental e de observação participante do tipo natural (Marconi; Lakatos, 2003, p. 194).

Aplicou-se o método dedutivo, conforme descrito por Marconi e Lakatos (2003, p. 92). Usou-se esse método para produzir um *framework* que viabilize a indicação das necessidades informacionais para a consciência situacional de defesa cibernética, tomando-se por premissas as definições do ciclo de conhecimento organizacional de Choo (1998, p. 232), controles que definem *frameworks* de segurança cibernética e elementos constituintes do ciclo de tomada de consciência situacional de defesa e segurança cibernética (Tadda e Salerno, 2010, p.17). Como consequentes desse processo, foram gerados os controles buscados na pesquisa. Uma vez elaborado o modelo sobre esses pressupostos e estabelecidas as conjecturas adequadas, os testes de validação perfizeram a fase de falseamento como etapa final.

Quanto aos procedimentos metodológicos relativos aos tipos de pesquisa, realizou-se a leitura e seleção dos elementos bibliográficos necessários, tomando como ponto de partida as perspectivas de Endsley (1995), Choo (1998a, 1998b), Boyd (2018), Barford, Dacier *et al*. (2010) e Carneiro (2012).

Quanto à pesquisa da documentação em fonte primária, a partir de documentos de planejamento e resultados das operações cibernéticas ocorridas no período entre 2012 e 2016, no Ministério da Defesa, período que houve a observação participativa, dentre os quais há o registro de 477 Lições Aprendidas (LA) e aproximadamente 500 itens de Análise Pós-Ação (APA), referente aos resultados alcançados.

4.2. PLANO DE PESQUISA

Este tópico descreve o sequenciamento das ações em que foram organizados os objetivos da pesquisa. Os quadros 3 e 4 contêm as tarefas correspondentes.

Quadro 3 - Objetivos geral e específicos

Objetivo Geral	Objetivos Específicos
Propor um *framework*, baseado no ciclo de conhecimento organizacional de Choo (1998, p. 240), que forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética, conforme definida por Endsley (1995, p.35), no contexto da Defesa Nacional Brasileira no seu nível estratégico.	a) Identificar e escolher quais *frameworks* consagrados internacionalmente para segurança cibernética, segurança da informação e de ataque cibernético serão úteis à pesquisa.
	b) Identificar e aplicar critérios para seleção de elementos presentes nos *frameworks* escolhidos que sejam compatíveis com os aspectos do ciclo de gestão do conhecimento de Choo (1998, p. 240).
	c) Identificar e aplicar critérios para relacionar os elementos de *frameworks* selecionados em relação ao ciclo de gestão do conhecimento de Choo (1998, p. 240) com os estágios de consciência situacional de Endsley (1995, p. 35) para primeira consolidação do *framework* a ser produzido na pesquisa.
	d) Aplicar o *framework* consolidado nas documentações regulatórias, doutrinárias do Setor Cibernético da Defesa brasileira, assim como nos planejamentos das operações de defesa cibernética e respectivas LA e APA ocorridas no período de 2012 a 2016 para identificar as necessidades informacionais de cada evento ocorrido no período.
	e) Discutir a pertinência do *framework* proposto por meio do relacionamento entre as necessidades informacionais primordiais de defesa cibernética e os registros das principais categorias de incidentes ocorridos nos grandes eventos do período estudado.

Fonte: Autor.

Quadro 4 – Tarefas relativas aos objetivos específicos (continua)

Objetivos Específicos	Tarefas
a) Identificar e escolher quais *frameworks* consagrados internacionalmente para segurança cibernética, segurança da informação e de ataque cibernético serão úteis à pesquisa.	a.1) Identificar os *frameworks* de segurança da informação e cibernética e de defesa ativa de maior utilização no campo da cibernética.
	a.2) Identificar e justificar os *frameworks* de segurança da informação e cibernética e de defesa ativa de maior compatibilidade com a pesquisa, conforme objetivo geral.
	a.3) Escolher os *frameworks* para utilização na pesquisa.
b) Identificar e aplicar critérios para seleção de elementos presentes nos *frameworks* escolhidos que sejam compatíveis com os aspectos do ciclo de gestão do conhecimento de Choo (1998, p. 240).	b.1) Declarar o critério para relacionar o ciclo de gestão do conhecimento e os controles que integram os *frameworks* selecionados, conforme escolhas adotadas no referencial teórico.
	b.2) Realizar o relacionamento entre os aspectos da teoria adotada para defesa cibernética e os controles que integram os *frameworks* selecionados, conforme critério declarado, de modo a formar *framework* de teoria adotada para defesa cibernética.
c) Identificar e aplicar critérios para relacionar os elementos de *frameworks* selecionados em relação ao ciclo de gestão do conhecimento de Choo (1998, p. 240) com os estágios de consciência situacional de Endsley (1995, p. 35) para primeira consolidação do *framework* a ser produzido na pesquisa.	c.1) Declarar o critério para relacionar o *framework* de teoria adotada para defesa cibernética e os estágios da consciência situacional, conforme escolhas adotadas no referencial teórico.
	c.2) Realizar o relacionamento entre o *framework* de teoria adotada para defesa cibernética e os estágios da consciência situacional, conforme critério declarado, enunciando as necessidades informacionais primordiais de consciência situacional para defesa cibernética (NIP-CS-DC).
d) Aplicar o *framework* consolidado nas documentações regulatórias, doutrinárias do Setor Cibernético da Defesa brasileira, assim como nos planejamentos das operações de defesa cibernética e respectivas LA e APA ocorridas no período de 2012 a 2016, para identificar as necessidades informacionais de cada evento ocorrido no período.	d.1) Coletar as documentações de planejamento, em níveis militares estratégico e operacional, assim como os registros de APA, das operações de defesa e segurança cibernética entre 2012 e 2016.
	d.2) Analisar a documentação de cada operação de defesa e segurança cibernética do período estudado, assinalando as NIP-CS-DC aplicáveis, assim como as não aplicáveis, de forma justificada.

Quadro 4 – Tarefas relativas aos objetivos específicos (conclusão)

Objetivos Específicos	Tarefas
e) Discutir a pertinência do *framework* proposto por meio do relacionamento entre as necessidades informacionais primordiais de defesa cibernética e os registros das principais categorias de incidentes e demais eventos anômalos ocorridos nas operações de defesa cibernética no período da pesquisa.	e.1) Identificar as principais categorias de eventos cibernéticos observados nas operações militares de defesa cibernética no período estudado pela pesquisa, assim como os respectivos processos para lidar com esses eventos.
	e.2) Para cada categoria de evento e processos identificados, indicar quais as etapas de consciência situacional com os respectivos *schematas* utilizados, à luz dos questionamentos obtidos pelo modelo de Barford *et al*. (2010, p. 3-5), adaptados, conforme referencial teórico.
	e.3) Analisar comparativamente os resultados obtidos pela avalição da tarefa (e.2) com os resultados obtidos do objetivo específico (d).

Fonte: Autor.

5. RESULTADOS

Neste capítulo são relatados os resultados alcançados com a execução dos objetivos específicos da pesquisa. Os resultados foram organizados de forma correspondente a cada grupo de tarefas nas quais os objetivos específicos foram subdivididos, conforme Quadro 4.

5.1. OBJETIVO ESPECÍFICO (a)

Neste subtítulo são descritos os procedimentos para a execução do objetivo específico (a), qual seja, “Identificar e escolher quais *frameworks* consagrados internacionalmente para segurança cibernética, segurança da informação e de ataque cibernético serão úteis à pesquisa”. Para tal, procedeu-se o registro dos resultados das tarefas (a.1) a (a.3), conforme consta no Quadro 4, no capítulo de Metodologia.

5.1.1. Tarefas (a.1), (a.2) e (a.3)

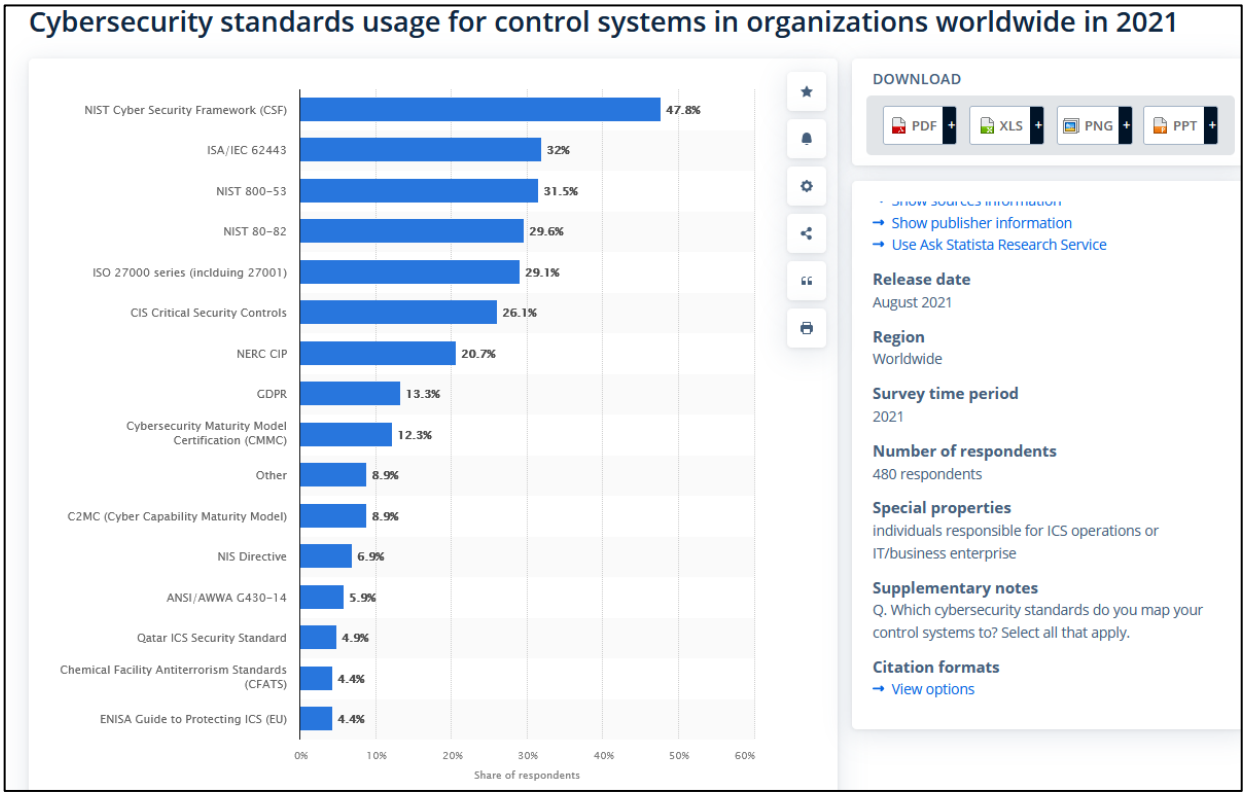
A tarefa (a.1) teve por finalidade identificar os *frameworks* de segurança da informação, cibernética e de defesa ativa de maior utilização de mercado. Para identificar os *frameworks* mais utilizados, buscou-se fontes primárias de levantamentos estatísticos que pudessem fundamentar a escolha. Cabe ressaltar que o mercado de segurança da informação ou cibernética pode prover indicativos a respeito, pois produtos, serviços e legislação podem, conforme o caso, indicar, exigir ou fazer uso de normas técnicas e *frameworks* específicos.

Tomando-se como critério principal localizar fontes estatísticas sobre a demanda, foi identificada a empresa Statista[19]. Na apresentação da empresa consta o seguinte: Statista é uma plataforma global de dados e *business intelligence* com uma extensa coleção de estatísticas, relatórios e insights sobre mais de 80.000 tópicos de 22.500 fontes em 170 setores. Fundada na Alemanha em 2007, a Statista opera em 13 locais em todo o mundo e emprega cerca de 1.100 profissionais[20].

[19] https://www.statista.com/, acessado em 30/01/2024.
[20] https://www.statista.com/aboutus/, acessado em 30/01/2024.

Ao se realizar uma pesquisa sobre uso de *frameworks* de segurança cibernética na página eletrônica da Statista, uma das respostas analisadas conduziu a pesquisa estatística representada na Figura nr 38.

Figura 38 – Estatística de uso de *frameworks* de segurança cibernética em 2021



Fonte: https://www.statista.com/statistics/1273188/cybersecurity-standards-usage-control-systems/

Pelo gráfico representado na Figura 38, pode-se constatar o *framework* NIST CSF como o mais utilizado em 2021, numa expressiva margem de diferença para os demais *frameworks* ou normas técnicas.

Não foram localizadas pesquisas estatísticas providas pela Statista ou outra entidade equivalente sobre uso de *frameworks* de ataque cibernético. No entanto, realizando-se pesquisas simples nos principais buscadores da internet, pôde-se identificar algumas opções de metodologias e *frameworks* relacionados a ataques cibernéticos, dentre as mais conhecidas: (i) a metodologia OSSTMM (*Open Source Security Testing Methodology Manual*[21]), muito utilizada para

[21] https://www.isecom.org/OSSTMM.3.pdf

testes de invasão de redes; (ii) o *Open Web Application Security Project* (OWASP)[22], focado em segurança de aplicações para internet (*web*); (iii) MITRE ATT&CK *framework*, que, embora não seja nem uma ferramenta nem uma metodologia, é estrutura em forma de *framework* sobre técnicas e táticas de ataque cibernético; (iv) a metodologia de teste NIST 800-115 (NIST, 2008), que compreende metodologias de teste de segurança cibernética.

Os *frameworks* considerados de maior compatibilidade para a pesquisa foram: (i) o NIST-CSF para aplicação relacionada à ação de segurança cibernética; (ii) o MITRE ATT&CK para aplicação relacionada às ações de exploração e ataque cibernético. As justificativas com as respectivas discussões para esta escolha encontram-se no capítulo 6, onde são feitas as discussões gerais dos resultados.

5.2. OBJETIVO ESPECÍFICO (b)

Neste subtítulo são descritos os procedimentos para a execução do objetivo específico (b), qual seja, “Identificar e aplicar critérios para seleção de elementos presentes nos *frameworks* escolhidos que sejam compatíveis com os aspectos do ciclo de gestão do conhecimento de Choo (1998, p. 240)”. Para tal, procedeu-se o registro dos resultados das tarefas (b.1) a (b.3), conforme consta no Quadro 4, no capítulo de Metodologia.

5.2.1. Tarefas (b.1) e (b.2)

As tarefas (b.1) e (b.2) resultaram nos Quadros 5 [tarefa (b.1)] e Quadros 6 e 7 [tarefa (b.2)].

O Quadro 5 representa o critério de relação entre os *frameworks* NIST CSF e MITRE ATT&CK e a teoria adotada para defesa cibernética, conforme definida no referencial teórico desta pesquisa. O critério é apresentado de forma composta, de modo a tornar viável percorrer os elementos (controles NIST e táticas MITRE) de cada *framework* e relacionar cada um aos aspectos da teoria adotada para defesa cibernética. Essa estruturação do critério buscado em

[22] https://owasp.org/

parâmetros específicos que o compõem resultou nos 13 subcritérios, sendo quatro relacionados às interpretações para defesa cibernética, quatro para o conhecimento explícito para defesa cibernética e cinco para as regras para defesa cibernética.

A aplicação do critério estabelecido no Quadro 5 em cada controle e tática dos *frameworks* NIST CSF e MITRE ATT&CK resultou nos Quadros 6 e 7. Nesses quadros, os controles e táticas foram rearranjados de modo a comporem três grandes blocos de controles de segurança cibernética ou táticas de exploração e ataque: interpretações, conhecimento explícito e regras para defesa cibernética. Para facilitação da referência a estes dois subconjuntos de controles de segurança cibernética NIST CSF e táticas MITRE rearranjados nos aspectos da teoria adotada para defesa cibernética, o conjunto geral será referido como *framework* de teoria adotada para defesa cibernética.

Neste tópico buscou-se apenas apresentar sumariamente os resultados, sendo as suas justificativas e demais discussões registradas no capítulo 6.

Quadro 5 - Critérios para relacionamentos enunciados na tarefa (b1)

ASPECTO	DEFINIÇÃO	CRITÉRIO 1	ID_Crit1	CRITÉRIO 2	ID_Crit1	CRITÉRIO 3	ID_Crit1	CRITÉRIO 4	ID_Crit1	CRITÉRIO 5	ID_Crit1
INTERPRETAÇÃO PARA DEFESA CIBERNÉTICA	Interpretações para defesa cibernética: Anomalias do espaço cibernético que ***envolvam*** eventos de segurança cibernética que mereçam atenção e análise dos gestores da organização e que se provem úteis para utilização futura, sendo registrados e armazenados para esse fim.	O controle recomenda ações de preparação para detecção ou a realização da detecção de anomalias no espaço cibernético que ***envolvam*** eventos de segurança.	I-C1	O controle recomenda ações de análise primárias de anomalias detectadas no espaço cibernético.	I-C2	O controle recomenda ações de armazenagem dos registros das anomalias detectadas no espaço cibernético para uso futuro.	I-C3	O controle recomenda ações de preparação ou viabilização para realização da ataques no espaço cibernético que envolvam eventos de segurança.	I-C4	------	------
CONHECIMENTOS EXPLÍCITOS PARA DEFESA CIBERNÉTICA	Conhecimento codificado em políticas, normativos, planos, relatórios técnicos, processos, metodologias, técnicas, categorias e estatísticas de ataque, lições aprendidas ou quaisquer outros conhecimentos codificados similares e passíveis de implementação e transmissão no contexto da defesa cibernética.	O controle recomenda ações de elaboração de conhecimento explícito na forma de políticas, normativos, planos, relatórios técnicos, processos, metodologias, técnicas, categorias e estatísticas de ataque ou quaisquer outros conhecimentos codificados similares e passíveis de aplicação ou difusão para a defesa cibernética.	C-C1	O controle recomenda ações de elaboração de conhecimento explícito para aperfeiçoar, atualizar ou outra possibilidade de retroalimentração para fins de absorção de lições aprendidas para evolução da aplicação segurança e da defesa cibernéticas.	C-C2	O controle recomenda ações de elaboração ou obtenção de conhecimento explícito na forma de técnicas e táticas de ataques cibernéticos ou quaisquer outros conhecimentos codificados similares e passíveis de aplicação ou difusão para a defesa cibernética.	C-C3	O controle recomenda ações de elaboração de conhecimento explícito na forma de políticas, normativos, planos, relatórios técnicos, processos, metodologias, técnicas, categorias e estatísticas de ataque ou quaisquer outros conhecimentos codificados similares e passíveis de aplicação ou difusão para a defesa cibernética.	C-C4	------	------
REGRAS PARA DEFESA CIBERNÉTICA	Regras que especificam o comportamento apropriado, a alocação de atenção, participação nas ocasiões de escolha de decisão para lidar com evento de segurança cibernética baseadas em subsídios advindos de gestão de riscos, registros de incidentes, inteligência cibernética e cenários de incidentes cibernéticos.	O controle recomenda ações de projeção de futuros possíveis baseadas em riscos.	R-C1	O controle recomenda ações de projeção de futuros possíveis baseadas em registros de incidentes, tanto para segurança quanto para ataque.	R-C2	O controle recomenda ações de projeção de futuros possíveis baseadas em inteligência, tanto para segurança quanto para ataque.	R-C3	O controle recomenda ações de projeção de futuros possíveis baseadas em cenários hipotéticos de crises, tanto para segurança quanto para ataque.	R-C4	O controle recomenda ações de projeção de futuros possíveis baseadas em critérios não cobertos pelos critérios de 1 a 4.	R-C5

Fonte: Autor

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Interpretações	***Dispositivos físicos e sistemas dentro da organização são inventariados.***	ID.AM-1	Gestão de Ativos (ID.AM)	ID.AM	IDENTIFICAR
Interpretações	***Plataformas de software e aplicações dentro da organização são inventariadas.***	ID.AM-2	Gestão de Ativos (ID.AM)	ID.AM	IDENTIFICAR
Interpretações	***Comunicações organizacionais e fluxos de dados são mapeados.***	ID.AM-3	Gestão de Ativos (ID.AM)	ID.AM	IDENTIFICAR
Interpretações	***Sistemas de informação externos são catalogados.***	ID.AM-4	Gestão de Ativos (ID.AM)	ID.AM	IDENTIFICAR
Interpretações	***O papel da organização na cadeia de suprimentos é identificado e comunicado.***	ID.BE-1	Ambiente de Negócios (ID.BE):	ID.BE	IDENTIFICAR
Interpretações	***A posição da organização na infraestrutura crítica e em seu setor industrial é identificada e comunicada.***	ID.BE-2	Ambiente de Negócios (ID.BE)	ID.BE	IDENTIFICAR
Interpretações	***As vulnerabilidades dos ativos são identificadas e documentadas.***	ID.RA-1	Avaliação de Riscos (ID.RA)	ID.RA	IDENTIFICAR
Interpretações	***Inteligência de ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações.***	ID.RA-2	Avaliação de Riscos (ID.RA)	ID.RA	IDENTIFICAR
Interpretações	***Ameaças, tanto internas quanto externas, são identificadas e documentadas.***	ID.RA-3	Avaliação de Riscos (ID.RA)	ID.RA	IDENTIFICAR
Interpretações	***Uma linha de base das operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada.***	DE.AE-1	Anomalias e Eventos (DE.AE)	DE.AE)	DETECT
Interpretações	***Eventos detectados são analisados para entender os alvos e métodos de ataque.***	DE.AE-2	Anomalias e Eventos (DE.AE)	DE.AE)	DETECT
Interpretações	***Dados de eventos são coletados e correlacionados de várias fontes e sensores.***	DE.AE-3	Anomalias e Eventos (DE.AE)	DE.AE)	DETECT
Interpretações	***O impacto dos eventos é determinado.***	DE.AE-4	Anomalias e Eventos (DE.AE)	DE.AE)	DETECT
Interpretações	***Limites de alerta de incidentes são estabelecidos.***	DE.AE-5	Anomalias e Eventos (DE.AE)	DE.AE)	DETECT

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Interpretações	***A rede é monitorada para detectar possíveis eventos de segurança cibernética.***	DE.CM-1	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética.***	DE.CM-2	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética.***	DE.CM-3	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***Código malicioso é detectado.***	DE.CM-4	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***Código móvel não autorizado é detectado.***	DE.CM-5	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***A atividade do provedor de serviços externos é monitorada para detectar possíveis eventos de segurança cibernética.***	DE.CM-6	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***Monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado.***	DE.CM-7	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***Varreduras de vulnerabilidade são realizadas.***	DE.CM-8	Monitoramento Contínuo de Segurança (DE.CM)	DE.CM	DETECT
Interpretações	***Funções e responsabilidades para detecção são bem definidas para garantir responsabilidade.***	DE.DP-1	Processos de Detecção (DE.DP)	DE.DP	DETECT
Interpretações	***As atividades de detecção estão em conformidade com todos os requisitos aplicáveis.***	DE.DP-2	Processos de Detecção (DE.DP)	DE.DP	DETECT
Interpretações	***Os processos de detecção são testados.***	DE.DP-3	Processos de Detecção (DE.DP)	DE.DP	DETECT
Interpretações	***As informações de detecção de eventos são comunicadas.***	DE.DP-4	Processos de Detecção (DE.DP)	DE.DP	DETECT
Interpretações	***Os processos de detecção são continuamente melhorados.***	DE.DP-5	Processos de Detecção (DE.DP)	DE.DP	DETECT

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Conhecimento Explícito	***Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em sua classificação, criticidade e valor para o negócio.***	ID.AM-5	Gestão de Ativos (ID.AM)	ID.AM	IDENTIFICAR
Conhecimento Explícito	***Funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidas.***	ID.AM-6	Gestão de Ativos (ID.AM)	ID.AM	IDENTIFICAR
Conhecimento Explícito	***Prioridades para a missão, objetivos e atividades organizacionais são estabelecidas e comunicadas.***	ID.BE-3	Ambiente de Negócios (ID.BE):	ID.BE	IDENTIFICAR
Conhecimento Explícito	***Dependências e funções críticas para a entrega de serviços essenciais são estabelecidas.***	ID.BE-4	Ambiente de Negócios (ID.BE):	ID.BE	IDENTIFICAR
Conhecimento Explícito	***A política organizacional de cibersegurança é estabelecida e comunicada.***	ID.GV-1	Governança (ID.GV)	ID.GV	IDENTIFICAR
Conhecimento Explícito	***As funções e responsabilidades de cibersegurança são coordenadas e alinhadas com funções internas e parceiros externos.***	ID.GV-2	Governança (ID.GV)	ID.GV	IDENTIFICAR
Conhecimento Explícito	***Requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados.***	ID.GV-3	Governança (ID.GV)	ID.GV	IDENTIFICAR
Conhecimento Explícito	***Os processos de governança e gerenciamento de riscos abordam os riscos de cibersegurança.***	ID.GV-4	Governança (ID.GV)	ID.GV	IDENTIFICAR
Conhecimento Explícito	***Processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais.***	ID.RM-1	Estratégia de Gerenciamento de Riscos (ID.RM)	ID.RM	IDENTIFICAR

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Conhecimento Explícito	***Processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais.***	ID.SC-1	Gestão de Riscos na Cadeia de Suprimentos (ID.SC)	ID.SC	IDENTIFICAR
Conhecimento Explícito	***Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos.***	ID.SC-2	Gestão de Riscos na Cadeia de Suprimentos (ID.SC)	ID.SC	IDENTIFICAR
Conhecimento Explícito	***Contratos com fornecedores e parceiros terceirizados são utilizados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de cibersegurança de uma organização e ao Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos.***	ID.SC-3	Gestão de Riscos na Cadeia de Suprimentos (ID.SC)	ID.SC	IDENTIFICAR
Conhecimento Explícito	***Fornecedores e parceiros terceirizados são rotineiramente avaliados por meio de auditorias, resultados de testes ou outras formas de avaliação para confirmar que estão cumprindo suas obrigações contratuais.***	ID.SC-4	Gestão de Riscos na Cadeia de Suprimentos (ID.SC)	ID.SC	IDENTIFICAR
Conhecimento Explícito	***Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.***	PR.AC-1	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER
Conhecimento Explícito	***O acesso físico aos ativos é gerenciado e protegido.***	PR.AC-2	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER
Conhecimento Explícito	***O acesso remoto é gerenciado.***	PR.AC-3	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Conhecimento Explícito	***As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções.***	PR.AC-4	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER
Conhecimento Explícito	***A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).***	PR.AC-5	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER
Conhecimento Explícito	***As identidades são verificadas e vinculadas às credenciais e afirmadas nas interações.***	PR.AC-6	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER
Conhecimento Explícito	***Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) proporcionalmente ao risco da transação (por exemplo, riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais).***	PR.AC-7	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC)	PR.AC	PROTEGER
Conhecimento Explícito	***Todos os usuários são informados e treinados.***	PR.AT-1	Conscientização e Treinamento (PR.AT)	PR.AT	PROTEGER
Conhecimento Explícito	***Usuários privilegiados entendem seus papéis e responsabilidades.***	PR.AT-2	Conscientização e Treinamento (PR.AT)	PR.AT	PROTEGER
Conhecimento Explícito	***As partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) entendem seus papéis e responsabilidades.***	PR.AT-3	Conscientização e Treinamento (PR.AT)	PR.AT	PROTEGER
Conhecimento Explícito	***Executivos seniores entendem seus papéis e responsabilidades.***	PR.AT-4	Conscientização e Treinamento (PR.AT)	PR.AT	PROTEGER

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Conhecimento Explícito	***Pessoal de segurança física e cibernética entendem seus papéis e responsabilidades.***	PR.AT-5	Conscientização e Treinamento (PR.AT)	PR.AT	PROTEGER
Conhecimento Explícito	***Dados em repouso são protegidos.***	PR.DS-1	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Dados em trânsito são protegidos.***	PR.DS-2	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Os ativos são gerenciados formalmente durante a remoção, transferências e disposição.***	PR.DS-3	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Capacidade adequada para garantir a disponibilidade é mantida.***	PR.DS-4	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Proteções contra vazamentos de dados são implementadas.***	PR.DS-5	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Mecanismos de verificação de integridade são usados para verificar a integridade do software, firmware e informações.***	PR.DS-6	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***O ambiente de desenvolvimento e teste é separado do ambiente de produção.***	PR.DS-7	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Mecanismos de verificação de integridade são usados para verificar a integridade do hardware.***	PR.DS-8	Segurança de Dados (PR.DS)	PR.DS	PROTEGER
Conhecimento Explícito	***Uma configuração básica de sistemas de tecnologia da informação/sistemas de controle industrial é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).***	PR.IP-1	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Um Ciclo de Vida de Desenvolvimento de Sistemas para gerenciar sistemas é implementado.***	PR.IP-2	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Conhecimento Explícito	***Processos de controle de mudanças de configuração estão em vigor.***	PR.IP-3	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Backups de informações são realizados, mantidos e testados.***	PR.IP-4	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Políticas e regulamentos referentes ao ambiente operacional físico de ativos organizacionais são atendidos.***	PR.IP-5	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Os dados são destruídos de acordo com a política.***	PR.IP-6	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Os processos de proteção são aprimorados.***	PR.IP-7	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***A eficácia das tecnologias de proteção é compartilhada.***	PR.IP-8	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e são gerenciados.***	PR.IP-9	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Planos de resposta e recuperação são testados.***	PR.IP-10	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***A cibersegurança é incluída nas práticas de recursos humanos (por exemplo, desativação de contas, triagem de pessoal).***	PR.IP-11	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER
Conhecimento Explícito	***Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado.***	PR.IP-12	Processos e Procedimentos de Proteção da Informação (PR.IP)	PR.IP	PROTEGER

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Conhecimento Explícito	***A manutenção e reparo de ativos organizacionais são realizados e registrados, utilizando ferramentas aprovadas e controladas.***	PR.MA-1	Manutenção (PR.MA):	PR.MA	PROTEGER
Conhecimento Explícito	***A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a evitar acesso não autorizado.***	PR.MA-2	Manutenção (PR.MA):	PR.MA	PROTEGER
Conhecimento Explícito	***Registros de auditoria/sistema são determinados, documentados, implementados e revisados de acordo com a política.***	PR.PT-1	Tecnologia de Proteção (PR.PT)	PR.PT	PROTEGER
Conhecimento Explícito	***Mídias removíveis são protegidas, e seu uso é restrito de acordo com a política.***	PR.PT-2	Tecnologia de Proteção (PR.PT)	PR.PT	PROTEGER
Conhecimento Explícito	***O princípio da menor funcionalidade é incorporado configurando sistemas para fornecer apenas as capacidades essenciais.***	PR.PT-3	Tecnologia de Proteção (PR.PT)	PR.PT	PROTEGER
Conhecimento Explícito	***Redes de comunicação e controle são protegidas.***	PR.PT-4	Tecnologia de Proteção (PR.PT)	PR.PT	PROTEGER
Conhecimento Explícito	***Mecanismos (por exemplo, failsafe, balanceamento de carga, hot swap) são implementados para atender a requisitos de resiliência em situações normais e adversas.***	PR.PT-5	Tecnologia de Proteção (PR.PT)	PR.PT	PROTEGER
Conhecimento Explícito	***As notificações dos sistemas de detecção são investigadas.***	RS.AN-1	Análise (RS.AN)	RS.AN	RESPONDER
Conhecimento Explícito	***A perícia é realizada.***	RS.AN-3	Análise (RS.AN)	RS.AN	RESPONDER
Conhecimento Explícito	***Processos são estabelecidos para receber, analisar e responder a vulnerabilidades divulgadas à organização de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança).***	RS.AN-5	Análise (RS.AN)	RS.AN	RESPONDER
Conhecimento Explícito	***Os planos de resposta incorporam lições aprendidas.***	RS.IM-1	Mitigação (RS.MI)	RS.IM	RESPONDER
Conhecimento Explícito	***As estratégias de resposta são atualizadas.***	RS.IM-2	Mitigação (RS.MI)	RS.IM	RESPONDER
Conhecimento Explícito	***Os planos de recuperação incorporam lições aprendidas.***	RC.IM-1	Melhorias (RC.IM)	RC.IM	RECUPERAR
Conhecimento Explícito	***Estratégias de recuperação são atualizadas.***	RC.IM-2	Melhorias (RC.IM)	RC.IM	RECUPERAR

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Regras	***Requisitos de resiliência para apoiar a entrega de serviços críticos são estabelecidos para todos os estados operacionais (por exemplo, sob pressão/ataque, durante a recuperação, operações normais).***	ID.BE-5	Ambiente de Negócios (ID.BE):	ID.BE	IDENTIFICAR
Regras	***Impactos e probabilidades potenciais nos negócios são identificados.***	ID.RA-4	Avaliação de Riscos (ID.RA)	ID.RA	IDENTIFICAR
Regras	***Ameaças, vulnerabilidades, probabilidades e impactos são utilizados para determinar o risco.***	ID.RA-5	Avaliação de Riscos (ID.RA)	ID.RA	IDENTIFICAR
Regras	***Respostas ao risco são identificadas e priorizadas.***	ID.RA-6	Avaliação de Riscos (ID.RA)	ID.RA	IDENTIFICAR
Regras	***A tolerância a riscos organizacional é determinada e claramente expressa.***	ID.RM-2	Estratégia de Gerenciamento de Riscos (ID.RM)	ID.RM	IDENTIFICAR
Regras	***A determinação da tolerância a riscos da organização é informada pelo seu papel na infraestrutura crítica e na análise de riscos específicos do setor.***	ID.RM-3	Estratégia de Gerenciamento de Riscos (ID.RM)	ID.RM	IDENTIFICAR
Regras	***O plano de resposta é executado durante ou após um incidente.***	RS.RP-1	Planejamento de Resposta (RS.RP)	RS.RP	RESPONDER
Regras	***Planejamento e testes de resposta e recuperação são conduzidos com fornecedores e provedores terceirizados.***	ID.SC-5	Gestão de Riscos na Cadeia de Suprimentos (ID.SC)	ID.SC	IDENTIFICAR
Regras	***O pessoal conhece suas funções e ordem de operações quando uma resposta é necessária.***	RS.CO-1	Comunicações (RS.CO)	RS.CO	RESPONDER
Regras	***Os incidentes são relatados de acordo com os critérios estabelecidos.***	RS.CO-2	Comunicações (RS.CO)	RS.CO	RESPONDER
Regras	***As informações são compartilhadas de acordo com os planos de resposta.***	RS.CO-3	Comunicações (RS.CO)	RS.CO	RESPONDER

Quadro 6 - *Framework* de Teoria Adotada para Defesa Cibernética NIST CSF (conclusão)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética com base no NIST CSF	Nr-SubCat NIST	Categorias de Controles NIST CSF	Nr-Cat NIST	Funções de Controles NIST CSF
Regras	***A coordenação com as partes interessadas ocorre de acordo com os planos de resposta.***	RS.CO-4	Comunicações (RS.CO)	RS.CO	RESPONDER
Regras	***O compartilhamento voluntário de informações ocorre com partes interessadas externas para alcançar uma compreensão mais ampla da situação de segurança cibernética.***	RS.CO-5	Comunicações (RS.CO)	RS.CO	RESPONDER
Regras	***O impacto do incidente é compreendido.***	RS.AN-2	Análise (RS.AN)	RS.AN	RESPONDER
Regras	***Os incidentes são categorizados de acordo com os planos de resposta.***	RS.AN-4	Análise (RS.AN)	RS.AN	RESPONDER
Regras	***Os incidentes são contidos.***	RS.MI-1	Mitigação (RS.MI)	RS.MI	RESPONDER
Regras	***Os incidentes são mitigados.***	RS.MI-2	Mitigação (RS.MI)	RS.MI	RESPONDER
Regras	***As vulnerabilidades recém-identificadas são mitigadas ou documentadas como riscos aceitos.***	RS.MI-3	Mitigação (RS.MI)	RS.MI	RESPONDER
Regras	***O plano de recuperação é executado durante ou após um incidente de cibersegurança.***	RC.RP-1	Planejamento de Recuperação (RC.RP)	RC.RP	RECUPERAR
Regras	***Relações públicas são gerenciadas.***	RC.CO-1	Comunicações (RC.CO)	RC.CO	RECUPERAR
Regras	***A reputação é restaurada após um incidente.***	RC.CO-2	Comunicações (RC.CO)	RC.CO	RECUPERAR
Regras	***As atividades de recuperação são comunicadas às partes interessadas internas e externas, bem como às equipes executivas e de gerenciamento.***	RC.CO-3	Comunicações (RC.CO)	RC.CO	RECUPERAR

Fonte: Autor

Quadro 7 - *Framework* de Teoria Adotada para Defesa Cibernética MITRE ATTACK *Entreprise*

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	*Framework* de Teoria Adotada para Defesa Cibernética para com base no MITRE ATTACK Enterprice	Tática MITRE (Enterprise)	Nr-TP MITRE
Interpretações	*O atacante está tentando coletar informações que podem ser usadas para planejar operações futuras.*	Reconhecimento	1
Interpretações	*O atacante está tentando estabelecer recursos que podem ser usados para apoiar operações.*	Desenvolvimento de Recursos	2
Interpretações	*O atacante está tentando entrar na sua rede.*	Acesso Inicial	3
Interpretações	*O atacante está tentando roubar nomes de conta e senhas.*	Acesso a Credenciais	8
Interpretações	*O atacante está tentando reunir dados de interesse para seu objetivo.*	Coleta	11
Conhecimento Explícito	*O atacante está tentando estabelecer recursos que podem ser usados para apoiar operações.*	Acesso Inicial	3
Conhecimento Explícito	*O atacante está tentando executar código malicioso.*	Execução	4
Conhecimento Explícito	*O atacante está tentando manter sua posição.*	Persistência	5
Conhecimento Explícito	*O atacante está tentando obter permissões de nível mais alto.*	Escalação de Privilégios	6
Conhecimento Explícito	*O atacante está tentando evitar ser detectado.*	Evasão de Defesa	7
Conhecimento Explícito	*O atacante está tentando entender o seu ambiente.*	Descoberta	9
Conhecimento Explícito	*O atacante está tentando se deslocar através do seu ambiente.*	Movimentação Lateral	10
Conhecimento Explícito	*O atacante está tentando se comunicar com sistemas comprometidos para controlá-los.*	Comando e Controle	12
Conhecimento Explícito	*O atacante está tentando roubar dados.*	Exfiltração	13
Regras	*O atacante está tentando coletar informações que podem ser usadas para planejar operações futuras.*	Reconhecimento	1
Regras	*O atacante está tentando estabelecer recursos que podem ser usados para apoiar operações.*	Desenvolvimento de Recursos	2
Regras	*O atacante está tentando reunir dados de interesse para seu objetivo.*	Coleta	11
Regras	*O atacante está tentando manipular, interromper ou destruir seus sistemas e dados.*	Impacto	14

Fonte: Autor

5.3. OBJETIVO ESPECÍFICO (c)

Neste subtítulo são descritos os procedimentos para a execução do objetivo específico (c), qual seja, “Identificar e aplicar critérios para relacionar os elementos dos *frameworks* selecionados em relação ao ciclo de gestão do conhecimento de Choo (1998, p. 240) com os estágios de consciência situacional de Endsley (1995, p. 35) para primeira consolidação do *framework* a ser produzido na pesquisa”. Para tal, procedeu-se o registro dos resultados das tarefas (c.1) e (c.2), conforme consta no Quadro 4, no capítulo de Metodologia.

5.3.1. Tarefas (c.1) e (c.2)

A tarefa (c.1) teve por finalidade declarar o critério para relacionar os elementos do *framework* de teoria adotada para defesa cibernética e os estágios da consciência situacional, conforme recortes estabelecidos no referencial teórico. Nesse sentido, o critério serviu de via pela qual se pôde percorrer os controles e táticas do *framework* obtido no objetivo (b), agrupando-os segundo os estágios da consciência situacional, conforme modelo de Endsley (1995).

Analogamente ao que ocorreu no objetivo específico (b), mostrou-se necessário elaborar um critério composto por subcritérios, resultando em uma composição de nove desses critérios componentes. Conforme Quadro 8, os subcritérios relacionados aos insumos metas, objetivos e perspectivas (Pe1-C1, Co1-C1 e Pr1-C1) serviram tanto para controles quanto para as táticas do *framework* de teoria adotada para defesa cibernética. Os demais subcritérios do critério 1 foram aplicáveis especificamente para os controles (segurança cibernética) do *framework* de teoria adotada para DC, enquanto os subcritérios do controle 2 serviram para as táticas (exploração e ataque). Por fim, o critério 3 serviu a todos os elementos do *framework*.

Os Quadros 9 e 10 sintetizam a aplicação dos critérios declarados na tarefa (c1) relacionando os controles do *framework* de teoria adotada para defesa cibernética com os estágios de consciência situacional, conforme definidos por Endsley (1995), apresentando a proposição estabelecida nesta pesquisa que é um *framework* para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética (NIP-CS-DC). Cada

NIP-CS-DC é identificada no formato X-NIP_nr, Onde X pode ser N (NIST CSF) ou M (MITRE), enquanto nr simboliza a numeração da NIP-CS-DC. Para fins de simplificação na redação neste documento de tese, eventualmente, se usou NIP ao invés de NIP-CS-DC.

A quantidade de NIP com base no NIST CSF, no Quadro 9, naturalmente coincide com o total de controles desse *framework*, no entanto, pode-se notar que diversas NIP se repetem, como, por exemplo, a N-NIP_5. Isso ocorreu porque os controles correspondentes foram considerados como contribuindo com pesos aproximadamente iguais em cada estágio da CS.

Quadro 8 - Critérios para relacionamentos enunciados na tarefa (c1)

ASPECTO CS	DEFINIÇÃO	INSUMOS	DEFINÇÃO DO INSUMO	ESTÁGIO DE CS	PERGUNTA DO CRITÉRIO	CRITÉRIO 1	ID Critério	CRITÉRIO 2	ID Critério	CRITÉRIO 3
PRÉ-ATENÇÃO	Processamento que busca notar no ambiente observado características dos elementos que compõem esse ambiente e que chamam a atenção para eles.	**Metas, Objetivos e Perspectivas**	Parâmetros estabelecidos *a priori* em relação a uma situação a ser observada.	**PERCEPÇÃO**	Que necessidades informacionais primordiais podem ser derivadas dos controles do *framework* de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo *schematas* de pré-atenção para parâmetros estabelecidos *a priori* em relação a operação cibernética?	O controle recomenda ações de elaboração ou aplicação de *schematas* para estabelecimento de metas, objetivos ou de elementos similares elaborados *a priori* para referenciar a operação e que sejam relevantes à pré-atenção.	Pe-C1	------	------	Expressão da necessidade informacional primordial de defesa cibernética (NIP-DC) em formato de pergunta, estruturada de modo que adapte a redação do texto do controle associado ao *schemata* escolhido para refletir a necessidade a ser considerada como ponto de partida para ações ou operações de defesa cibernética.
PRÉ-ATENÇÃO	Idem	***Schematas* de pré-atenção**	Estruturas de representação sob as quais sistemas de informação, mesmo os complexos, podem ser interpretados e representados de modo simplificado e aplicáveis na pré-atenção.	**PERCEPÇÃO**	Que necessidades informacionais primordiais podem ser derivadas dos controles do *framework* de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo *schematas*, as quais viabilizam ou realizam a pré-atenção necessária para identificação de eventos de segurança cibernética no espaço cibernético de interesse da operação cibernética?	O controle recomenda ações de elaboração ou aplicação de *schematas* para realizar ou viabilizar a percepção (pré-atenção) de eventos de interesse no espaço cibernético.	Pe-C2	O controle recomenda ações de elaboração ou aplicação de *schematas* para realizar ou viabilizar a percepção (pré-atenção) de indícios ou constatações de que um ataque contra um alvo está sendo viabilizado.	Pe-C3	Idem.
MEMÓRIA DE LONGO PRAZO	Repositório de onde a mente humana pode recuperar conhecimentos dominados os quais desempenham papel fundamental no reconhecimento de padrões, estabelecimento de categorizações, aplicação de regras, técnicas e controles, além de diversos outras possibilidades de consubstanciar o uso de conhecimentos em relação à situação corrente.	**Metas, Objetivos e Perspectivas**	Parâmetros estabelecidos *a priori* em relação a uma situação a ser observada.	**COMPREENSÃO**	Que necessidades informacionais primordiais podem ser derivadas dos controles do *framework* de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo *schematas* para a memória de longo prazo de parâmetros estabelecidos *a priori* em relação a operação cibernética?	O controle recomenda ações de elaboração ou aplicação de metas, objetivos ou de elementos similares elaborados *a priori* para referenciar a operação, servindo de parâmetro para verificar alinhamento da compreensão à finalidade da operação.	C-C1	------	C-C1	Idem.
MEMÓRIA DE LONGO PRAZO	Idem	***Schematas* de memória de longo prazo**	Estruturas de representação sob as quais sistemas de informação, mesmo os complexos, podem ser interpretados e representados de modo simplificado aplicáveis pela memória de longo prazo.	**COMPREENSÃO**	Que necessidades informacionais primordiais podem ser derivadas dos controles do *framework* de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo *schematas* para a memória de longo prazo necessários à compreensão de eventos de segurança cibernética?	O controle recomenda ações de elaboração ou aplicação de *schematas* para compreensão (*) de eventos de interesse no espaço cibernético. (*) Reconhecimento de padrões, estabelecimento de categorizações, aplicação de regras, técnicas e controles inerentes a aplicação de controles de defesa cibernética, além de diversos outras possibilidades de consubstanciar o uso de conhecimentos em relação à situação corrente.	C-C2	O controle recomenda ações de elaboração ou aplicação de *schematas* para realizar ou viabilizar por adaptação contínua de um ataque contra um alvo.	C-C2	Idem.
MEMÓRIA DE LONGO PRAZO	Idem	**Metas, Objetivos e Perspectivas**	Parâmetros estabelecidos *a priori* em relação a uma situação a ser observada.	**PROJEÇÃO**	Que necessidades informacionais primordiais podem ser derivadas dos controles do *framework* de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo *schematas* para a memória de longo prazo de parâmetros estabelecidos *a priori* em relação a operação cibernética?	O controle recomenda ações de elaboração ou aplicação de *schematas* para projeção (*) de eventos de interesse no espaço cibernético. (*) Habilidade de projetar as ações dos elementos do ambiente como consequência direta do conhecimento do estado e da dinâmica desses elementos e da compreensão da situação corrente, conforme as quatro áreas da segurança cibernética delineadas no referencial teórico.	Pr-C1	------	Pr-C1	Idem.
MEMÓRIA DE LONGO PRAZO	Idem	***Schematas* de memória de longo prazo**	Estruturas de representação sob as quais sistemas de informação, mesmo os complexos, podem ser interpretados e representados de modo simplificado aplicáveis pela memória de longo prazo.	**PROJEÇÃO**	Que necessidades informacionais primordiais podem ser derivadas dos controles do *framework* de teoria adotada para defesa cibernética que, uma vez satisfeitas, podem gerar estruturas de representação do tipo *schematas* para a memória de longo prazo necessários à projeção dos desdobramentos de eventos de segurança cibernética?	O controle recomenda ações de elaboração ou aplicação de *schemats* para projeção (*) de eventos de interesse no espaço cibernético. (*) Habilidade de projetar as ações dos elementos do ambiente como consequência direta do conhecimento do estado e da dinâmica desses elementos e da compreensão da situação corrente.	Pr-C2	O controle recomenda ações de elaboração ou aplicação de *schematas* para avaliar que possibilidades podem ser ativadas ou geradas para continuação ou conclusão de ataques contra um alvo.	Pr-C2	Idem.

Fonte: Autor

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Interpretações	*Dispositivos físicos e sistemas dentro da organização são inventariados.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_1	*Quais os ativos informacionais internos físicos e de sistemas relevantes para a operação a serem inventariados?*
Interpretações	*Plataformas de software e aplicações dentro da organização são inventariadas.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_2	*Quais os ativos informacionais internos de aplicações e de software relevantes para a operação a serem inventariados?*
Interpretações	*Comunicações organizacionais e fluxos de dados são mapeados.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_3	*Quais são as comunicações e fluxos informacionais a serem mapeados?*
Interpretações	*Sistemas de informação externos são catalogados.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_4	*Quais os sistemas de informação externos a serem catalogados?*
Interpretações	*O papel da organização na cadeia de suprimentos é identificado e comunicado.*	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_5	*Qual o papel da organização na cadeia de suprimentos envolvida na operação e para quem deve ser comunicado?*
Interpretações	*O papel da organização na cadeia de suprimentos é identificado e comunicado.*	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_5	*Qual o papel da organização na cadeia de suprimentos envolvida na operação e para quem deve ser comunicado?*
Interpretações	*O papel da organização na cadeia de suprimentos é identificado e comunicado.*	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_5	*Qual o papel da organização na cadeia de suprimentos envolvida na operação e para quem deve ser comunicado?*
Interpretações	*A posição da organização na infraestrutura crítica e em seu setor industrial é identificada e comunicada.*	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_6	*(Apenas para organizaões consideradas IEC) Qual a posição da organização na infraestrutura crítica e em seu setor industrial e para quem deve ser comunicada?*
Interpretações	*A posição da organização na infraestrutura crítica e em seu setor industrial é identificada e comunicada.*	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_6	*(Apenas para organizaões consideradas IEC) Qual a posição da organização na infraestrutura crítica e em seu setor industrial e para quem deve ser comunicada?*
Interpretações	*A posição da organização na infraestrutura crítica e em seu setor industrial é identificada e comunicada.*	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_6	*(Apenas para organizaões consideradas IEC) Qual a posição da organização na infraestrutura crítica e em seu setor industrial e para quem deve ser comunicada?*
Interpretações	*As vulnerabilidades dos ativos são identificadas e documentadas.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_7	*Quais são as vulnerabilidades dos ativos que devem ser identificadas e documentadas?*
Interpretações	*Inteligência de ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações.*	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_8	*Quais os foruns e fontes de compartilhamento de informações sobre ameaças cibernéticas são relevantes para a missão?*
Interpretações	*Inteligência de ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações.*	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_8	*Quais os foruns e fontes de compartilhamento de informações sobre ameaças cibernéticas são relevantes para a missão?*
Interpretações	*Inteligência de ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações.*	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_8	*Quais os foruns e fontes de compartilhamento de informações sobre ameaças cibernéticas são relevantes para a missão?*
Interpretações	*Ameaças, tanto internas quanto externas, são identificadas e documentadas.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_9	*Quais são as ameaças internas e externas a serem identificadas e documentadas?*
Interpretações	*Uma linha de base das operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada.*	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_10	*Quais as linhas de base das operações de rede e fluxos de dados esperados para usuários e sistemas devem ser estabelecidas e gerenciadas?*

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Interpretações	***Eventos detectados são analisados para entender os alvos e métodos de ataque.***	MLP	COMPREENSÃO	C-C2.	N-NIP_11	***Que requisitos são necessários para especificar uma estrutura para detectar e analisar eventos para entender os alvos e métodos de ataque?***
Interpretações	***Dados de eventos são coletados e correlacionados de várias fontes e sensores.***	MLP	COMPREENSÃO	C-C2.	N-NIP_12	***Que tipos de dados de eventos devem ser coletados e correlacionados e quais as fontes e sensores devem ser usadas?***
Interpretações	***O impacto dos eventos é determinado.***	MLP	COMPREENSÃO	C-C2.	N-NIP_13	***Que critérios de impacto dos eventos são adequados para a operação?***
Interpretações	***Limites de alerta de incidentes são estabelecidos.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_14	***Que critérios devem ser usados para estabelecer um esquema de categorias de alertas de incidentese com respectivos limites e ações?***
Interpretações	***A rede é monitorada para detectar possíveis eventos de segurança cibernética.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_15	***Que redes devem ser monitoradas para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?***
Interpretações	***O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_16	***Que ambientes físicos devem ser monitorados para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?***
Interpretações	***A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_17	***Que tipo de atividade de pessoal deve ser monitorado para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?***
Interpretações	***Código malicioso é detectado.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_18	***Que métodos e tecnologias devem ser empregadas para detecção de código malicioso?***
Interpretações	***Código malicioso é detectado.***	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_18	***Que métodos e tecnologias devem ser empregadas para detecção de código malicioso?***
Interpretações	***Código malicioso é detectado.***	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_18	***Que métodos e tecnologias devem ser empregadas para detecção de código malicioso?***
Interpretações	***Código móvel não autorizado é detectado.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_19	***Que métodos e tecnologias devem ser empregadas para detecção de código móvel não autorizado?***
Interpretações	***Código móvel não autorizado é detectado.***	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_19	***Que métodos e tecnologias devem ser empregadas para detecção de código móvel não autorizado?***
Interpretações	***Código móvel não autorizado é detectado.***	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_19	***Que métodos e tecnologias devem ser empregadas para detecção de código móvel não autorizado?***
Interpretações	***A atividade do provedor de serviços externos é monitorada para detectar possíveis eventos de segurança cibernética.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_20	***Que tipo de atividade de provedor de serviços externos deve ser monitorado para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?***
Interpretações	***Monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_21	***Que tipo de atividade de monitoração de pessoal, conexões, dispositivos e software não autorizados deve ser realizada para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?***
Interpretações	***Varreduras de vulnerabilidade são realizadas.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_22	***Que tipo de varreduras de vulnerabilidade devem ser realizadas?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Interpretações	***Funções e responsabilidades para detecção são bem definidas para garantir responsabilidade.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_23	***Que tipo de funções e atribuições para detecção devem ser definidas para garantir responsabilidade?***
Interpretações	***As atividades de detecção estão em conformidade com todos os requisitos aplicáveis.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_24	***Que critérios de conformidade devem ser adotados para se verificar se as atividades de detecção estão em conformidade com todos os requisitos aplicáveis?***
Interpretações	***Os processos de detecção são testados.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_25	***Que tipo de testes devem ser aplicados e mantidos para os processos de detecção?***
Interpretações	***As informações de detecção de eventos são comunicadas.***	MLP	PROJEÇÃO	Pe-C2.	N-NIP_26	***Que processos de compartilhamento da informação devem ser realizados sobre eventos detectados no espaço cibernético da operação?***
Interpretações	***Os processos de detecção são continuamente melhorados.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_27	***Como os processos de detecção devem ser continuamente melhorados?***
Conhecimento Explícito	***Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em sua classificação, criticidade e valor para o negócio.***	Pré-atenção	PERCEPÇÃO	Pe-C2.	N-NIP_28	***Como deve ser organizada uma sistemática de priorização de recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software), tendo por base a sua classificação, criticidade e valor para o negócio?***
Conhecimento Explícito	***Funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidas.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_29	***Que funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros devem ser estabelecidas?***
Conhecimento Explícito	***Funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidas.***	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_29	***Que funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros devem ser estabelecidas?***
Conhecimento Explícito	***Funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidas.***	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_29	***Que funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros devem ser estabelecidas?***
Conhecimento Explícito	***Prioridades para a missão, objetivos e atividades organizacionais são estabelecidas e comunicadas.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_30	***Quais são as prioridades para a missão, objetivos e atividades organizacionais a serem estabelecidas e comunicadas?***
Conhecimento Explícito	***Prioridades para a missão, objetivos e atividades organizacionais são estabelecidas e comunicadas.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_30	***Quais são as prioridades para a missão, objetivos e atividades organizacionais a serem estabelecidas e comunicadas?***
Conhecimento Explícito	***Prioridades para a missão, objetivos e atividades organizacionais são estabelecidas e comunicadas.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_30	***Quais são as prioridades para a missão, objetivos e atividades organizacionais a serem estabelecidas e comunicadas?***
Conhecimento Explícito	***Dependências e funções críticas para a entrega de serviços essenciais são estabelecidas.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS-C2.	N-NIP_31	***Quais são os serviços essenciais que sustentam a infraestrutura da operação e quais sãos as dependências e funções críticas para o seu provimento?***
Conhecimento Explícito	***Dependências e funções críticas para a entrega de serviços essenciais são estabelecidas.***	Pré-atenção, MLP	COMPREENSÃO	TODOS-C2.	N-NIP_31	***Quais são os serviços essenciais que sustentam a infraestrutura da operação e quais sãos as dependências e funções críticas para o seu provimento?***
Conhecimento Explícito	***Dependências e funções críticas para a entrega de serviços essenciais são estabelecidas.***	Pré-atenção, MLP	PROJEÇÃO	TODOS-C2.	N-NIP_31	***Quais são os serviços essenciais que sustentam a infraestrutura da operação e quais sãos as dependências e funções críticas para o seu provimento?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Conhecimento Explícito	***A política organizacional de cibersegurança é estabelecida e comunicada.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_32	***A política organizacional de cibersegurança está estabelecida e comunicada?***
Conhecimento Explícito	***A política organizacional de cibersegurança é estabelecida e comunicada.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_32	***A política organizacional de cibersegurança está estabelecida e comunicada?***
Conhecimento Explícito	***A política organizacional de cibersegurança é estabelecida e comunicada.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_32	***A política organizacional de cibersegurança está estabelecida e comunicada?***
Conhecimento Explícito	***As funções e responsabilidades de cibersegurança são coordenadas e alinhadas com funções internas e parceiros externos.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_33	***Quais as funções e responsabilidades de cibersegurança, funções internas e parceiros externos devem ser coordenadas e alinhadas?***
Conhecimento Explícito	***As funções e responsabilidades de cibersegurança são coordenadas e alinhadas com funções internas e parceiros externos.***	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_33	***Quais as funções e responsabilidades de cibersegurança, funções internas e parceiros externos devem ser coordenadas e alinhadas?***
Conhecimento Explícito	***As funções e responsabilidades de cibersegurança são coordenadas e alinhadas com funções internas e parceiros externos.***	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_33	***Quais as funções e responsabilidades de cibersegurança, funções internas e parceiros externos devem ser coordenadas e alinhadas?***
Conhecimento Explícito	***Requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_34	***Quais são os requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis devem ser compreendidos e gerenciados?***
Conhecimento Explícito	***Requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_34	***Quais são os requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis devem ser compreendidos e gerenciados?***
Conhecimento Explícito	***Requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis, são compreendidos e gerenciados.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_34	***Quais são os requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis devem ser compreendidos e gerenciados?***
Conhecimento Explícito	***Os processos de governança e gerenciamento de riscos abordam os riscos de cibersegurança.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_35	***Quais os riscos de cibersegurança são abordados nos processos de governança e gerenciamento de riscos?***
Conhecimento Explícito	***Os processos de governança e gerenciamento de riscos abordam os riscos de cibersegurança.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_35	***Quais os riscos de cibersegurança são abordados nos processos de governança e gerenciamento de riscos?***
Conhecimento Explícito	***Os processos de governança e gerenciamento de riscos abordam os riscos de cibersegurança.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_35	***Quais os riscos de cibersegurança são abordados nos processos de governança e gerenciamento de riscos?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Conhecimento Explícito	***Processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_36	***Quais os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais e quais outras são necessários?***
Conhecimento Explícito	***Processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_36	***Quais os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais e quais outras são necessários?***
Conhecimento Explícito	***Processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_36	***Quais os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais e quais outras são necessários?***
Conhecimento Explícito	***Processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	TODOS	N-NIP_37	***Quais os processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais e quais outros são necessários?***
Conhecimento Explícito	***Processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	TODOS	N-NIP_37	***Quais os processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais e quais outros são necessários?***
Conhecimento Explícito	***Processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	TODOS	N-NIP_37	***Quais os processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais e quais outros são necessários?***
Conhecimento Explícito	***Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	TODOS	N-NIP_38	***Quais fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos e quais outros também o devem ser?***
Conhecimento Explícito	***Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	TODOS	N-NIP_38	***Quais fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos e quais outros também o devem ser?***
Conhecimento Explícito	***Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	TODOS	N-NIP_38	***Quais fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos e quais outros também o devem ser?***
Conhecimento Explícito	***Contratos com fornecedores e parceiros terceirizados são utilizados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de cibersegurança de uma organização e ao Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	TODOS	N-NIP_39	***Os objetivos do programa de cibersegurança da organização envolvida na operação e Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos são atendidos nos contratos com fornecedores e parceiros terceirizados?***
Conhecimento Explícito	***Contratos com fornecedores e parceiros terceirizados são utilizados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de cibersegurança de uma organização e ao Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	TODOS	N-NIP_39	***Os objetivos do programa de cibersegurança da organização envolvida na operação e Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos são atendidos nos contratos com fornecedores e parceiros terceirizados?***
Conhecimento Explícito	***Contratos com fornecedores e parceiros terceirizados são utilizados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de cibersegurança de uma organização e ao Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	TODOS	N-NIP_39	***Os objetivos do programa de cibersegurança da organização envolvida na operação e Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos são atendidos nos contratos com fornecedores e parceiros terceirizados?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Conhecimento Explícito	***Fornecedores e parceiros terceirizados são rotineiramente avaliados por meio de auditorias, resultados de testes ou outras formas de avaliação para confirmar que estão cumprindo suas obrigações contratuais.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	TODOS	N-NIP_40	***Que avaliações por meio de auditorias, resultados de testes ou outras formas de avaliação, fornecedores e parceiros terceirizados devem ser rotineiramente avaliados para confirmar que estão cumprindo suas obrigações contratuais?***
Conhecimento Explícito	***Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.***	MLP	COMPREENSÃO	C-C2.	N-NIP_41	***Quais são as identidades e credenciais a serem emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados?***
Conhecimento Explícito	***O acesso físico aos ativos é gerenciado e protegido.***	MLP	COMPREENSÃO	C-C2.	N-NIP_42	***Quais são os acessos físicos aos ativos a serem gerenciados e protegidos?***
Conhecimento Explícito	***O acesso remoto é gerenciado.***	MLP	COMPREENSÃO	C-C2.	N-NIP_43	***Quais serão os acessos remotos necessários e qual a forma de gerenciamento deve ser empregada?***
Conhecimento Explícito	***As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções.***	MLP	COMPREENSÃO	C-C2.	N-NIP_44	***Quais as permissões e autorizações de acesso incorporando os princípios de privilégio mínimo e separação de funções devem ser estabelecidas e gerenciadas?***
Conhecimento Explícito	***A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).***	MLP	COMPREENSÃO	C-C2.	N-NIP_45	***Quais ações para proteger a integridade da rede devem ser realizadas?***
Conhecimento Explícito	***As identidades são verificadas e vinculadas às credenciais e afirmadas nas interações.***	MLP	COMPREENSÃO	C-C2.	N-NIP_46	***Quais as ações para verificar as identidades e as vincular às respectivas credenciais?***
Conhecimento Explícito	***Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) proporcionalmente ao risco da transação (por exemplo, riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais).***	MLP	COMPREENSÃO	C-C2.	N-NIP_47	***O que é necessário para autenticar usuários, dispositivos e outros ativos proporcionalmente ao risco da transação?***
Conhecimento Explícito	***Todos os usuários são informados e treinados.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_48	***Quais informações e treinamentos devem ser dados aos usuários?***
Conhecimento Explícito	***Todos os usuários são informados e treinados.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_48	***Quais informações e treinamentos devem ser dados aos usuários?***
Conhecimento Explícito	***Todos os usuários são informados e treinados.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_48	***Quais informações e treinamentos devem ser dados aos usuários?***
Conhecimento Explícito	***Usuários privilegiados entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_49	***Usuários privilegiados entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***Usuários privilegiados entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_49	***Usuários privilegiados entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***Usuários privilegiados entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_49	***Usuários privilegiados entendam seus papéis e responsabilidades?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Conhecimento Explícito	***As partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_50	***O que deve se realizado para que as partes interessadas de terceiros entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***As partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_50	***O que deve se realizado para que as partes interessadas de terceiros entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***As partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_50	***O que deve se realizado para que as partes interessadas de terceiros entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***Executivos seniores entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_51	***O que deve se realizado para que executivos seniores entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***Executivos seniores entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_51	***O que deve se realizado para que executivos seniores entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***Executivos seniores entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_51	***O que deve se realizado para que executivos seniores entendam seus papéis e responsabilidades?***
Conhecimento Explícito	***Pessoal de segurança física e cibernética entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_52	***O que deve se realizado para que o pessoal de segurança física e cibernética entendem seus papéis e responsabilidades?***
Conhecimento Explícito	***Pessoal de segurança física e cibernética entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_52	***O que deve se realizado para que o pessoal de segurança física e cibernética entendem seus papéis e responsabilidades?***
Conhecimento Explícito	***Pessoal de segurança física e cibernética entendem seus papéis e responsabilidades.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_52	***O que deve se realizado para que o pessoal de segurança física e cibernética entendem seus papéis e responsabilidades?***
Conhecimento Explícito	***Dados em repouso são protegidos.***	MLP	COMPREENSÃO	C-C2.	N-NIP_53	***Quais ações devem ser realizadas para proteger dados em repouso?***
Conhecimento Explícito	***Dados em trânsito são protegidos.***	MLP	COMPREENSÃO	C-C2.	N-NIP_54	***Quais ações devem ser realizadas para proteger dados em trânsito?***
Conhecimento Explícito	***Os ativos são gerenciados formalmente durante a remoção, transferências e disposição.***	MLP	COMPREENSÃO	C-C2.	N-NIP_55	***O que é necessário para formalmente gerenciar os ativos de dados durante a remoção, transferências e disposição?***
Conhecimento Explícito	***Capacidade adequada para garantir a disponibilidade é mantida.***	MLP	COMPREENSÃO	C-C2.	N-NIP_56	***O que é necessário para manter a capacidade adequada para garantir a disponibilidade?***
Conhecimento Explícito	***Proteções contra vazamentos de dados são implementadas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_57	***Que proteções contra vazamentos de dados devem ser implementadas?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Conhecimento Explícito	*Mecanismos de verificação de integridade são usados para verificar a integridade do software, firmware e informações.*	MLP	COMPREENSÃO	C-C2.	N-NIP_58	*Quais mecanismos de verificação de integridade são usados para verificar a integridade do software, firmware e informações?*
Conhecimento Explícito	*O ambiente de desenvolvimento e teste é separado do ambiente de produção.*	MLP	COMPREENSÃO	C-C2.	N-NIP_59	*Que é necessário realizar para criar e manter ambientes de desenvolvimento e teste separados do ambiente de produção?*
Conhecimento Explícito	*Mecanismos de verificação de integridade são usados para verificar a integridade do hardware.*	MLP	COMPREENSÃO	C-C2.	N-NIP_60	*Que mecanismos de verificação de integridade devem ser usados para verificar a integridade do hardware?*
Conhecimento Explícito	*Uma configuração básica de sistemas de tecnologia da informação/sistemas de controle industrial é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).*	MLP	COMPREENSÃO	C-C2.	N-NIP_61	*O que é necessário para criar e manter uma configuração básica de sistemas de tecnologia da informação/sistemas de controle industrial, incorporando princípios de segurança?*
Conhecimento Explícito	*Um Ciclo de Vida de Desenvolvimento de Sistemas para gerenciar sistemas é implementado.*	MLP	COMPREENSÃO	C-C2.	N-NIP_62	*Qual deve ser o Ciclo de Vida de Desenvolvimento de Sistemas empregado na gerência de sistemas empregados na operação?*
Conhecimento Explícito	*Processos de controle de mudanças de configuração estão em vigor.*	MLP	COMPREENSÃO	C-C2.	N-NIP_63	*Quais pocessos de controle de mudanças de configuração devem estar em vigor?*
Conhecimento Explícito	*Backups de informações são realizados, mantidos e testados.*	MLP	COMPREENSÃO	C-C2.	N-NIP_64	*Quais informações devem possuir backups e que processos devem ser realizados para mantê-los testá-los?*
Conhecimento Explícito	*Políticas e regulamentos referentes ao ambiente operacional físico de ativos organizacionais são atendidos.*	MLP	COMPREENSÃO	C-C2.	N-NIP_65	*Que ações são necessárias para que políticas e regulamentos referentes ao ambiente operacional físico de ativos organizacionais sejam atendidos?*
Conhecimento Explícito	*Os dados são destruídos de acordo com a política.*	MLP	COMPREENSÃO	C-C2.	N-NIP_66	*Que processo deve ser realizado para que os dados sejam destruídos de acordo com a política?*
Conhecimento Explícito	*Os processos de proteção são aprimorados.*	MLP	COMPREENSÃO	C-C2.	N-NIP_67	*O que é necessário para aprimorar os processos de proteção?*
Conhecimento Explícito	*A eficácia das tecnologias de proteção é compartilhada.*	MLP	COMPREENSÃO	C-C2.	N-NIP_68	*Como compartilhar a eficácia das tecnologias de proteção?*
Conhecimento Explícito	*Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e são gerenciados.*	MLP	COMPREENSÃO	C-C2.	N-NIP_69	*O que é necessário para manter em vigor e gerenciar os Planos de Resposta a Incidentes e Continuidade de Negócios e os planos de Recuperação de Incidentes e Recuperação de Desastres?*
Conhecimento Explícito	*Planos de resposta e recuperação são testados.*	MLP	COMPREENSÃO	C-C2.	N-NIP_70	*O que é necesário para testear os planos de resposta e recuperação?*
Conhecimento Explícito	*A cibersegurança é incluída nas práticas de recursos humanos (por exemplo, desativação de contas, triagem de pessoal).*	MLP	COMPREENSÃO	C-C2.	N-NIP_71	*O que é necessário para incluir a cibersegurança nas práticas de recursos humanos?*
Conhecimento Explícito	*Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado.*	MLP	COMPREENSÃO	C-C2.	N-NIP_72	*O que é necessário para desenvolver e implementar um plano de gerenciamento de vulnerabilidades?*
Conhecimento Explícito	*A manutenção e reparo de ativos organizacionais são realizados e registrados, utilizando ferramentas aprovadas e controladas.*	MLP	COMPREENSÃO	C-C2.	N-NIP_73	*O que é necessário para que a manutenção e reparo de ativos organizacionais sejam realizados e registrados, utilizando ferramentas aprovadas e controladas?*
Conhecimento Explícito	*A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a evitar acesso não autorizado.*	MLP	COMPREENSÃO	C-C2.	N-NIP_74	*O que é necessário para aprovar, registrar e realizar a manutenção remota de ativos organizacionais, evitando acesso não autorizado?*
Conhecimento Explícito	*Registros de auditoria/sistema são determinados, documentados, implementados e revisados de acordo com a política.*	MLP	COMPREENSÃO	C-C2.	N-NIP_75	*O que é necessário para determinar, documentar, implementar e revisar registros de auditoria/sistema de acordo com a política?*

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Conhecimento Explícito	***Mídias removíveis são protegidas, e seu uso é restrito de acordo com a política.***	MLP	COMPREENSÃO	C-C2.	N-NIP_76	***O que é necessário para proteger mídias removíveis e restringir o seu uso de acordo com a política?***
Conhecimento Explícito	***O princípio da menor funcionalidade é incorporado configurando sistemas para fornecer apenas as capacidades essenciais.***	MLP	COMPREENSÃO	C-C2.	N-NIP_77	***O que é necessário para incorporar o princípio da menor funcionalidade configurando sistemas para fornecer apenas as capacidades essenciais?***
Conhecimento Explícito	***Redes de comunicação e controle são protegidas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_78	***O que é necessário para proteger as redes de comunicação e controle da operação?***
Conhecimento Explícito	***Mecanismos (por exemplo, failsafe, balanceamento de carga, hot swap) são implementados para atender a requisitos de resiliência em situações normais e adversas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_79	***Quais devem ser os requisitos de resiliências e os respectivos mecanismos (por exemplo, failsafe, balanceamento de carga, hot swap) a serem implementados para utilização em situações normais e adversas?***
Conhecimento Explícito	***As notificações dos sistemas de detecção são investigadas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_80	***O que é necessário para investigar as notificações dos sistemas de detecção?***
Conhecimento Explícito	***A perícia é realizada.***	MLP	COMPREENSÃO	C-C2.	N-NIP_81	***O que é necessário para realizar a perícia?***
Conhecimento Explícito	***Processos são estabelecidos para receber, analisar e responder a vulnerabilidades divulgadas à organização de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança).***	MLP	COMPREENSÃO	C-C2.	N-NIP_82	***O que é necessário para sistematicamente receber, analisar e responder a vulnerabilidades informadas à organização de fontes internas e externas?***
Conhecimento Explícito	***Os planos de resposta incorporam lições aprendidas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_83	***O que é necessário para incorporar lições aprendidas aos planos de resposta?***
Conhecimento Explícito	***As estratégias de resposta são atualizadas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_84	***O que é necessário para atualizar as estratégias de respostas?***
Conhecimento Explícito	***Os planos de recuperação incorporam lições aprendidas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_85	***O que é necessário para incorporar lições aprendidas aos planos de recuperação?***
Conhecimento Explícito	***Estratégias de recuperação são atualizadas.***	MLP	COMPREENSÃO	C-C2.	N-NIP_86	***O que é necessário para atualizar as estratégias de recuperação?***
Regras	***Requisitos de resiliência para apoiar a entrega de serviços críticos são estabelecidos para todos os estados operacionais (por exemplo, sob pressão/ataque, durante a recuperação, operações normais).***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_87	***Quais são os requisitos de resiliência que devem ser estabelecidos para todos os estados operacionais para apoiar a entrega de serviços críticos (por exemplo, sob pressão/ataque, durante a recuperação, operações normais)?***
Regras	***Requisitos de resiliência para apoiar a entrega de serviços críticos são estabelecidos para todos os estados operacionais (por exemplo, sob pressão/ataque, durante a recuperação, operações normais).***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_87	***Quais são os requisitos de resiliência que devem ser estabelecidos para todos os estados operacionais para apoiar a entrega de serviços críticos (por exemplo, sob pressão/ataque, durante a recuperação, operações normais)?***
Regras	***Requisitos de resiliência para apoiar a entrega de serviços críticos são estabelecidos para todos os estados operacionais (por exemplo, sob pressão/ataque, durante a recuperação, operações normais).***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_87	***Quais são os requisitos de resiliência que devem ser estabelecidos para todos os estados operacionais para apoiar a entrega de serviços críticos (por exemplo, sob pressão/ataque, durante a recuperação, operações normais)?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Regras	***Impactos e probabilidades potenciais nos negócios são identificados.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_88	***Que impactos e probabilidades potenciais nos negócios podem ser identificados?***
Regras	***Impactos e probabilidades potenciais nos negócios são identificados.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_88	***Que impactos e probabilidades potenciais nos negócios podem ser identificados?***
Regras	***Impactos e probabilidades potenciais nos negócios são identificados.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_88	***Que impactos e probabilidades potenciais nos negócios podem ser identificados?***
Regras	***Ameaças, vulnerabilidades, probabilidades e impactos são utilizados para determinar o risco.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_89	***Que ameaças, vulnerabilidades, probabilidades e impactos devem ser considerados são utilizados para determinar o risco?***
Regras	***Ameaças, vulnerabilidades, probabilidades e impactos são utilizados para determinar o risco.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_89	***Que ameaças, vulnerabilidades, probabilidades e impactos devem ser utilizados para determinar o risco?***
Regras	***Ameaças, vulnerabilidades, probabilidades e impactos são utilizados para determinar o risco.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_89	***Que ameaças, vulnerabilidades, probabilidades e impactos devem ser considerados são utilizados para determinar o risco?***
Regras	***Respostas ao risco são identificadas e priorizadas.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_90	***O que é necessário para identificar e priorizar as respostas ao risco?***
Regras	***Respostas ao risco são identificadas e priorizadas.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_90	***O que é necessário para identificar e priorizar as respostas ao risco?***
Regras	***Respostas ao risco são identificadas e priorizadas.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_90	***O que é necessário para identificar e priorizar as respostas ao risco?***
Regras	***A tolerância a riscos organizacional é determinada e claramente expressa.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_91	***O que é necessário para determinar a tolerância organizacional aos riscos e claramente a expressar?***
Regras	***A tolerância a riscos organizacional é determinada e claramente expressa.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_91	***O que é necessário para determinar a tolerância organizacional aos riscos e claramente a expressar?***
Regras	***A tolerância a riscos organizacional é determinada e claramente expressa.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_91	***O que é necessário para determinar a tolerância organizacional aos riscos e claramente a expressar?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (continua)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Regras	***A determinação da tolerância a riscos da organização é informada pelo seu papel na infraestrutura crítica e na análise de riscos específicos do setor.***	Metas, Objetivos e Perspectivas	PERCEPÇÃO	C1.	N-NIP_92	***O que é necessário para informar a determinação da tolerância a riscos da organização, considerando o seu papel na infraestrutura crítica e na análise de riscos específicos do setor?***
Regras	***A determinação da tolerância a riscos da organização é informada pelo seu papel na infraestrutura crítica e na análise de riscos específicos do setor.***	Metas, Objetivos e Perspectivas	COMPREENSÃO	C1.	N-NIP_92	***O que é necessário para informar a determinação da tolerância a riscos da organização, considerando o seu papel na infraestrutura crítica e na análise de riscos específicos do setor?***
Regras	***A determinação da tolerância a riscos da organização é informada pelo seu papel na infraestrutura crítica e na análise de riscos específicos do setor.***	Metas, Objetivos e Perspectivas	PROJEÇÃO	C1.	N-NIP_92	***O que é necessário para informar a determinação da tolerância a riscos da organização, considerando o seu papel na infraestrutura crítica e na análise de riscos específicos do setor?***
Regras	***Planejamento e testes de resposta e recuperação são conduzidos com fornecedores e provedores terceirizados.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_93	***O que é necessário para planejar e testar as resposta e procedimentos de recuperação com fornecedores e provedores terceirizados?***
Regras	***O plano de resposta é executado durante ou após um incidente.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_94	***O que é necessário para executar o plano de resposta durante ou após um incidente?***
Regras	***O plano de resposta é executado durante ou após um incidente.***	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_94	***O que é necessário para executar o plano de resposta durante ou após um incidente?***
Regras	***O plano de resposta é executado durante ou após um incidente.***	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_94	***O que é necessário para executar o plano de resposta durante ou após um incidente?***
Regras	***O pessoal conhece suas funções e ordem de operações quando uma resposta é necessária.***	Pré-atenção, MLP	PERCEPÇÃO	TODOS	N-NIP_95	***O que é necessário para que o pessoal conheça suas funções e ordem de operações quando uma resposta é necessária?***
Regras	***O pessoal conhece suas funções e ordem de operações quando uma resposta é necessária.***	Pré-atenção, MLP	COMPREENSÃO	TODOS	N-NIP_95	***O que é necessário para que o pessoal conheça suas funções e ordem de operações quando uma resposta é necessária?***
Regras	***O pessoal conhece suas funções e ordem de operações quando uma resposta é necessária.***	Pré-atenção, MLP	PROJEÇÃO	TODOS	N-NIP_95	***O que é necessário para que o pessoal conheça suas funções e ordem de operações quando uma resposta é necessária?***
Regras	***Os incidentes são relatados de acordo com os critérios estabelecidos.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_96	***O que é necessário para relatar os incidentes de acordo com os critérios estabelecidos?***
Regras	***As informações são compartilhadas de acordo com os planos de resposta.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_97	***O que é necessário para compartilhar as informações de acordo com os planos de resposta?***

Quadro 9 - Necessidades Informacionais de Consciência Situacional para DC – proteção cibernética (conclusão)

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	Framework de Teoria Adotada para Defesa Cibernética com base no NIST CSF	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Id NIP_CS_DC	NECESSIDADE INFORMACIONAL PRIMORDIAL DE CS de DC (NIP_CS_DC)
Regras	***A coordenação com as partes interessadas ocorre de acordo com os planos de resposta.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_98	***O que é necessário para coordenar com as partes interessadas de acordo com os planos de resposta?***
Regras	***O compartilhamento voluntário de informações ocorre com partes interessadas externas para alcançar uma compreensão mais ampla da situação de segurança cibernética.***	MLP	COMPREENSÃO	C-C2.	N-NIP_99	***O que é necessário para realizar um compartilhamento voluntário de informações com as partes interessadas externas para alcançar uma compreensão mais ampla da situação de segurança cibernética?***
Regras	***O impacto do incidente é compreendido.***	MLP	COMPREENSÃO	C-C2.	N-NIP_100	***O que é necessário para compreender o impacto de um incidente?***
Regras	***Os incidentes são categorizados de acordo com os planos de resposta.***	MLP	COMPREENSÃO	C-C2.	N-NIP_101	***O que é necessário para categorizar os incidentes de acordo com os planos de resposta?***
Regras	***Os incidentes são contidos.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_102	***O que é necessário para conter um incidentes?***
Regras	***Os incidentes são mitigados.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_103	***O que é necessário para mitigar um incidentes?***
Regras	***As vulnerabilidades recém-identificadas são mitigadas ou documentadas como riscos aceitos.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_104	***O que é necessário para mitigar as vulnerabilidades recém-identificadas ou documentá-las como riscos aceitos?***
Regras	***O plano de recuperação é executado durante ou após um incidente de cibersegurança.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_105	***O que é necessário para a execução de um plano de recuperação durante ou após um incidente de cibersegurança?***
Regras	***Relações públicas são gerenciadas.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_106	***O que é necesário para gerenciar as relações públicas?***
Regras	***A reputação é restaurada após um incidente.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_107	***O que é necessário para restaurar a reputação após um incidente.***
Regras	***As atividades de recuperação são comunicadas às partes interessadas internas e externas, bem como às equipes executivas e de gerenciamento.***	MLP	PROJEÇÃO	Pr-C2.	N-NIP_108	***O que é necessário para comunicar as atividades de recuperação às partes interessadas internas e externas, bem como às equipes executivas e de gerenciamento?***

Fonte: Autor

Quadro 10 - Necessidades Informacionais de Consciência Situacional para DC – exploração e ataque cibernéticos

TEORIA ADOTADA PARA DEFESA CIBERNÉTICA	INSUMO	ESTÁGIO DE CS	Critério Aplicado	Nr NIP	NECESSIDADE INFORMACIONAL PRIMORDIAL DE DC	Tática MITRE (Enterprise)	Nr-TP MITRE
Interpretações	Pré-Atenção	PERCEPÇÃO	Pe-C3.	M-NIP1	***Quais informações do alvo se deve tentar coletar que possam ser usadas para planejar operações futuras?***	**Reconhecimento**	**1**
Interpretações	Pré-Atenção	PERCEPÇÃO	Pe-C2.	M-NIP2	***Que recursos se deve obter e estabelecer que possam ser usados para apoiar operações para alcançar o alvo?***	**Desenvolvimento de Recursos**	**2**
Interpretações	Pré-Atenção	PERCEPÇÃO	Pe-C2.	M-NIP3	***Quais as formas para se tentar entrar na sua rede do alvo?***	**Acesso Inicial**	**3**
Interpretações	Pré-Atenção	PERCEPÇÃO	Pe-C2.	M-NIP4	***Quais e de que forma devem ser obtidas nomes de conta e senhas do alvo?***	**Acesso a Credenciais**	**8**
Interpretações	Pré-Atenção	PERCEPÇÃO	Pe-C2.	M-NIP5	***Quais dados de interesse para seu objetivo específico na rede do alvo devem ser reunidos?***	**Coleta**	**11**
Conhecimento Explícito	MPL	COMPREENSÃO	C-C2.	M-NIP6	***De que forma e quais códigos maliciosos se deve tentar executar em locais específicos da rede do alvo?***	**Execução**	**4**
Conhecimento Explícito	MPL	COMPREENSÃO	C-C2.	M-NIP7	***O que é necesário para se tentar manter a posição na rede do alvo?***	**Persistência**	**5**
Conhecimento Explícito	MPL	COMPREENSÃO	C-C2.	M-NIP8	***O que é necessário para se obter permissões de nível mais alto na rede do alvo?***	**Escalação de Privilégios**	**6**
Conhecimento Explícito	MPL	COMPREENSÃO	C-C2.	M-NIP9	***O que é necessário para evitar ser detectado?***	**Evasão de Defesa**	**7**
Conhecimento Explícito	MPL	COMPREENSÃO	C-C2.	M-NIP10	***O que é necessário para se entender o ambiente atacado?***	**Descoberta**	**9**
Conhecimento Explícito	MPL	COMPREENSÃO	C-C2.	M-NIP11	***O que é necessário para realizar o deslocamento através do ambiente da rede do alvo?***	**Movimentação Lateral**	**10**
Regras	MPL	PROJEÇÃO	Pr-C2.	M-NIP12	***O que é necessário para se comunicar com os sistemas comprometidos na rede do alvo para controlá-los?***	**Comando e Controle**	**12**
Regras	MPL	PROJEÇÃO	Pr-C2.	M-NIP13	***O que é necessário para se apoderar de dados do alvo?***	**Exfiltração**	**13**
Regras	MPL	PROJEÇÃO	Pr-C2.	M-NIP14	***O que é necessário para tentar manipular, interromper ou destruir os sistemas e dados do alvo?***	**Impacto**	**14**

Fonte: Autor

5.4. OBJETIVO ESPECÍFICO (d)

Neste subtítulo são apresentados os resultados da execução do objetivo específico (d), qual seja, “d) Aplicar o *framework* consolidado nas documentações regulatórias e doutrinárias do Setor Cibernético da Defesa brasileira, assim como nos planejamentos das operações de defesa cibernética e respectivas LA e APA ocorridas no período de 2012 a 2016, para identificar as necessidades informacionais de cada evento ocorrido no período”. Para tal, procedeu-se o registro dos resultados das tarefas (d.1) e (d.2), conforme consta no Quadro 4, no capítulo de Metodologia.

5.4.1. Tarefa (d.1)

A tarefa (d.1) teve por finalidade coletar as documentações de planejamento, nos níveis militares estratégico e operacional, assim como os registros de APA, das operações de defesa e segurança cibernética do período de 2012 a 2016.

Para satisfazer essa tarefa, foram reunidos, além da documentação estratégica, os documentos e registros de LA e APA das seguintes operações:

- Operação Amazônia 2012;
- Operação para Segurança da Conferência das Nações Unidas para o Desenvolvimento Sustentável / 2012 (Rio+20);
- Operação Atlantico III / 2012;
- Operação para Segurança da Copa das Confederações 2013;
- Operação para Segurança da Jornada Mundial da Juventude;
- Operação Laçador 2013;
- Operação Combinada PANAMAX 2013;
- Operação para Segurança da Copa do Mundo 2014;
- Operação Amazônia 2014;
- Operação para Segurança dos Jogos Olímpicos e Paralímpicos 2016.

A documentação de caráter estratégico reunida foi a seguinte:

- Estratégia Nacional de Defesa (END) (Brasil, 2008)
- Política de Defesa Cibernética (Brasil, 2012b);
- Doutrina Militar de Defesa Cibernética (Brasil, 2014).

Das documentações pesquisadas sobre operações, decidiu-se selecionar para análise as operações dos grandes eventos Rio+20, Copa das Confederações 2013 e Jogos Olímpicos e Paralímpicos 2016, assim como as operações de adestramento militar Atlântico III 2012 e Laçador 2013. A razão dessas escolhas foi a possibilidade de observar a evolução da capacidade de consciência situacional, conforme *framework* proposto nesta pesquisa, tomando-se como referência uma operação de complexidade simples, outra de grau intermediário e, por fim, a de maior complexidade do período para os Grandes Eventos. Para as operações do MD, apenas duas foram selecionadas em razão de suas documentações estarem completas.

Entenda-se por “simples” e “complexas” como conceitos associados à maturidade do CDCiber em termos de capacidades de realizar ações de defesa cibernética no período estudado. Essa escolha deu-se pelo fato observado que, em termos de demanda de ações cibernéticas, todas as operações estudadas foram muito similares. Por outro lado, as capacidades do CDCiber foram se modificando e evoluindo a cada ocasião de emprego.

A escolha das documentações estratégicas recaiu sobre a Política de Defesa Cibernética (Brasil, 2012) e a Doutrina Militar de Defesa Cibernética (Brasil, 2014) em razão de essas duas traçarem explicitamente os direcionamentos da área, o que não ocorre com a Estratégia Nacional de Defesa (END) (Brasil, 2008).

Para cada operação foram selecionadas as documentações de planejamento de nível tático – operacional, denominadas Ordens de Operação (OOp), além dos registros de avaliação pós-ação (APA) e lições aprendidas (LA). Não foram considerados os planejamentos estratégicos e operacionais, níveis de planejamento superiores às Ordens de Operações, pois, na sua avaliação, constatou-se que as menções à cibernética eram majoritariamente genéricas ou muito semelhantes ao registrado nas próprias OOp de cibernética. Isso se deu pelo fato de que a cibernética era um novo eixo de combate inserido nas operações, ainda de caráter abstrato para os níveis superiores de gestão, o que provocou poucas inserções de nível documental desses níveis, sendo que, as que ocorreram, estavam diretamente refletidas nas OOp.

Em síntese, as documentações especificamente analisadas foram:

(i) Política de Defesa Cibernética (Brasil, 2012b);
(ii) Doutrina Militar de Defesa Cibernética (Brasil, 2014);
(iii) OOp da Operação para Segurança da Conferência das Nações Unidas para o Desenvolvimento Sustentável / 2012 (Rio+20);
(iv) OOp da Operação Atlantico III / 2012;
(v) OOp da Operação para Segurança da Copa das Confederações 2013;
(vi) OOp da Operação Laçador 2013;
(vii) OOp da Operação para Segurança dos Jogos Olímpicos e Paralímpicos 2016;
(viii) APA das operações listadas de (iii) a (vii);
(ix) LA das operações listadas de (iii) a (vii).

Como observação final relativa aos resultados da tarefa (d.1), ressalta-se que, além das informações escritas, o autor desta pesquisa, como participante de todos os eventos realizados, sendo três das vezes como comandante de Destacamento (operações Atlântico III, Copa das Confederações 2013 e Jogos Olímpicos 2016), complementou os dados que não estavam disponíveis na ocasião da pesquisa ou estavam incompletos, ou ainda que não foram registrados, mas foram vivenciados pelo pesquisador.

5.4.2. Tarefa (d.2)

A tarefa (d.2) teve por finalidade analisar a documentação de cada operação de defesa cibernética do período estudado, assinalando as NIP-CS-DC aplicáveis, assim como as não aplicáveis, de forma justificada.

5.4.2.1. Documentação Doutrinária

Do exame dos documentos listados nos itens (i) e (ii), do subtítulo 5.4.1, quais sejam, Política de Defesa Cibernética (Brasil, 2012b), Doutrina Militar de Defesa Cibernética (Brasil, 2014), extraiu-se os seguintes elementos de relevância:

Política de Defesa Cibernética: Objetivos.

a. assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional;
b. capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD;

c. colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
d. desenvolver e manter atualizada a doutrina de emprego do St Ciber;
e. implementar medidas que contribuam para a Gestão da SIC no âmbito do MD;
f. adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber;
g. definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber;
h. cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e
i. contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD.

A razão da escolha do registro apenas dos objetivos foi pela constatação de que o documento está focado totalmente nesse tema, além do fato de que, para fins do estudo desta pesquisa, um dos elementos que compõem o modelo de Endsley (1995) e que é referência para as avaliações e análises feitas no estudo, são as metas, objetivos e perspectivas, conforme Figura 29.

Doutrina Militar de Defesa Cibernética: conceitos e aplicação.

A Doutrina Militar de Defesa Cibernética é um documento tanto conceitual, no que diz respeito a definir a defesa cibernética e caracterizar os elementos subjacentes, quanto de aplicação para operações militares em um primeiro nível de complexidade. Assim, seu conteúdo deve ser absorvido como um todo para orientação da definição das NIP de defesa cibernética e para justificar seu uso ou não em cada operação analisada.

5.4.2.2. Documentação de APA e LA

Do exame da documentação relativa às análises pós-ação (APA) e lições aprendidas (LA), respectivamente, os itens (viii) e (ix) do subtítulo 5.4.1, constatou-se uma variedade de níveis gerenciais para os fatos relatados nas APA e as lições aprendidas, desde o nível de execução até o nível estratégico. Os relatos de APA e

LA abrangeram como temas principais: Operações (atuação como CSIRT), Inteligência, Logística e Comando e Controle (gestão de TI interna ao Dst para fins de operação).

Os registros de APA e LA para o tema logística foram eliminados da análise, pois tratavam de assuntos totalmente não relacionados à cibernética. Dos demais temas, foram filtrados os registros de APA e LA de caráter estratégico, de modo a estar consonante com a aplicação do *framework* buscado na pesquisa. Como resultado final, de um total de 477 lições aprendidas e 490 registros de APA, restaram 39% de item selecionados. Essas lições aprendidas e registros de APA restantes foram usados no estudo. Uma das principais utilidades das LA e registros de APA analisados, uma vez que eram naturalmente separadas por operação de defesa cibernética, foi subsidiar a averiguação se uma NIP era aplicável, foi ou não utilizada na operação estudada e em qual estágio da CS eram melhor empregada.

5.4.2.3. Ordens de Operações

As OOp das operações listadas nos itens (iii) a (vii) do subtítulo 5.4.1 foram analisadas à luz das documentações doutrinárias e das LA e registros de APA respectivas, de modo a revelar o uso das NIP propostas no *framework* de NIP-CS-DC.

Como primeira constatação importante, foi observado que as operações de grandes eventos analisadas, Rio+20, Copa das Confederações 2013 e Jogos Olímpicos 2016, foram operações eminentemente de proteção cibernética, conforme definido na Doutrina Militar de Defesa Cibernética (Brasil, p. 23), ou, simplesmente, de segurança cibernética, o que excluiu a aplicação das NIP com base nas táticas de exploração e ataque, por serem, por excelência, de caráter ofensivo.

Verificando-se NIP a NIP, por operação selecionada, foram encontrados os resultados de maior destaque, conforme os subtítulos 5.4.2.3.1 a 5.4.2.3.3.

Outro destaque aplicável a todas as operações de proteção cibernética é que, pelo fato de haver uma relação biunívoca entre NIP e controles do *framework* original, a quantidade de NIP com base no NIST naturalmente coincidia em número com os 108 controles do NIST CSF. No entanto, nas tabelas, indica-se um total de 168 NIP. A explicação para a diferença é que, da análise feita NIP a NIP, constatou-

se que em 30 delas, os *schematas* que se podiam visualizar da sua aplicação abrangiam os três estágios da consciência situacional. Assim, cada uma dessas 30 NIP, é aplicável tanto para percepção, compreensão e projeção, gerando, cada uma, duas a mais, distinguindo-se umas das outras por serem identificadas não só pela numeração que a identifica, mas pelo estágio de CS associado.

O desenvolvimento da análise revelou que a simples constatação de que se uma NIP fora ou não utilizada não seria suficiente para avaliação do *framework* produzido pela pesquisa, pois, pelo estudo da documentação, em particular das LA, foi possível observar que uma mesma NIP poderia ter sido aplicada em operações diferentes, porém em graus de maturidade muito dispares. Assim, foi introduzido um parâmetro de maturidade para a análise que foi graduado em cinco níveis e valores: baixo (B), valor 1; médio-baixo (M-B), valor 2; médio (M), valor 3; médio-alto (M-A), valor 4; alto (A), valor 5.

Cabe ressaltar que o termo “maturidade” pode assumir acepções diversas, sejam de ordem técnica e comercial, para produtos tecnológicos, ou acadêmicas, conforme a referência que se tome, o que pode levar a alguma dubiedade na interpretação das informações tabuladas. Assim, faz-se necessário especificar que, para fins das constatações desta pesquisa, o termo “maturidade” foi utilizado para expressar o nível da capacidade de gerir o processo da aplicação da NIP considerada.

Os níveis de maturidade adotados na pesquisa tiveram por referência principal o estabelecido no NIST CSF (NIST, 2018, p.8) para localizar organizações quanto a sofisticação da aplicação do processo de gestão de risco como um todo, o que é feito pela definição de níveis (*tiers*) em analogia a níveis de maturidade de aplicação do processo de gestão de riscos. Muito embora, como esclarecido no próprio *framework* NIST CSF (NIST, 2018, p.8), esses níveis não tenham sido concebidos aferir maturidade nas organizações, proveem uma analogia adequada para, a partir dele, construir-se na presente pesquisa uma escala compatível com a necessidade surgida nas medições. Nas definições do NIST CSF a respeito dos mencionados níveis, há quatro deles (NIST, 2018, p.9-11), no entanto, para fins desta tese, e frente ao observado no material estudado e do testemunho do pesquisador, optou-se por incluir um degrau a mais entre o nível mediano e o nível máximo.

Assim, os níveis de maturidade adotados corresponderam, respectivamente, às seguintes acepções de capacidade de gerir o processo da aplicação da NIP: (B) - aplicado apenas para uma ocasião específica (*ad hoc*); (M-B) - aplicado consuetudinariamente, (M) - aplicado conforme registro formal, mas sem pormenorizações das ações; (M-A) - aplicado conforme registro formal, com pormenorizações das ações, mas sem melhorias formais; (A) - aplicado conforme registro formal, com pormenorizações das ações, tendo passado por melhorias formais.

5.4.2.3.1. Operação Rio+20

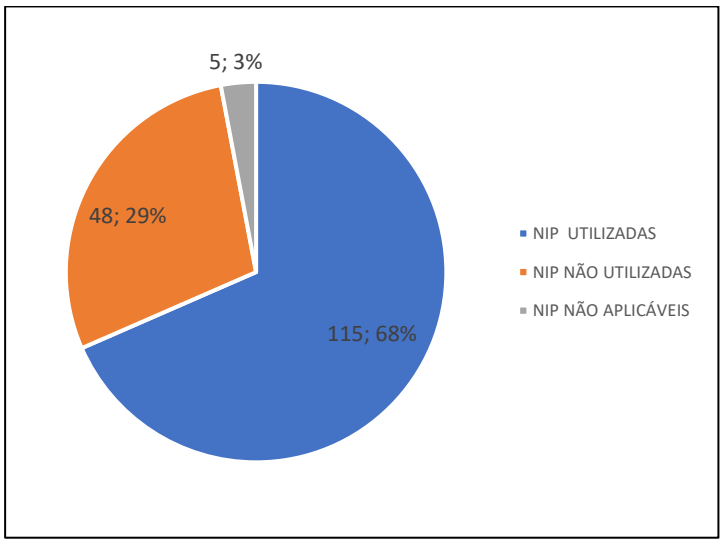
A análise da operação Rio+20 revelou os valores tabulados nas Tabelas de 1 a 10 e representados pelas respectivas Figuras de 39 a 48.

Tabela 1 - Totais de NIP da Rio+20 analisadas

NIP utilizadas	NIP não utilizadas	NIP não aplicáveis	Total
115	48	5	168

Fonte: Autor

Figura 39 - Totais de NIP da Rio+20 analisadas



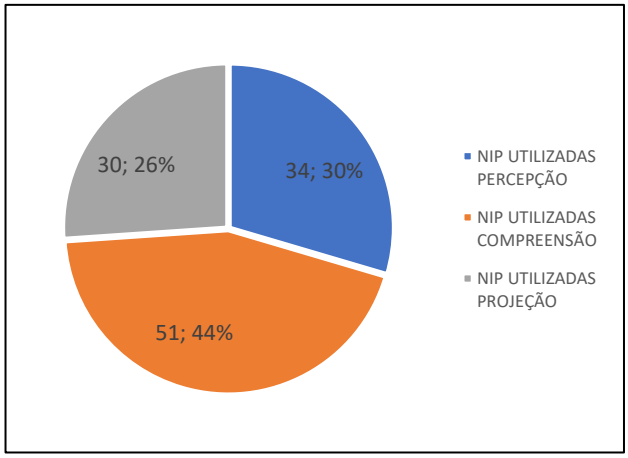
Fonte: Autor

Tabela 2 - NIP utilizadas por estágio de CS na operação Rio+20

NIP UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
34	51	30	115

Fonte: Autor

Figura 40 - Distribuição de NIP utilizadas por estágio de CS na operação Rio+20



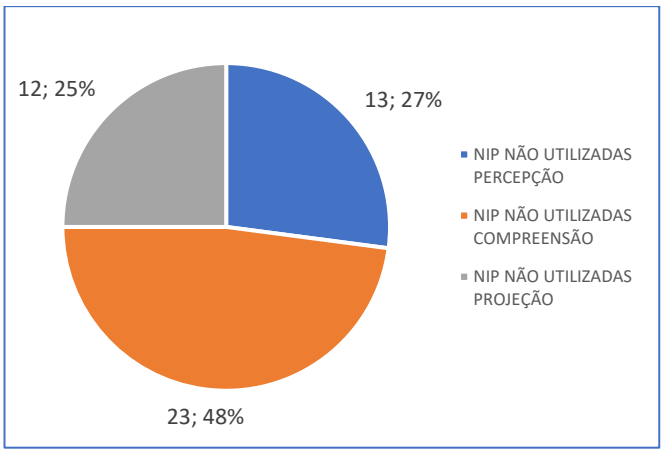
Fonte: Autor

Tabela 3 – NIP não utilizadas por estágio de CS na operação Rio+20

NIP NÃO UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
13	23	12	48

Fonte: Autor

Figura 41 - Distribuição de NIP não utilizadas por estágio de CS na operação Rio+20



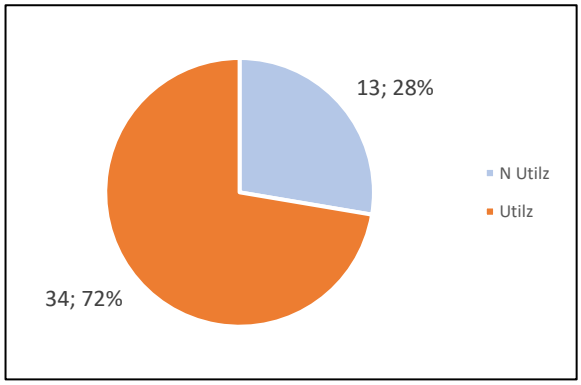
Fonte: Autor

Tabela 4 – NIP utilizadas e não utilizadas de Percepção na operação Rio+20

NIP UTILIZADAS E NÃO UTILIZADAS DE PERCEPÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
13	34	47	27,7	72,3

Fonte: Autor

Figura 42 – NIP utilizadas e não utilizadas de Percepção na operação Rio+20



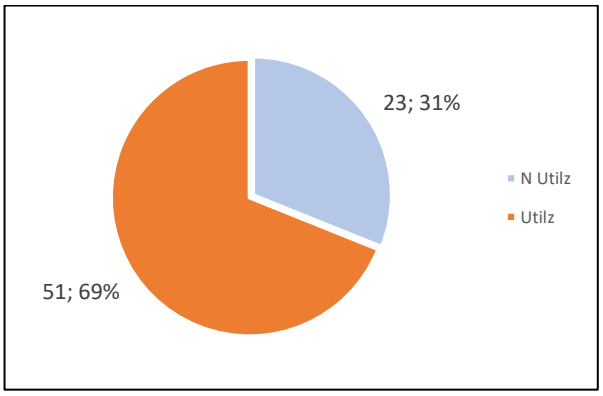
Fonte: Autor

Tabela 5 – NIP utilizadas e não utilizadas de Compreensão na operação Rio+20

NIP UTILIZADAS E NÃO UTILIZADAS DE COMPREENSÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
23	51	74	31,1	68,9

Fonte: Autor

Figura 43 – NIP utilizadas e não utilizadas de Compreensão na operação Rio+20



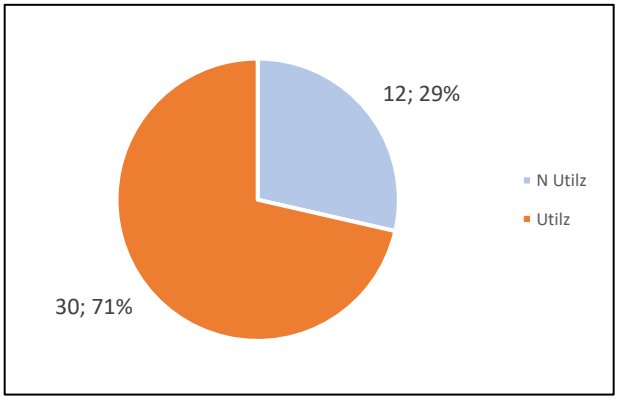
Fonte: Autor

Tabela 6 – NIP utilizadas e não utilizadas de Projeção na Rio+20

NIP UTILIZADAS E NÃO UTILIZADAS DE PROJEÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
12	30	42	28,6	71,4

Fonte: Autor

Figura 44 – NIP utilizadas e não utilizadas de Projeção na operação Rio+20



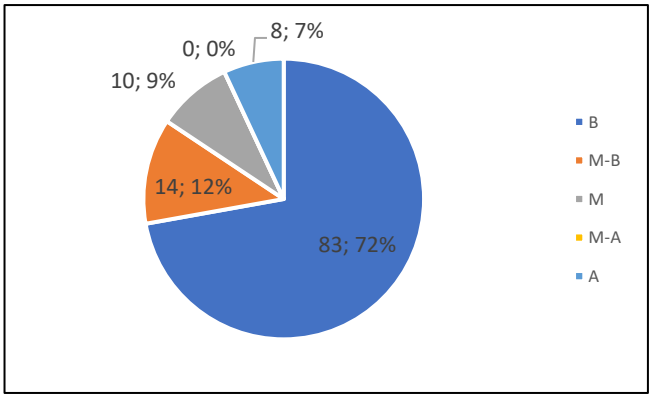
Fonte: Autor

Tabela 7 – Maturidade Geral das NIP na operação Rio+20

MATURIDADE						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**Total**
83	14	10	0	8	53	168

Fonte: Autor

Figura 45 - Maturidade Geral das NIP na operação Rio+20



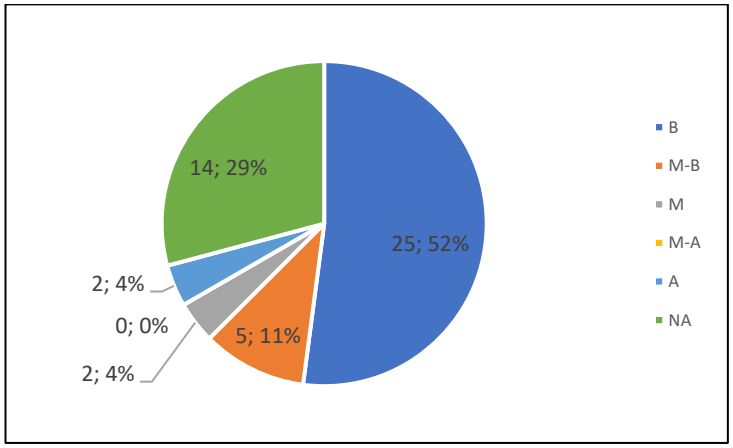
Fonte: Autor

Tabela 8 – Maturidade de Percepção das NIP na operação Rio+20

MATURIDADE DE PERCEPÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
25	5	2	0	2	14	48

Fonte: Autor

Figura 46 – Maturidade de Percepção das NIP na operação Rio+20



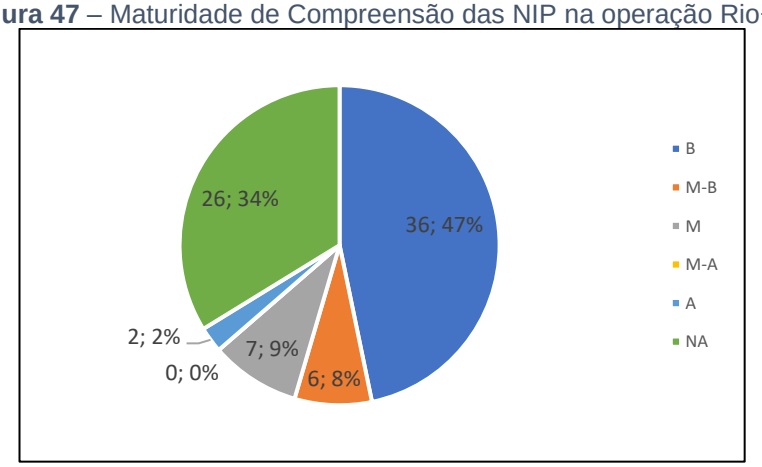
Fonte: Autor

Tabela 9 – Maturidade de Compreensão das NIP na Rio+20

MATURIDADE DE COMPREENSÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
36	6	7	0	2	26	77

Fonte: Autor

Figura 47 – Maturidade de Compreensão das NIP na operação Rio+20



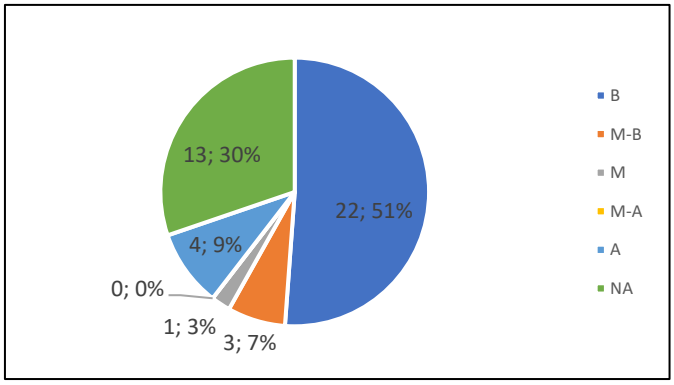
Fonte: Autor

Tabela 10 – Maturidade de Projeção das NIP na Rio+20

MATURIDADE DE PROJEÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
22	3	1	0	4	13	43

Fonte: Autor

Figura 48 – Maturidade de Projeção das NIP na operação Rio+20



Fonte: Autor

5.4.2.3.2. Operação Copa das Confederações 2013

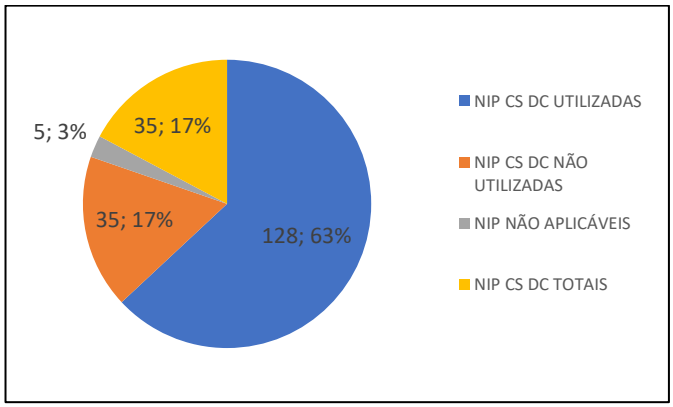
A análise da operação Copa das Confederações 2013 revelou os valores tabulados nas tabelas de 11 a 20 e representados pelas respectivas Figuras de 49 a 58.

Tabela 11 – Totais de NIP da Copa das Confederações analisadas

NIP CS DC UTILIZADAS	NIP CS DC NÃO UTILIZADAS	NIP NÃO APLICÁVEIS	NIP CS DC TOTAIS
128	35	5	35

Fonte: Autor

Figura 49 – Totais de NIP da Copa das Confederações analisadas



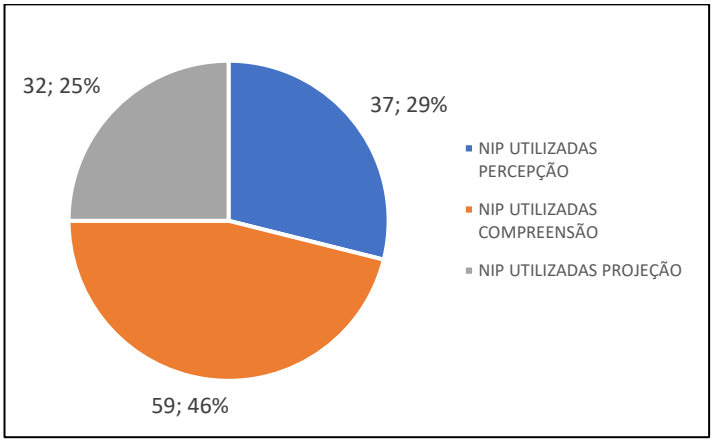
Fonte: Autor

Tabela 12 – NIP utilizadas por estágio de CS na Copa das Confederações 2013

NIP UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
37	59	32	128

Fonte: Autor

Figura 50 – Distribuição de NIP utilizadas por estágio de CS na Copa das Confederações 2013



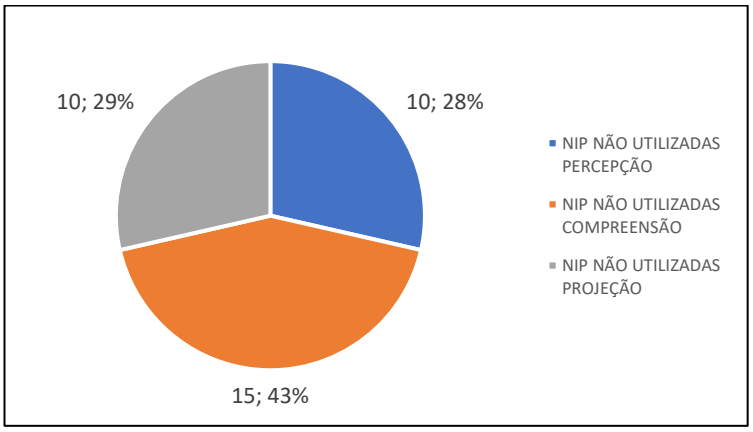
Fonte: Autor

Tabela 13 – NIP não utilizadas por estágio de CS na Copa das Confederações 2013

NIP NÃO UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
10	15	10	35

Fonte: Autor

Figura 51 – Distribuição de NIP não utilizadas por estágio de CS na Copa das Confederações 2013



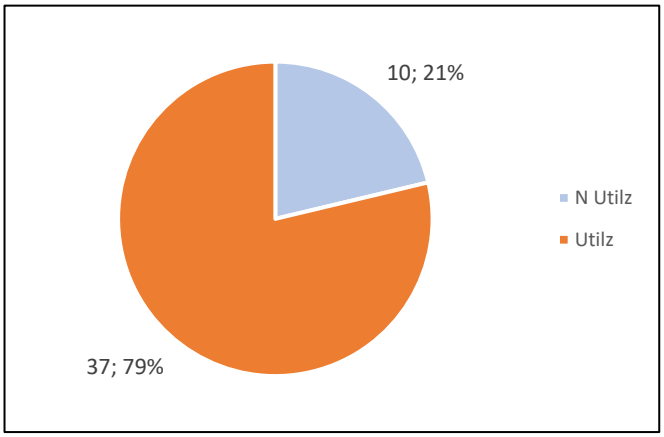
Fonte: Autor

Tabela 14 - NIP utilizadas e não utilizadas de Percepção na Copa das Confederações 2013

NIP UTILIZADAS E NÃO UTILIZADAS DE PERCEPÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
10	37	47	21,3	78,7

Fonte: Autor

Figura 52 - NIP utilizadas e não utilizadas de Percepção na Copa das Confederações 2013



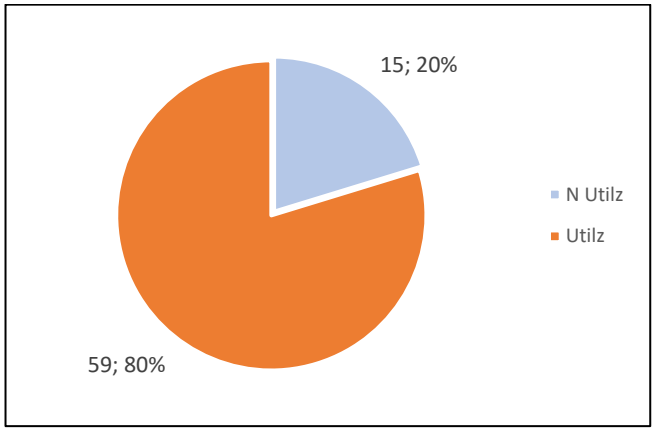
Fonte: Autor

Tabela 15 - NIP utilizadas e não utilizadas de Compreensão na Copa das Confederações 2013

COMPREENSÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
15	59	74	20,3	79,7

Fonte: Autor

Figura 53 – NIP utilizadas e não utilizadas de Compreensão na Copa das Confederações 2013



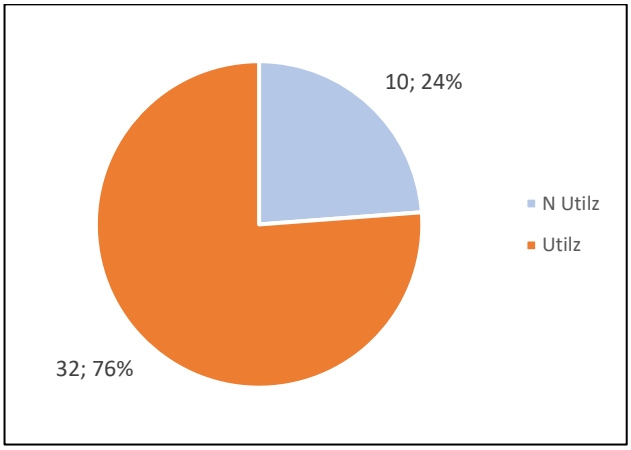
Fonte: Autor

Tabela 16 - NIP utilizadas e não utilizadas de Projeção na Copa das Confederações 2013

PROJEÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
10	32	42	23,8	76,2

Fonte: Autor

Figura 54 – NIP utilizadas e não utilizadas de Projeção na Copa das Confederações 2013



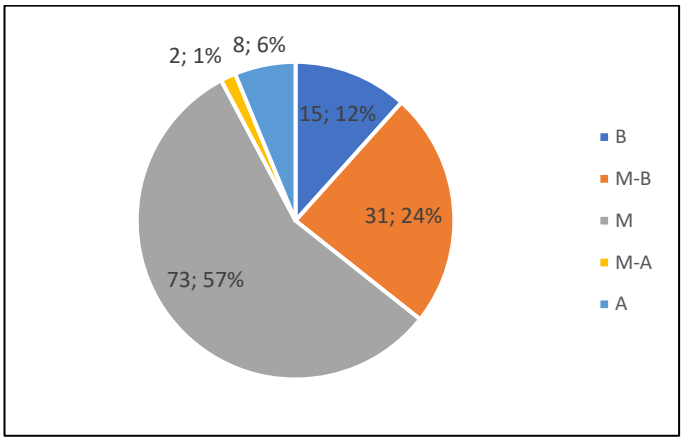
Fonte: Autor

Tabela 17 – Maturidade Geral das NIP na Copa das Confederações 2013

MATURIDADE						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**Total**
15	31	73	2	8	39	168

Fonte: Autor

Figura 55 – Maturidade Geral das NIP na Copa das Confederações 2013



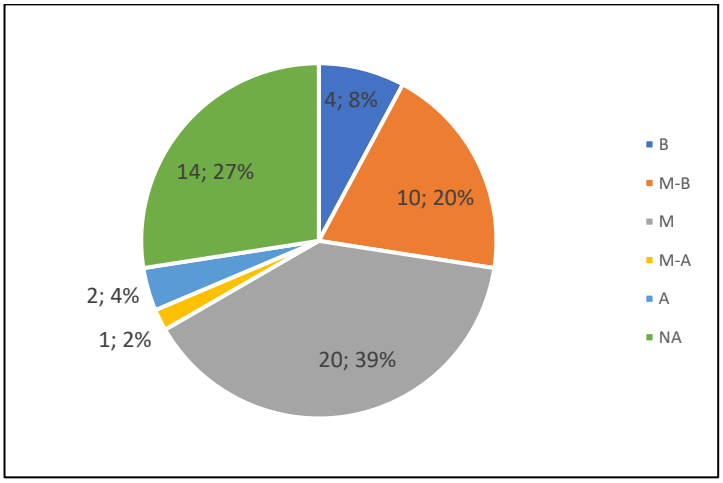
Fonte: Autor

Tabela 18 – Maturidade de Percepção das NIP na Copa das Confederações 2013

MATURIDADE DE PERCEPÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
4	10	20	1	2	14	51

Fonte: Autor

Figura 56 – Maturidade de Percepção das NIP na Copa das Confederações 2013



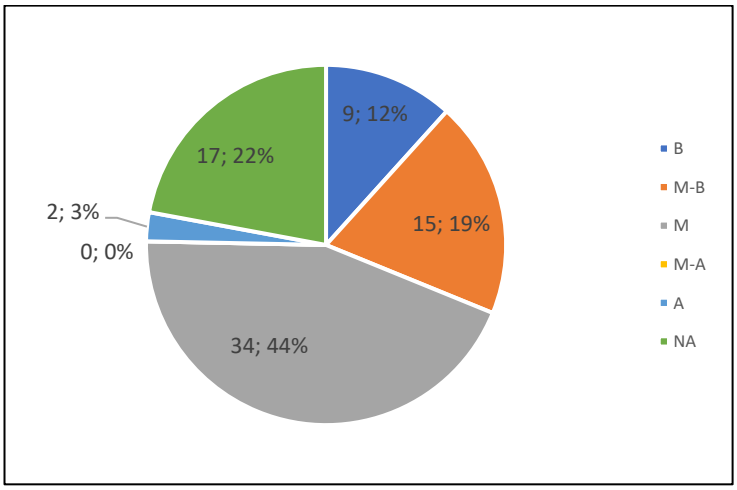
Fonte: Autor

Tabela 19 – Maturidade de Compreensão das NIP na Copa das Confederações 2013

MATURIDADE DE COMPREENSÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
9	15	34	0	2	17	77

Fonte: Autor

Figura 57 – Maturidade de Compreensão das NIP na Copa das Confederações 2013



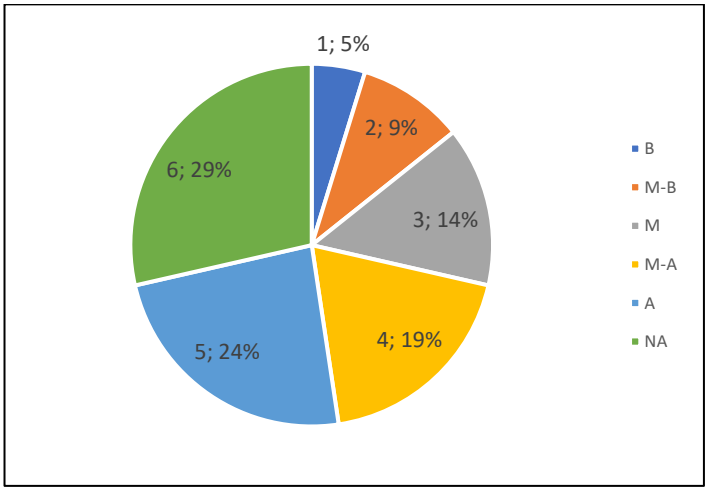
Fonte: Autor

Tabela 20 – Maturidade de Projeção das NIP na Copa das Confederações 2013

MATURIDADE DE PROJEÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
1	2	3	4	5	6	21

Fonte: Autor

Figura 58 – Maturidade de Projeção das NIP na Copa das Confederações 2013



Fonte: Autor

5.4.2.3.3. Operação Jogos Olímpicos e Paralímpicos 2016

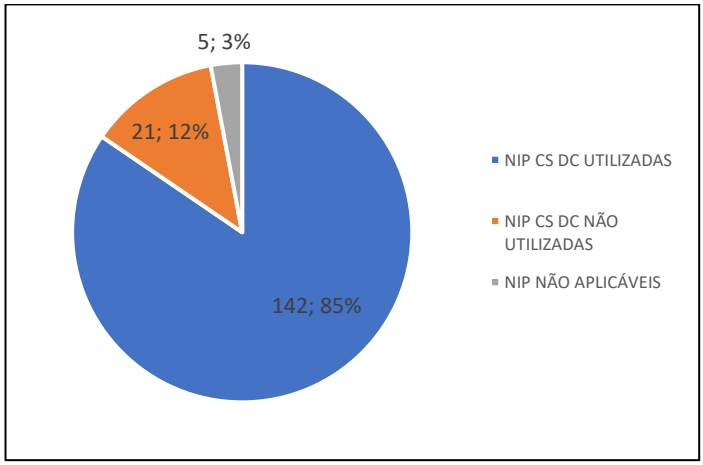
A análise da operação Jogos Olímpicos e Paralímpicos 2016 revelou os valores tabulados nas tabelas de 21 a 30 e representados pelas respectivas Figuras de 59 a 68.

Tabela 21 – Totais de NIP dos Jogos Olímpicos e Paralímpicos 2016

NIP CS DC UTILIZADAS	NIP CS DC NÃO UTILIZADAS	NIP NÃO APLICÁVEIS	NIP CS DC TOTAIS
142	21	5	168

Fonte: Autor

Figura 59 – Totais de NIP dos Jogos Olímpicos e Paralímpicos 2016



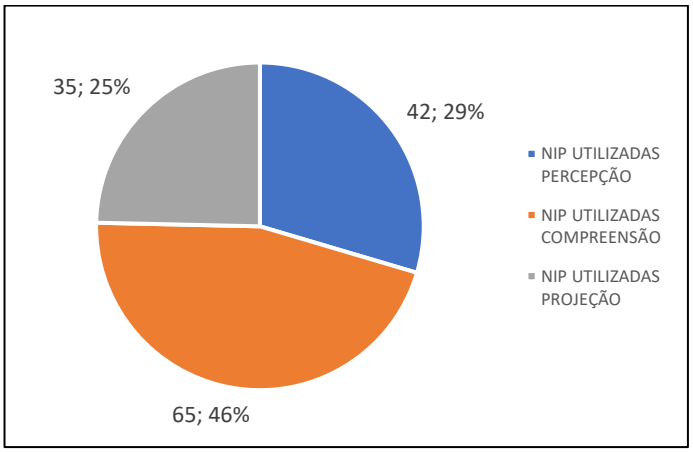
Fonte: Autor

Tabela 22 – NIP utilizadas por estágio de CS nos Jogos Olímpicos e Paralímpicos 2016

NIP UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
42	65	35	142

Fonte: Autor

Figura 60 – NIP utilizadas por estágio de CS nos Jogos Olímpicos e Paralímpicos 2016



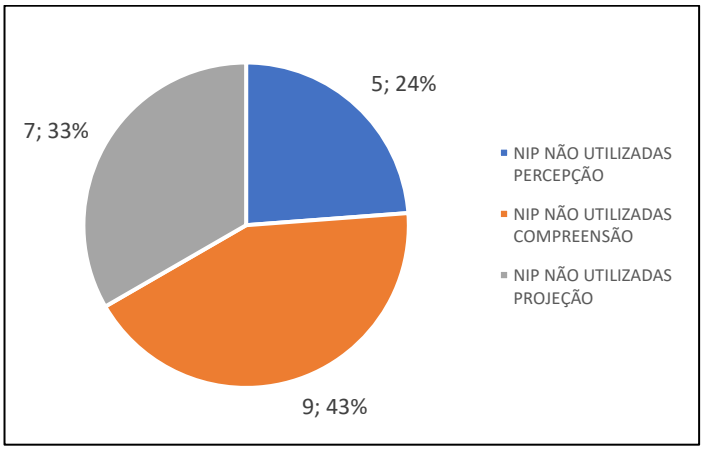
Fonte: Autor

Tabela 23 – NIP não utilizadas por estágio de CS nos Jogos Olímpicos e Paralímpicos 2016

NIP NÃO UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
5	9	7	21

Fonte: Autor

Figura 61 – Distribuição de NIP não utilizadas por estágio de CS nos JO e Paralímpicos 2016



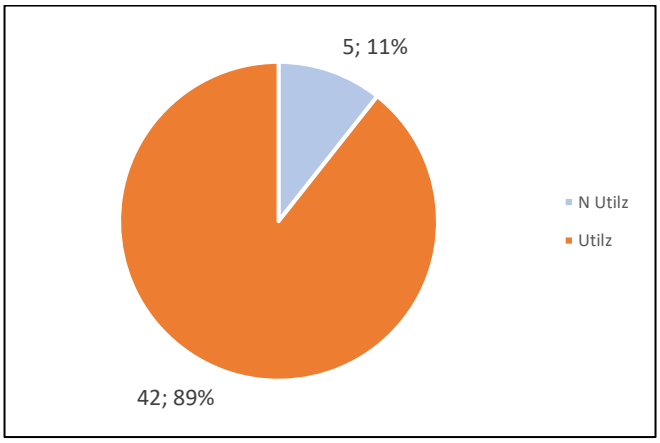
Fonte: Autor

Tabela 24 – NIP utilizadas e não utilizadas de Percepção nos Jogos Olímpicos e Paralímpicos 2016

NIP UTILIZADAS E NÃO UTILIZADAS PERCEPÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
5	42	47	10,6	89,4

Fonte: Autor

Figura 62 – NIP utilizadas e não utilizadas de Percepção nos Jogos Olímpicos e Paralímpicos 2016



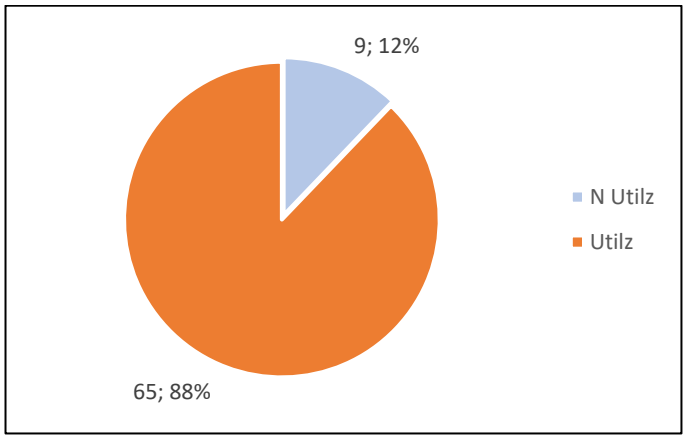
Fonte: Autor

Tabela 25 – NIP utilizadas e não utilizadas de Compreensão nos JO e Paralímpicos 2016

NIP UTILIZADAS E NÃO UTILIZADAS DE COMPREENSÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
9	65	74	12,2	87,8

Fonte: Autor

Figura 63 – NIP utilizadas e não utilizadas de Compreensão nos JO e Paralímpicos 2016



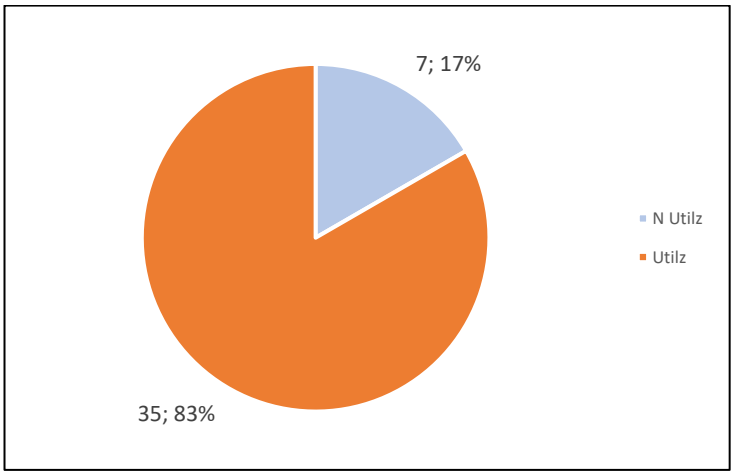
Fonte: Autor

Tabela 26 – NIP utilizadas e não utilizadas de Projeção nos Jogos Olímpicos e Paralímpicos 2016

NIP UTILIZADAS E NÃO UTILIZADAS DE PROJEÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
7	35	42	16,7	83,3

Fonte: Autor

Figura 64 – NIP utilizadas e não utilizadas de Projeção nos Jogos Olímpicos e Paralímpicos 2016



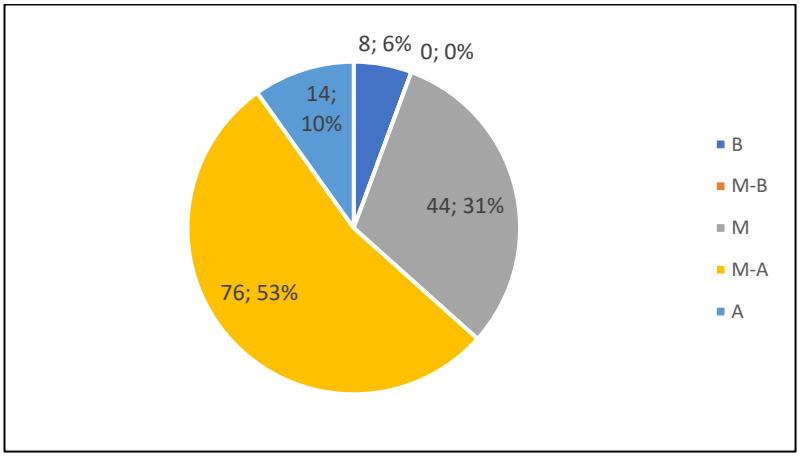
Fonte: Autor

Tabela 27 – Maturidade Geral das NIP nos Jogos Olímpicos e Paralímpicos 2016

MATURIDADE						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**Total**
8	0	44	76	14	26	168

Fonte: Autor

Figura 65 – Maturidade Geral das NIP nos Jogos Olímpicos e Paralímpicos 2016



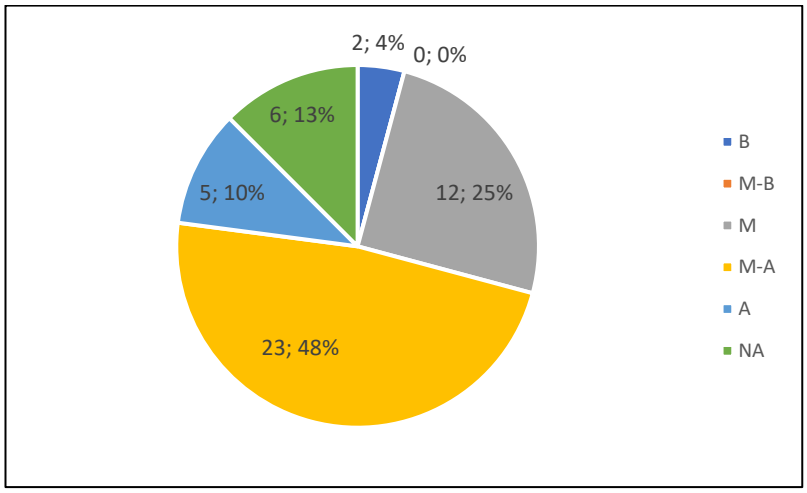
Fonte: Autor

Tabela 28 – Maturidade de Percepção nos Jogos Olímpicos e Paralímpicos 2016

MATURIDADE DE PERCEPÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
2	0	12	23	5	6	48

Fonte: Autor

Figura 66 – Maturidade de Percepção nos Jogos Olímpicos e Paralímpicos 2016



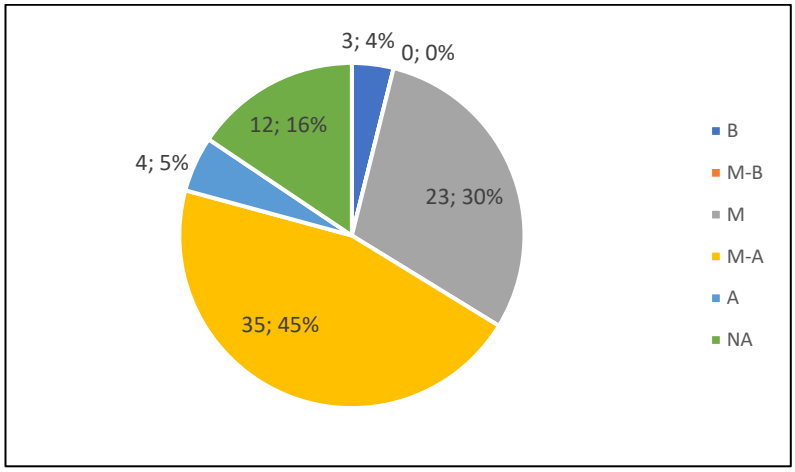
Fonte: Autor

Tabela 29 – Maturidade de Compreensão nos Jogos Olímpicos e Paralímpicos 2016

MATURIDADE DE COMPREENSÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
3	0	23	35	4	12	77

Fonte: Autor

Figura 67 – Maturidade de Compreensão nos Jogos Olímpicos e Paralímpicos 2016



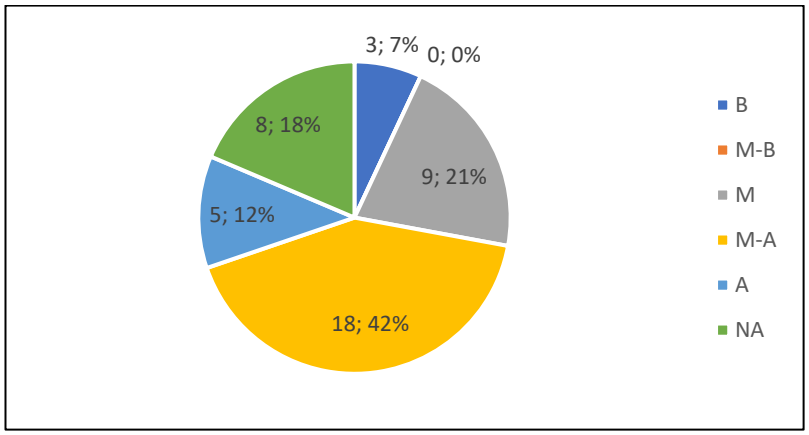
Fonte: Autor

Tabela 30 – Maturidade de Compreensão das NIP nos Jogos Olímpicos e Paralímpicos 2016

MATURIDADE DE PROJEÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
3	0	9	18	5	8	43

Fonte: Autor

Figura 68 – Maturidade de Percepção nos Jogos Olímpicos e Paralímpicos 2016



Fonte: Autor

5.4.2.3.4. Operações de Treinamento do Ministério da Defesa

De modo diferente das operações dos Grandes Eventos, que foram operações reais, as operações de treinamento do Ministério da Defesa, tais como a Atlântico III 2012 e Laçador 2013, são operações fictícias e têm por finalidade o adestramento militar das tropas das três Forças Armadas para atuação conjunta, ou seja, para realizar ações simultâneas e coordenadas frente a uma ameaça ao país. Devido a esse caráter de operação simulada, faz-se necessário uma breve contextualização das características dessas operações antes da apresentação dos seus resultados utilizados na pesquisa.

Esse tipo de exercício é praticado sob coordenação do Ministério da Defesa, tendo diversos objetivos, tais como: testar o treinamento e a efetividade das tropas; verificar as capacidades das estruturas da Defesa Nacional de coordenar os meios necessários para fazer frente à ameaça ao país; testar a capacidade de decisão dos comandantes e o assessoramento de seus estados-maiores.

Operações tais como Atlântico III e Laçador 2013 ocorrem tendo por base um cenário fictício de uma possível contenda bélica, criado a partir de documentação sigilosa a respeito das hipóteses consideradas mais prováveis do envolvimento do

Brasil nesse tipo de conflito. Desse modo, o treinamento, ainda que fictício, ocorre em condições verossímeis e gera nas tropas referências adequadas para que, numa necessidade real, as ações sejam as mais acertadas que seja possível. Os testes aplicados para verificar as capacidades e habilidades para o combate são ministrados por meio de problemas a serem resolvidos, seja teoricamente, seja com ação real no terreno. Esses problemas são chamados problemas militares simulados (PMS).

A cibernética, antes das operações de 2012, era considerada de forma muito pontual e *ad hoc*, porém, de 2012 em diante, todo um conjunto de objetivos, funções e unidades militares específicas de cibernética passaram a ser envolvidas.

Esses tipos de operações foram especificamente escolhidos nesta pesquisa para que houvesse a possibilidade de testar a parte do *framework* proposto voltado para as ações de ataque e exploração cibernética, pois, em contraste com as operações de grandes eventos, as quais são eminentemente de proteção cibernética, as operações militares de adestramento das tropas envolvem os aspectos ofensivos.

5.4.2.3.5. Operações Atlântico III (2012)

Ao se examinar os PMS aplicados ao Destacamento de Guerra Cibernética (conforme foi designada a unidade militar de defesa cibernética para o exercício) empregado na operação Atlântico III, constatou-se que, de um total de oito PMS, todos demandavam soluções majoritariamente de proteção cibernética. Logo, com base nas soluções apresentadas para os PMS de cibernética, não foi possível verificar a descrição de ações de ataque e exploração. No entanto, verificou-se nas demais documentações relativas à operação que, embora não tenham sido registrados nas soluções apresentadas para os PMS aplicados, houve planejamento de ações ofensivas, o que viabilizou a aplicação do *framework* de NIP em seus aspectos de exploração e ataque cibernético.

Ao se examinar os registros de APA e LA da operação, constatou-se que três hipóteses relacionadas às ações cibernéticas de exploração e ataque foram levantadas. Duas dessas hipóteses não foram desenvolvidas, mas apenas mencionadas nas soluções apresentadas dos PMS nr 3 e 27 (a numeração dos PMS

não correspondia apenas aos problemas simulados de cibernética, mas de todas as áreas avaliadas), sendo relacionadas às possibilidades de neutralizar computadores de onde partiam ataques cibernéticos do inimigo fictício e de monitoramento de atividades de atores que promoviam hostilidades no espaço cibernético contra o país a ser defendido.

A terceira hipótese foi desenvolvida e planejada, portanto, passível de ser analisada para esta pesquisa, estando voltada para o desenvolvimento de um ataque, do tipo negação de serviço, contra alguns computadores de relevância do país fictício agressor para suspender seu funcionamento. Essa hipótese não foi apresentada na solução de um problema específico pelo fato de ter sido demandada um ator do cenário fictício diferente daquele que formalmente elaborava os PMS, e, embora a demanda fosse legítima e coerente com a metodologia do exercício, não houve tempo para formalizá-la em um PMS. Assim, com base na análise do planejamento dessa hipótese, foi possível verificar que NIP foram consideradas.

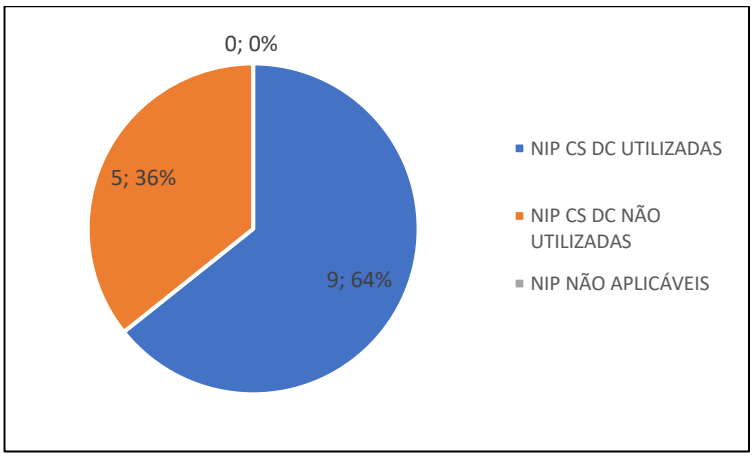
Os achados foram registrados nas Tabelas 31 a 40 e representados nas Figuras 69 a 78.

Tabela 31 – Totais de NIP da Operação Atlântico III - 2012

NIP CS DC UTILIZADAS	NIP CS DC NÃO UTILIZADAS	NIP NÃO APLICÁVEIS	NIP CS DC TOTAIS
9	5	0	14

Fonte: Autor

Figura 69 – Totais de NIP da Operação Atlântico III - 2012



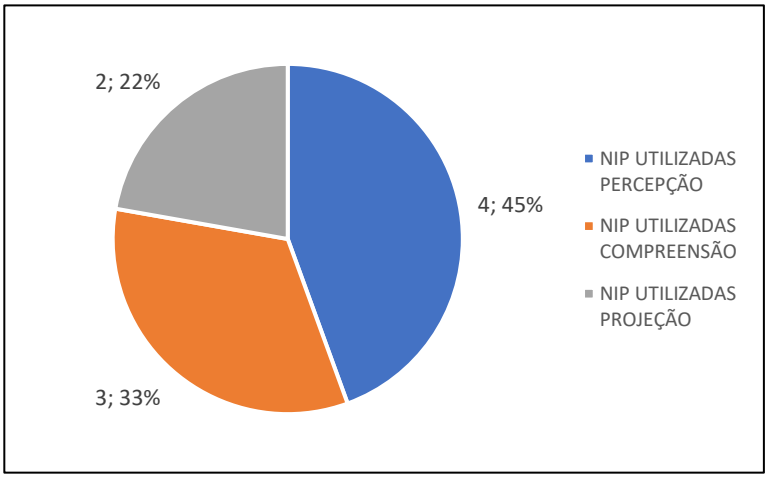
Fonte: Autor

Tabela 32 - NIP utilizadas na Operação Atlântico III - 2012

NIP UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
4	3	2	9

Fonte: Autor

Figura 70 – NIP utilizadas na Operação Atlântico III - 2012



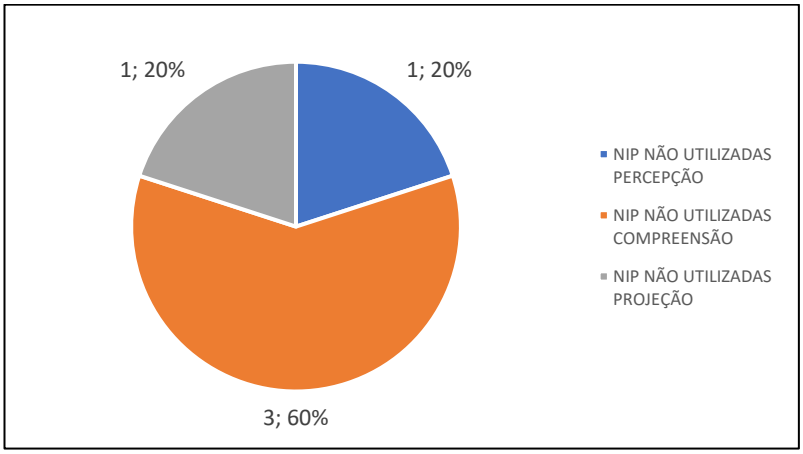
Fonte: Autor

Tabela 33 – NIP não utilizadas na Operação Atlântico III - 2012

NIP NÃO UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
1	3	1	5

Fonte: Autor

Figura 71 – NIP não utilizadas na Operação Atlântico III - 2012



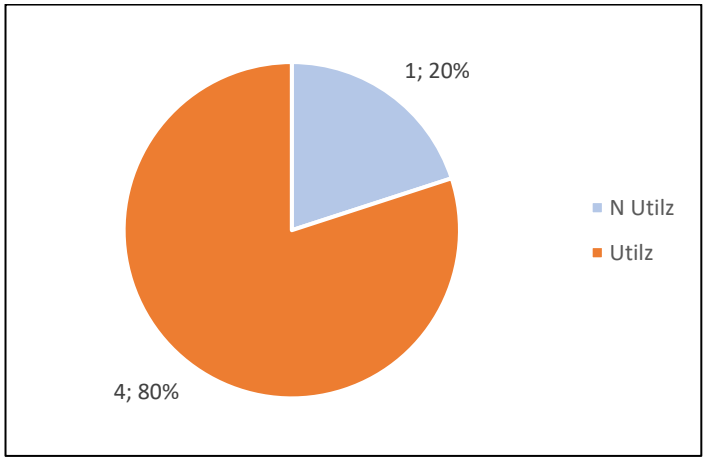
Fonte: Autor

Tabela 34 – NIP utilizadas e não utilizadas de Percepção na Operação Atlântico III - 2012

NIP UTILIZADAS E NÃO UTILIZADAS DE PERCEPÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
1	4	5	20,0	80,0

Fonte: Autor

Figura 72 – NIP utilizadas e não utilizadas de Percepção na Operação Atlântico III - 2012



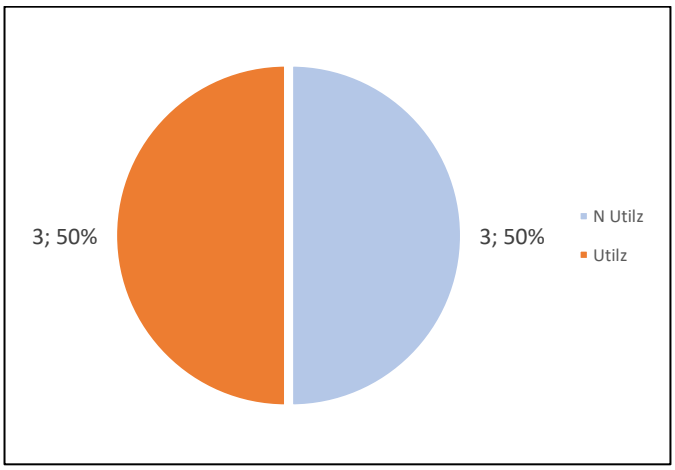
Fonte: Autor

Tabela 35 – NIP utilizadas e não utilizadas de Compreensão na Operação Atlântico III - 2012

NIP UTILIZADAS E NÃO UTILIZADAS DE COMPREENSÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
3	3	6	50,0	50,0

Fonte: Autor

Figura 73 – NIP utilizadas e não utilizadas de Compreensão na Operação Atlântico III - 2012



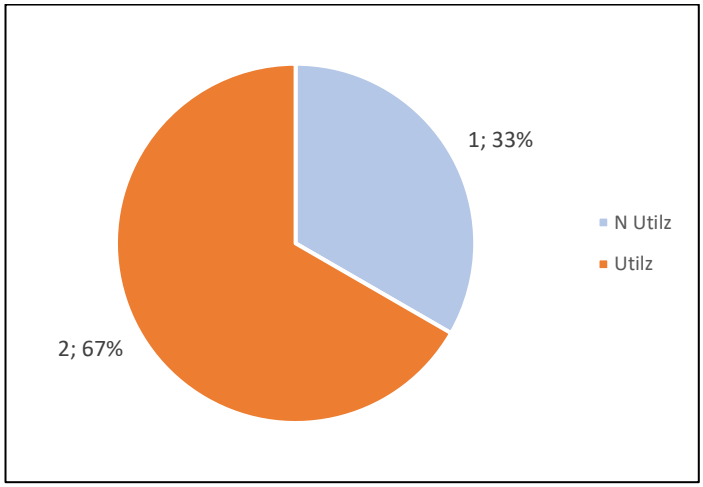
Fonte: Autor

Tabela 36 – NIP utilizadas e não utilizadas de Projeção na Operação Atlântico III - 2012

NIP UTILIZADAS E NÃO UTILIZADAS DE PROJEÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
1	2	3	33,3	66,7

Fonte: Autor

Figura 74 – NIP utilizadas e não utilizadas de Projeção na Operação Atlântico III - 2012



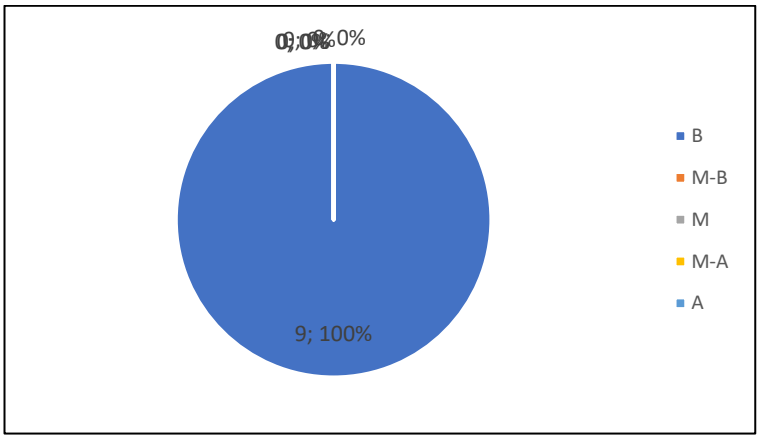
Fonte: Autor

Tabela 37 – Maturidade Geral das NIP na Operação Atlântico III - 2012

MATURIDADE						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**Total**
9	0	0	0	0	5	14

Fonte: Autor

Figura 75 – Maturidade Geral das NIP na Operação Atlântico III - 2012



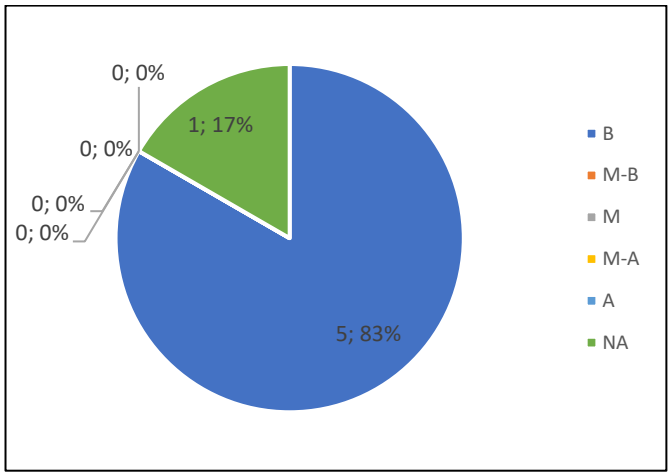
Fonte: Autor

Tabela 38 – Maturidade de Percepção das NIP na Operação Atlântico III - 2012

MATURIDADE DE PERCEPÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
5	0	0	0	0	1	6

Fonte: Autor

Figura 76 – Maturidade de Percepção das NIP na Operação Atlântico III - 2012



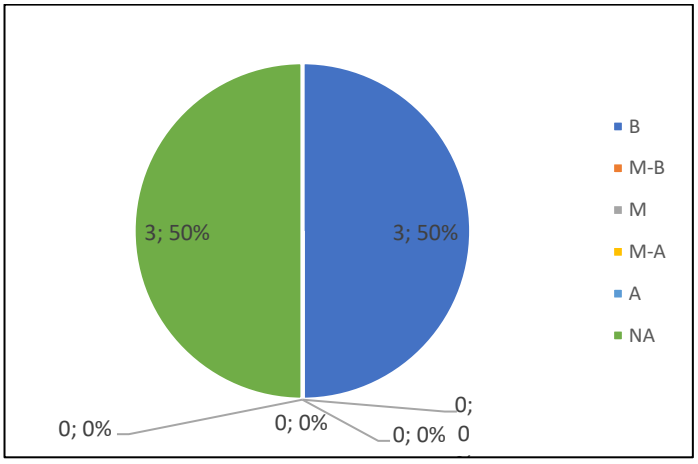
Fonte: Autor

Tabela 39 – Maturidade de Compreensão das NIP na Operação Atlântico III - 2012

MATURIDADE DE COMPREENSÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
3	0	0	0	0	3	6

Fonte: Autor

Figura 77 – Maturidade de Compreensão das NIP na Operação Atlântico III - 2012



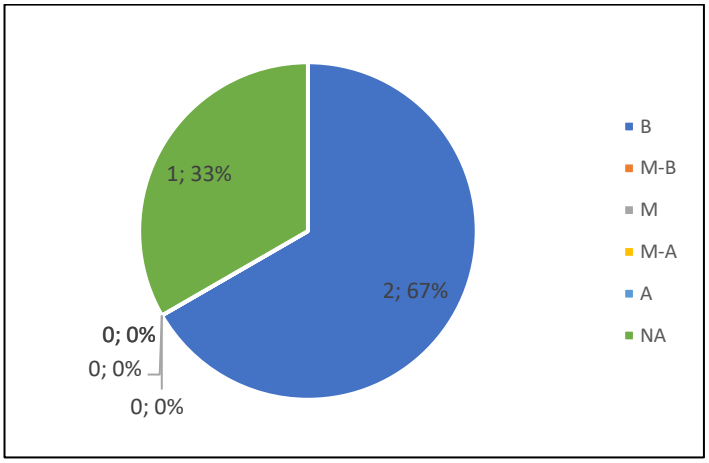
Fonte: Autor

Tabela 40 – Maturidade de Projeção das NIP na Operação Atlântico III - 2012

MATURIDADE DE PROJEÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
2	0	0	0	0	1	3

Fonte: Autor

Figura 78 – Maturidade de Projeção das NIP na Operação Atlântico III - 2012



Fonte: Autor

5.4.2.3.6. Operações Laçador 2013

Da análise da operação Laçador 2013, pôde-se constatar resultados muito próximos aos observados para a operação Atlântico III. A diferença básica entre os aspectos de cibernética das operações foram os cenários estabelecidos para desenvolvimento dos PMS. Enquanto na operação Atlântico III os PMS foram focados de modo que o Dst de Guerra Cibernética atuasse majoritariamente como um CSIRT, na operação Laçador, os PMS abordaram aspectos estratégicos e efeitos cibernéticos e cinéticos em elementos críticos do teatro de operações.

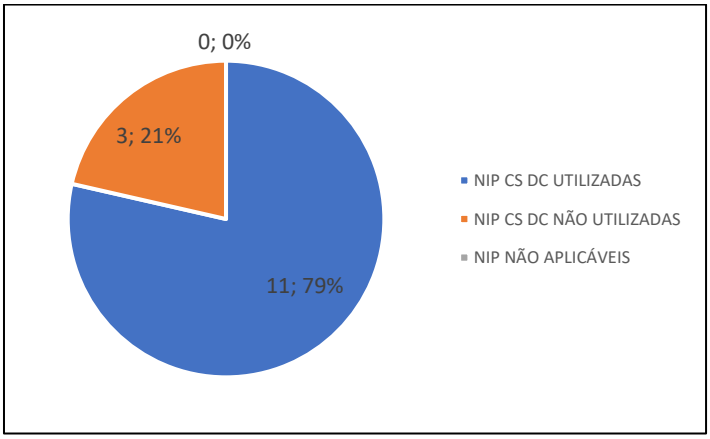
As situações idealizadas para os problemas militares simulados na operação Laçador foram tais que, por meio de dois PMS, nr 7 e 11, foram evocadas necessidades informacionais para o ciclo de preparação e execução de ações cibernéticas de exploração e ataque. Assim, com resultados muito próximos aos observados na operação Atlântico III, porém com discretos incrementos de NIP e em valores de maturidade, chegou-se aos resultados representados nas Tabelas 41 a 50 e nas Figuras 79 a 88.

Tabela 41 – Totais de NIP da Operação Laçador 2013

NIP CS DC UTILIZADAS	NIP CS DC NÃO UTILIZADAS	NIP NÃO APLICÁVEIS	NIP CS DC TOTAIS
11	3	0	14

Fonte: Autor

Figura 79 – Totais de NIP da Operação Laçador 2013



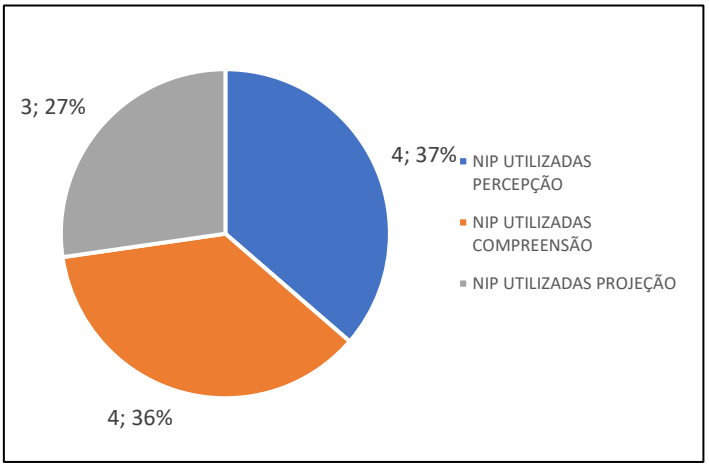
Fonte: Autor

Tabela 42 – NIP utilizadas na Operação Laçador 2013

NIP UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
4	4	3	11

Fonte: Autor

Figura 80 – NIP utilizadas na Operação Laçador 2013



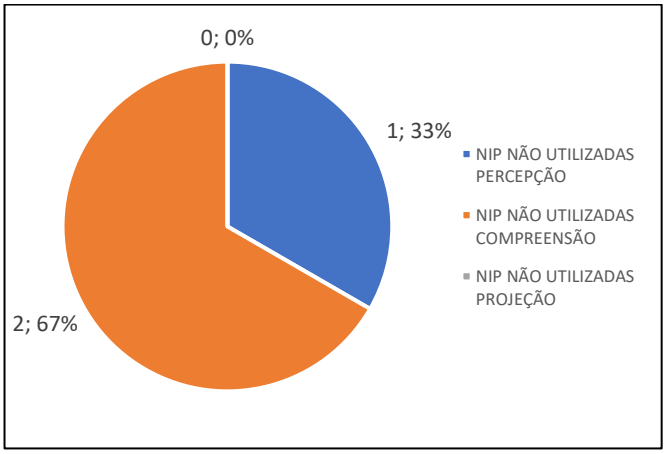
Fonte: Autor

Tabela 43 – NIP não utilizadas na Operação Laçador 2013

NIP NÃO UTILIZADAS			
PERCEPÇÃO	**COMPREENSÃO**	**PROJEÇÃO**	**TOTAL**
1	2	0	3

Fonte: Autor

Figura 81 – NIP não utilizadas na Operação Laçador 2013



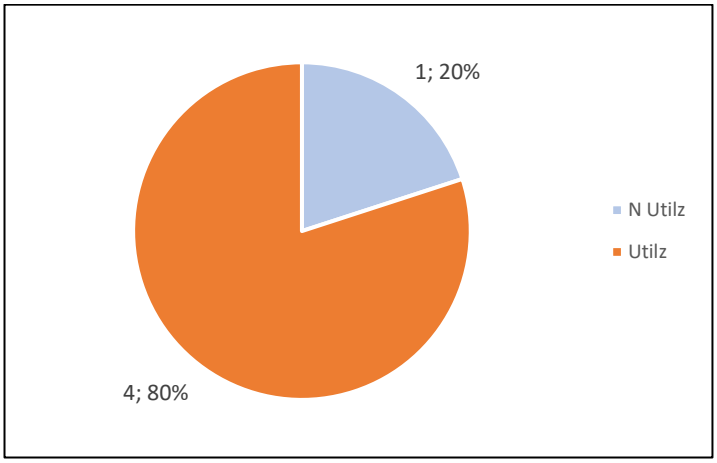
Fonte: Autor

Tabela 44 – NIP utilizadas e não utilizadas de Percepção na Operação Laçador 2013

NIP UTILIZADAS E NÃO UTILIZADAS DE PERCEPÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
1	4	5	20,0	80,0

Fonte: Autor

Figura 82 – NIP utilizadas e não utilizadas de Percepção na Operação Laçador 2013



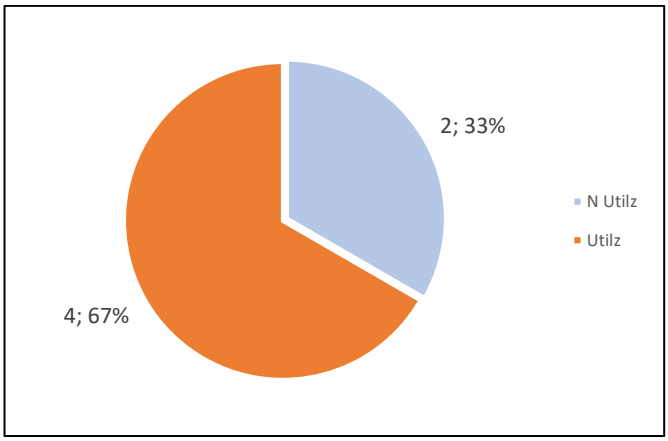
Fonte: Autor

Tabela 45 – NIP utilizadas e não utilizadas de Compreensão na Operação Laçador 2013

NIP UTILIZADAS E NÃO UTILIZADAS DE COMPREENSÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
2	4	6	33,3	66,7

Fonte: Autor

Figura 83 – NIP utilizadas e não utilizadas de Compreensão na Operação Laçador 2013



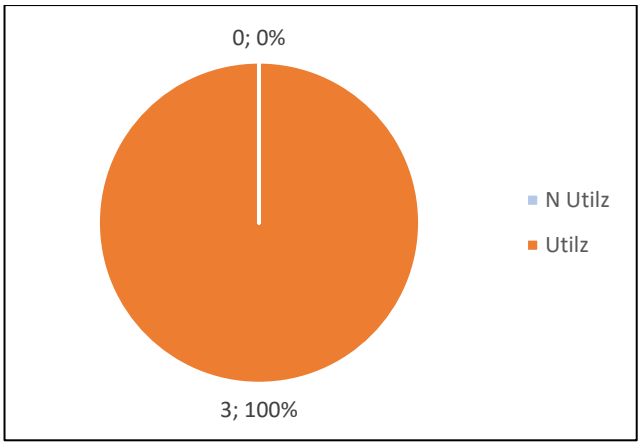
Fonte: Autor

Tabela 46 – NIP utilizadas e não utilizadas de projeção na Operação Laçador 2013

NIP UTILIZADAS E NÃO UTILIZADAS DE PROJEÇÃO				
N Utilz	**Utilz**	**Total**	**% N Utilz**	**% Utilz**
0	3	3	0,0	100,0

Fonte: Autor

Figura 84 – NIP utilizadas e não utilizadas de projeção na Operação Laçador 2013



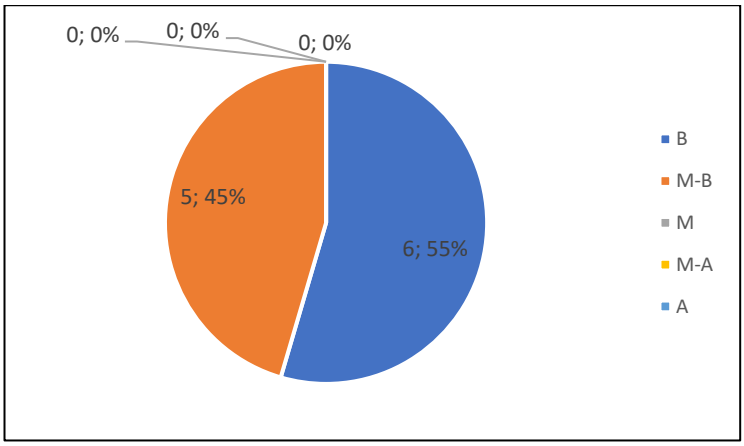
Fonte: Autor

Tabela 47 – Maturidade Geral das NIP na Operação Laçador 2013

MATURIDADE						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**Total**
6	5	0	0	0	3	14

Fonte: Autor

Figura 85 – Maturidade Geral das NIP na Operação Laçador 2013



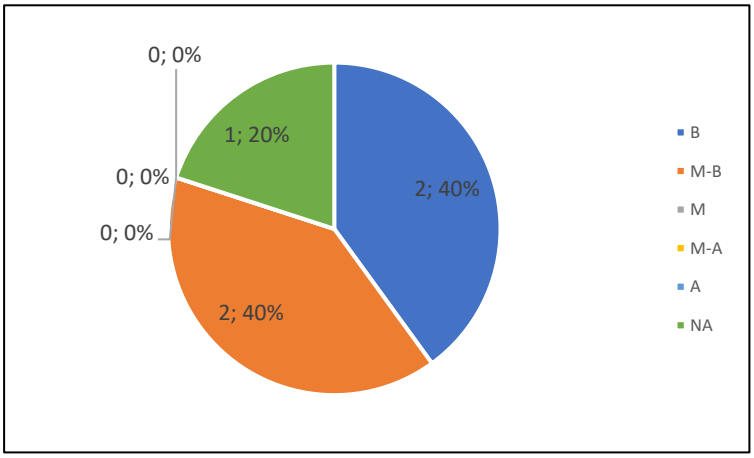
Fonte: Autor

Tabela 48 – Maturidade de Percepção das NIP na Operação Laçador 2013

MATURIDADE DE PERCEPÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
2	2	0	0	0	1	5

Fonte: Autor

Figura 86 – Maturidade de Percepção das NIP na Operação Laçador 2013



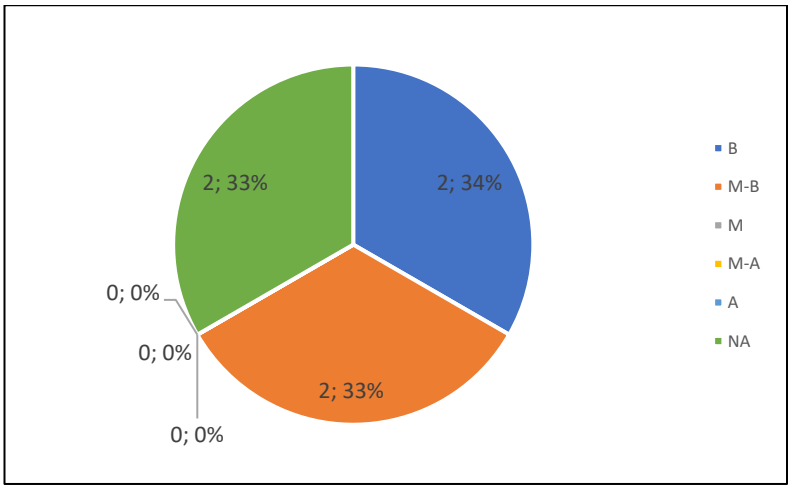
Fonte: Autor

Tabela 49 – Maturidade de Compreensão das NIP na Operação Laçador 2013

MATURIDADE DE COMPREENSÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
2	2	0	0	0	2	6

Fonte: Autor

Figura 87 – Maturidade de Compreensão das NIP na Operação Laçador 2013



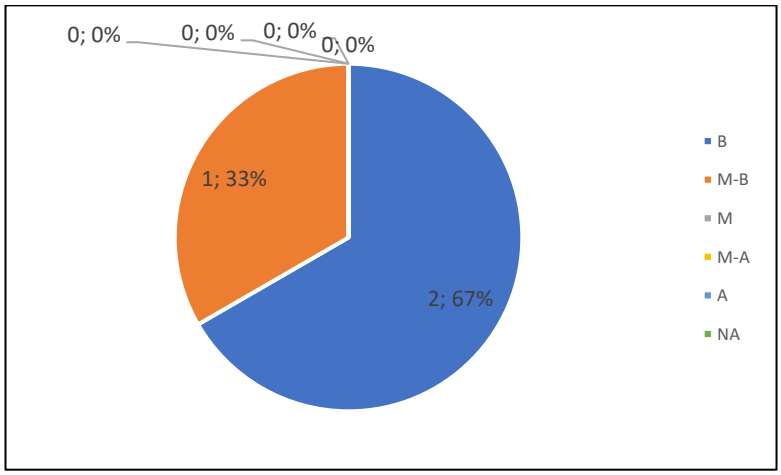
Fonte: Autor

Tabela 50 – Maturidade de Projeção das NIP na Operação Laçador 2013

MATURIDADE DE PROJEÇÃO						
B	**M-B**	**M**	**M-A**	**A**	**NA**	**TOTAL**
2	1	0	0	0	0	3

Fonte: Autor

Figura 88 – Maturidade de Projeção das NIP na Operação Laçador 2013



Fonte: Autor

5.5. OBJETIVO ESPECÍFICO (e)

Neste subtítulo é abordado o objetivo específico (e), qual seja, “e) Discutir a pertinência do *framework* proposto por meio do relacionamento entre as necessidades informacionais primordiais de defesa cibernética e os registros das principais categorias de incidentes e demais eventos anômalos ocorridos nas operações de defesa cibernética no período da pesquisa. Para tal, procedeu-se o registro dos resultados das tarefas (e.1) a (e.3), conforme consta no Quadro 4, no capítulo de Metodologia.

Considerando que o objetivo (e) é eminentemente voltado para discussão dos resultados, neste capítulo de resultados foram registradas as constatações a que se chegou com a resolução das tarefas (e.1) e (e.2), fazendo-se apenas uma breve menção à tarefa (e.3), a qual será completamente explorada no capítulo 6.

5.5.1. Tarefa (e.1)

A tarefa (e.1) teve por finalidade identificar as principais categorias de eventos cibernéticos observados nas operações militares de defesa cibernética no período estudado pela pesquisa, assim como os respectivos processos para lidar com esses eventos.

Para realizar essa tarefa, foram analisados os registros de incidentes de segurança ocorridos nas operações sob estudo, os respectivos registros de LA e APA e os documentos de planejamento para operação. Dessa análise, chegou-se às seguintes constatações:

a) Três categorias principais de eventos considerados anomalias no espaço cibernético de interesse das operações foram comuns a todas as operações: (i) riscos a que estão submetidos os ativos digitais de relevância para a operação; (ii) eventos de segurança (incidentes de segurança ou fatos de relevância) tanto para proteção quanto para a exploração e ataques cibernéticos; (iii) detecção de dados de relevância no canal de atuação da Inteligência.
b) Os processos associados à detecção de cada tipo de anomalia a ser considerada foram: (i) gestão de riscos; (ii) tratamento de incidentes de segurança computacional (para operações de proteção cibernética) ou monitoração do efeito de ataques e explorações (para operações de potencial ofensivo); (iii) ciclo de inteligência para dados captados no canal de Inteligência.

5.5.2. Tarefa (e.2)

A tarefa (e.2) teve por finalidade indicar, para cada categoria de evento e processo identificados na tarefa (e.1), quais as etapas de consciência situacional com os respectivos *schematas* utilizados, conforme os questionamentos obtidos pelo modelo de Barford *et al*. (2010, p. 3-5), adaptados, conforme referencial teórico. O resultado dessa análise está representado nos Quadros 10 e 11.

Nos Quadros 10 e 11, as colunas designadas por Pe1, Pe2, Co1, Co2, Co3, Pr1 e Pr2 correspondem aos questionamentos baseados no modelo de Baford *et al* (2010, p. 3-5), conforme consta do Quadro 2, do capítulo de referencial teórico. As abreviaturas Pe, Co e Pr simbolizam, respectivamente, os estágios de percepção, compreensão e projeção da consciência situacional.

Quadro 11 - Categorias de Eventos Anômalos de interesse para a CS nas Operações dos Grandes Eventos entre 2012 e 2016

CATEGORIAS DE EVENTO ANÔMALO	PROCESSO	OPERAÇÃO	PE 1	PE 2	PRINCIPAIS *SCHEMATAS* DE PERCEPÇÃO	MATUR. DE PERC.	CO 1	CO 2	CO 3	PRINCIPAIS *SCHEMATAS* DE COMPREENSÃO	MATUR. DE COMPREENSÃO	PR1	PR2	PRINCIPAIS *SCHEMATAS* DE PROJEÇÃO	MATUR. DE PROJEÇÃO
Riscos de Ativos	Gestão de Riscos	Rio+20	1	1	Pe1: (1) Diagnósticos de Riscos dos Ativos. Pe2: (1) Processo de atualização de kb.	M-B	1	NA	1	Co1: (1) Diagnósticos de Riscos dos Ativos. Co2: NA Co3: (1) Reuniões técnicas com gerentes de ativos.	M-B	1	1	Pr1: (1) Processo de atualização de diagnósticos de Riscos dos Ativos. Pr2: (1) Diagnósticos de Riscos dos Ativos.	B
Eventos de segurança	Tratamento de Incidentes	Rio+21	3	1	Pe1: (1) Notificações de Segurança; (2) Monitoração de disponibilidade de página; (3) Proteção da própria rede. Pe2: (1) Processo de triagem de evento.	B	1	1	2	Co1: (1) Processo de análise de incidente. Co2: (1) Processo de análise de incidente. Co3: (1) Diagnósticos de Riscos doas Ativos; (2) Processo de análise de incidente.	M-B	2	1	Pr1: (1) Processo de análise de incidente; (2) Notificação de segurança. Pr2: (1) Processo análise de incidente.	B
Detecção no canal de Inteligência	Ciclo de Inteligência	Rio+22	3	1	Pe1: (1) Processo de detecção por Ontologias; (2) Mensagens de Inteligência; (3) Monitoração de ativos. Pe2: (1) Processo de avaliação de fonte de inteligência.	M	1	1	1	Co1: (1) Análise de Inteligência. Co2: (1) Análise de Inteligência. Co3: (1) Análise de Inteligência.	M	3	NA	Pr1: (1) Processo de detecção por Ontologias; (2) Mensagens de Inteligência; (3) Monitoração de ativo. Pr2: NA	M
Riscos de Ativos	Gestão de Riscos	Copa Conf2013	1	1	Pe1: (1) Diagnósticos de Riscos dos Ativos. Pe2: (1) Processo de atualização de kb.	M	1	NA	1	Co1: (1) Diagnósticos de Riscos dos Ativos. Co2: NA Co3: (1) Reuniões técnicas com gerentes de ativos.	M	1	1	Pr1: (1) Processo de atualização de diagnósticos de Riscos dos Ativos. Pr2: (1) Diagnósticos de Riscos dos Ativos.	M
Eventos de segurança	Tratamento de Incidentes	Copa Conf2013	3	1	Pe1: (1) Notificações de Segurança; (2) Monitoração de alguns ativos de forma automática; (3) Proteção da própria rede. Pe2: (1) Processo de triagem de evento.	M	2	1	2	Co1: (1) Processo de análise de incidente; (2) Manual de procedimentos para gestão de incidentes próprio. Co2: (1) Processo de análise de incidente. Co3: (1) Diagnósticos de Riscos dos Ativos; (2) Processo de análise de incidente.	M	2	1	Pr1: (1) Processo de análise de incidente; (2) Notificação de segurança. Pr2: (1) Processo análise de incidente.	M
Detecção no canal de Inteligência	Ciclo de Inteligência	Copa Conf2013	3	1	Pe1: (1) Processo de detecção por Ontologias; (2) Mensagens de Inteligência; (3) Monitoração de ativos. Pe2: (1) Processo de avaliação de fonte de inteligência.	M-A	1	1	1	Co1: (1) Análise de Inteligência. Co2: (1) Análise de Inteligência. Co3: (1) Análise de Inteligência.	M-A	3	NA	Pr1: (1) Processo de detecção por Ontologias; (2) Mensagens de Inteligência; (3) Monitoração de ativo. Pr2: NA	M-A
Riscos de Ativos	Gestão de Riscos	JO 2016	1	1	Pe1: (1) Diagnósticos de Riscos dos Ativos. Pe2: (1) Processo de atualização de kb.	M-A	3	NA	1	Co1: (1) Diagnósticos de Riscos dos Ativos; (2) Relatórios de visitas técnicas; (3) processo de aplicação de ferramenta *end-point* . Co2: NA Co3: (1) Reuniões técnicas com gerentes de ativos.	M-A	1	1	Pr1: (1) Processo de atualização de diagnósticos de Riscos dos Ativos. Pr2: (1) Diagnósticos de Riscos dos Ativos.	M-A
Eventos de segurança	Tratamento de Incidentes	JO 2016	3	1	Pe1: (1) Notificações de Segurança; (2) Monitoração de muitos ativos de canais de comunicação de forma automática; (3) Proteção da própria rede reformulada. Pe2: (1) Processo de triagem de evento.	M-A	2	2	2	Co1: (1) Processo de análise de incidente; (2) Manual de procedimentos para gestão de incidentes do Cert.br. Co2: (1) Processo de análise de incidente; (2) Relatórios de Empresas colaboradoras. Co3: (1) Diagnósticos de Riscos dos Ativos; (2) Processo de análise de incidente.	M-A	3	1	Pr1: (1) Processo de análise de incidente; (2) Notificação de segurança; (3) Alertas de empresas colaboradoras. Pr2: (1) Processo análise de incidente.	M
Detecção no canal de Inteligência	Ciclo de Inteligência	JO 2016	3	1	Pe1: (1) Processo de detecção por Ontologias; (2) Mensagens de Inteligência; (3) Monitoração de ativo. Pe2: (1) Processo de avaliação de fonte de inteligência.	M-A	1	1	1	Co1: (1) Análise de Inteligência. Co2: (1) Análise de Inteligência. Co3: (1) Análise de Inteligência.	M-A	3	NA	Pr1: (1) Processo de detecção por Ontologias; (2) Mensagens de Inteligência; (3) Monitoração de ativo. Pr2: NA	M-A

Fonte: Autor

Quadro 12 - Categorias de Eventos Anômalos de interesse para a CS nas Operações Atlântico III 2012 e Laçador 2013

CATEGORIAS DE EVENTO ANÔMALO	PROCESSO	OPERAÇÃO	PE1	PE2	PRINCIPAIS *SCHEMATAS* DE PERCEPÇÃO	MATUR. DE PERC.	CO1	CO2	CO3	PRINCIPAIS *SCHEMATAS* DE COMPREENSÃO	MATUR. DE COMPREE.	PR1	PR2	PRINCIPAIS *SCHEMATAS* DE PROJEÇÃO	MATUR. DE PROJ.
Riscos de Ativos	Gestão de Riscos	Atlântico III	1	NA	Pe1: Orientações de segurança nos planejamentos operacionais. Pe2: NA.	M	NA	NA	NA	Co1: NA Co2: NA Co3: NA	NA	NA	NA	Pr1: NA Pr2: NA	NA
Eventos de segurança (proteção, exploração e ataque)	Tratamento de Incidentes; Processos de ataque e exploração.	Atlântico III	1	2	Pe1: (1) Problemas militares simulados (PMS). Pe2: (1) Classificação d informação no pms (quando disponível); (2) processo de triagem de incidente narrado em PMS.	M	3	3	3	Co1: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais. Co2: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais. Co3: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais.	M	3	3	Pr1: (1) PMS; Pr2: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais.	M
Detecção no canal de Inteligência	Ciclo de Inteligência	Atlântico III	1	2	Pe1: (1) Problemas militares simulados (PMS). Pe2: (1) Classificação d informação no pms (quando disponível); (2) processo de análise de inteligência.	M	3	3	3	Co1: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais. Co2: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais. Co3: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais.	M	3	3	Co1: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais. Co2: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais. Co3: (1) PMS; (2) Processo de tratamento de incidentes; (3) Técnicas de brain storm e mapas mentais.	M
Riscos de Ativos	Gestão de Riscos	Laçador 2013	1	NA	Pe1: Orientações de segurança nos planejamentos operacionais. Pe2: NA.	M	1	NA	1	Co1: (1) PMS; Co2: NA Co3: (1) PMS	NA	NA	NA	Pr1: NA Pr2: NA	NA
Eventos de segurança (proteção, exploração e ataque)	Tratamento de Incidentes; Processos de ataque e exploração.	Laçador 2013	1	2	Pe1: (1) Problemas militares simulados (PMS). Pe2: (1) Classificação de informação no pms (quando disponível); (2) processo de triagem do incidente narrado em PMS.	M-B	2	2	2	Co1: (1) PMS; (2) Processo de tratamento de incidentes. Co2: 1) PMS; (2) Processo de tratamento de incidentes. Co3: 1) PMS; (2) Processo de tratamento de incidentes.	M-B	2	2	Pr1: (1) PMS; (2) Processo de tratamento de incidentes. Pr2: (1) PMS; (2) Processo de tratamento de incidentes.	M-B
Detecção no canal de Inteligência	Ciclo de Inteligência	Laçador 2013	1	2	Pe1: (1) Problemas militares simulados (PMS). Pe2: (1) Classificação d informação no pms (quando disponível); (2) Processo de análise de inteligência.	M	2	2	2	Co1: (1) PMS; (2) Análise de Inteligência. Co2: 1) PMS; (2) Análise de Inteligência. Co3: 1) PMS; (2) Análise de Inteligência.	M-B	2	2	Pr1: (1) PMS; (2) Análise de Inteligência. Pr2: (1) PMS; (2) Análise de Inteligência.	M-B

Fonte: Autor

5.5.3. Tarefa (e.3)

A tarefa (e.3) teve por finalidade analisar comparativamente os resultados obtidos pela execução da tarefa (e.2) com os resultados obtidos do objetivo específico (d), mais especificamente a tarefa (d.2).

Essa análise comparativa será efetivada no capítulo 6, sendo registrado na conclusão deste capítulo de resultados os seguintes pontos de atenção na comparação efetuada:

a) A comparação foi efetuada entre os resultados da aplicação do *framework* das NIP proposto pela pesquisa e os resultados da aplicação do modelo de Barford *et al*. (2010, p. 3-5), adaptado, em dois grupos distintos: operações dos Grandes Eventos e as operações de adestramento militar do MD.
b) As mesmas escalas utilizadas para verificar a aplicação das NIP na tarefa (d.2) foram utilizadas para estimar os valores de maturidade nos quadros referentes à tarefa (e.3).
c) Foi observado que entre as operações dos Grandes Eventos houve uma nítida escalada na maturidade do exercício da consciência situacional, sendo que, de uma operação para a outra, cada item analisado se apresentou mais elevado que o anterior ou, em apenas 4 das 27 estimativas, permaneceu estável, o que se mostrou estar em consonância com a progressão esperada pela aplicação das NIP.
d) Foi observado que entre as operações Atlântico III e Laçador 2013 houve uma leve retração na maturidade do exercício da consciência situacional, sendo que, de 9 pares de itens analisados (3 categorias de eventos anômalos x 3 estágios de CS, para cada operação), 1 não foi aplicado, 1 aumentou, 2 permaneceram estáveis e 5 regrediram, o que parece estar em contraposição com a progressão esperada pela aplicação das NIP.

No próximo capítulo, são providas as discussões que complementam e interpretam os resultados registrados neste capítulo.

6. DISCUSSÃO DOS RESULTADOS

Neste capítulo são discutidos os resultados da pesquisa, conforme estabelecido pelos objetivos específicos do trabalho. Considerando a estrutura dos objetivos, as discussões foram concentradas nos objetivos específicos (d) e (e), por meio dos quais foi gerado e avaliado o produto final da pesquisa, ou seja, o *framework* de necessidades informacionais primordiais para consciência situacional de defesa cibernética. Além da demonstração do alcance do resultado proposto para o trabalho, este capítulo de discussões busca verificar, por meio das observações dos fatos analisados a pertinências das escolhas realizadas no referencial teórico.

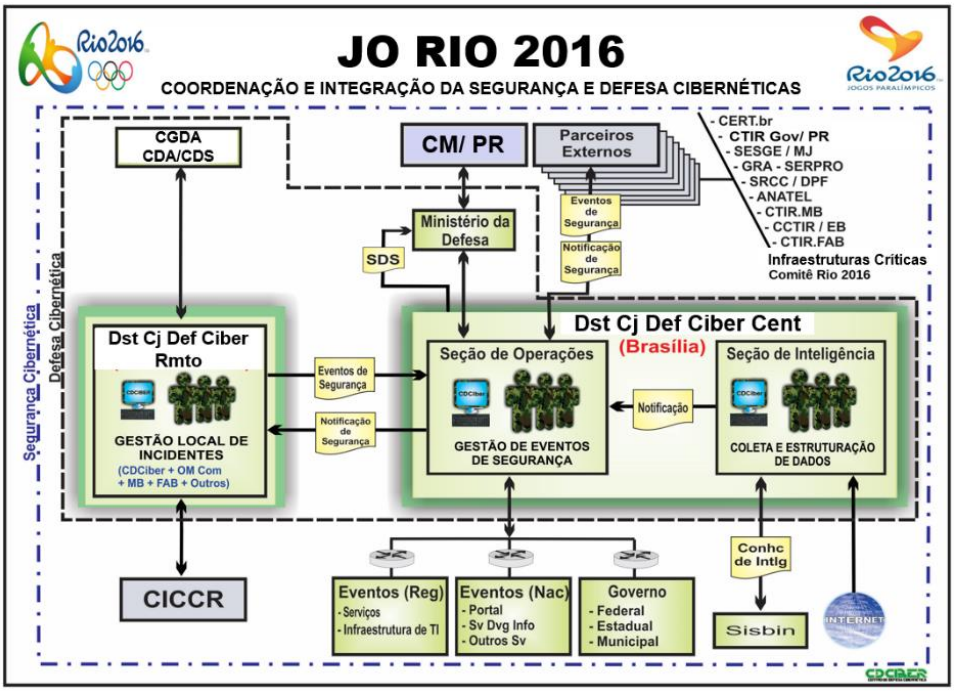
6.1. OBJETIVO ESPECÍFICO (a)

As tarefas (a.2) e (a.3), correspondem às ações de identificar, de modo justificado, os *frameworks* de segurança da informação e cibernética e de defesa ativa de maior compatibilidade com a pesquisa, assim como estabelecer quais, especificamente, devem ser utilizados na tese.

De modo a ser possível justificar a escolha, é importante apresentar uma breve caracterização das operações de defesa cibernética ocorridas no período estudado à luz da documentação doutrinária expedida à época. A forma mais simples de prover essa descrição é fazer uso de uma imagem exaustivamente apresentada em conferências, simpósios, além de outros tipos de eventos dessa natureza, pelos representantes do Centro de Defesa Cibernética, dentre eles o autor desta tese. O CDCiber foi a organização militar do Exército Brasileiro que, na ocasião dos eventos estudados, desempenhou papel central nas operações de defesa cibernética de 2012 a 2016, em especial os chamados Grandes Eventos. Essa imagem está representada na Figura 88.

Foi escolhida a versão da imagem utilizada para o último grande evento, qual seja, os Jogos Olímpicos e Paralímpicos, pois foi a que mais agregou as melhorias desde o primeiro grande evento, a Rio+20. Cabe ressaltar que, embora com algumas modificações, a essência do modelo de atuação permaneceu fundamentalmente a mesma em todas as operações. O modelo representado sempre esteve associado ao Destacamento de Defesa Cibernética (Dst DefCiber), a unidade temporária que representava o CDCiber nas operações, conforme já descrito nesta pesquisa.

Figura 89 - Modelo gráfico da forma de atuação do Dst DefCiber



Fonte: Autor.

Nas apresentações públicas realizadas com base na imagem representada na Figura 88, buscou-se transmitir os seguintes significados essenciais do que a ilustração simboliza:

(i) O Destacamento era desdobrado em duas partes, uma central que atuava nas instalações físicas do CDCiber, e outras remotas (Dst Rem), que atuavam em diversas partes do país, conforme a operação, a exceção da operação Rio+20, onde toda a força de trabalho concentrou-se no local do evento.

(ii) O Destacamento Central (Dst Central) coordenava todas as ações e atuava num modelo híbrido, operando de forma similar a um CSIRT (Seção de Operações) e unidade de inteligência (Seção de Inteligência).

(iii) O Destacamento Central atuava como um concentrador e distribuidor de informações, fossem eventos de segurança cibernética, os quais eram compartilhados com parceiros externos, fossem informações de inteligência, as quais eram compartilhadas com as agências de inteligência parceiras ou, conforme a natureza da informação coletada, com a Seção de Operações.

(iv) O Dst Central recebia, ainda, informações de sensores remotos que monitoravam ativos de tecnologia da informação de interesse, além dos mensagem dos Destacamentos Remotos. Nas localidades desses sensores e Dst Rem, os gestores de TI e segurança eram orientados a adotarem as melhores práticas de segurança cibernética nos seus ativos e manter seu estado de segurança informado ao Dst Central.

(v) Os Destacamentos Remotos eram compostos por representantes do Dst Central que atuavam como que sensores nas localidades em que havia centros de comando e controle civis e militares. A missão desses representantes era prover informações ao Dst Central sobre qualquer evento local de segurança cibernética, inteligência desenvolvida no espaço cibernético ou outro evento que, potencialmente, pudesse estar relacionado ao espaço cibernético de interesse da missão.
(vi) As operações eram precedidas de análises e avalições de riscos dos ativos envolvidos na missão, com suporte de empresa especializada, resultando esse trabalho na composição de inventário de ativos críticos para a missão e diagnostico de riscos desses ativos.
(vii) O Dst Central atuava como um centro de consciência situacional de defesa cibernética para os comandos e coordenações gerais evolvidos na operação, trocando mensagens diárias com o Ministério da Defesa e Comandantes das localidades remotas.
(viii) Nos grandes eventos a atuação de Destacamento era eminentemente de proteção cibernética.
(ix) Nas operações de adestramento militar, as quais simulavam conflitos internacionais para treinamento das tropas sob coordenação do Ministério da Defesa, a atuação do Dst Def Ciber deveria cobrir todas as ações cibernética doutrinárias: proteção, exploração e ataque cibernético (Brasil, 2014, p.23).

Em síntese, o desenvolvimento do Setor Cibernético na Defesa Nacional no período coberto pela pesquisa teve quatro aspectos principais de nível operacional: gestão de riscos em segurança cibernética, gestão de incidentes de segurança cibernética, inteligência advinda da fonte cibernética e técnicas de exploração e ataque cibernético. Este último aspecto, o de exploração e ataque, possivelmente o mais importante de todos, pois é o aspecto que diferencia a defesa cibernética da segurança cibernética, foi desenvolvido de forma diminuta se comparado aos outros no mesmo período, devido à falta de capacitação, talentos, legislação e infraestrutura para atuação.

Em consequência, o *framework* que tem larga aceitação e execução bem-sucedida nas organizações em nível mundial e com características de segurança cibernética que vai ao encontro dos três primeiros aspectos citados, é o *framework* NIST CSF. Considerando-se as cinco funções principais do NIST CSF, as funções identificar e proteger cobrem sobejamente o aspecto de gestão de riscos e

parcialmente a de inteligência, e as demais, ou seja, detectar, responder e recuperar, cobrem a gestão de incidentes e, mais uma vez, parcialmente a inteligência.

Para o último aspecto, qual seja o de exploração e ataque cibernético, há uma certa equivalência entre o *framework* MITRE e as metodologias do NIST 800-115 e OSSTMM, com certa predominância para este último. No entanto tanto o NIST 800-115 e OSSTMM são metodologias mais compatíveis com processo e planejamento de testes de intrusão, enquanto o MITRE tem em sua estrutura a apresentação das táticas principais e técnicas e subtécnicas para compor explorações e ataques. Na estruturação de um processo corporativo, todos esses métodos acabam por ser complementares. No entanto, para efeito de produção de necessidades informacionais primordiais de defesa cibernética, o MITRE se mostra mais direto.

Assim, satisfazendo as tarefas (a.2) e (a.3) e encerrar a execução do objetivo (a) desta pesquisa, foram escolhidos os *frameworks* NIST CSF e MITRE ATT&CK.

6.2. OBJETIVO ESPECÍFICO (b)

A tarefa (b.1) teve por finalidade declarar o critério para relacionar o ciclo de gestão do conhecimento e os controles que integram os *frameworks* selecionados, conforme escolhas adotadas no referencial teórico. Nesse sentido, o critério serviu de via pela qual se pôde varrer os controles dos *frameworks* selecionados, discernindo-se qual controle correspondia majoritariamente a qual aspecto de teoria adota para defesa cibernética.

Para a estruturação desse critério, foi preciso rememorar o recorte e as definições dadas no referencial teórico sobre as arenas de conhecimento. Quanto ao recorte, conforme referencial teórico, a pesquisa focalizou os aspectos de teoria adotada de cada arena. Como desdobramento desse recorte, as definições dos elementos de teoria adotada para as arenas de formação de significado, criação de conhecimento e tomada de decisão, foram adaptadas, o que, de forma condensada e para fins desta pesquisa, chamou-se de teoria adota para defesa cibernética. Esses elementos estão representados em conjunto na Figura 35.

Como consequência do fato de haver três elementos que compõem a teoria adotada para a defesa cibernética, o critério buscado foi subdividido em três componentes correspondentes às interpretações, ao conhecimento explícito e as

regras para defesa cibernética. Por sua vez, para cada um desses componentes, outros desdobramentos foram efetuados para comportar as possibilidades de categorias de elementos informacionais, passíveis de serem gerados no ciclo de conhecimento aplicado à cibernética.

Assim, os subcritérios estabelecidos para o objetivo (b) da pesquisa foram declarados tendo as respectivas sentenças obedecido a uma mesma estrutura que denotasse a busca, nos controles e táticas dos *frameworks,* de ações que realizassem ou gerassem produtos informacionais, conforme o aspecto da teoria adotada. Cabe ressaltar que, no elemento de tomada de decisão, foram enunciados produtos informacionais específicos, conforme estabelecimento feito no referencial teórico.

Deste modo, os controles e táticas dos *frameworks* escolhidos foram analisados, um a um, sob os critérios do Quadro 5, escolhendo-se o subcritério de maior compatibilidade com o elemento vindo do *framework*. Logo, para que tal ou qual controle ou tática fosse relacionado com um aspecto específico da teoria adotada para defesa cibernética, foi realizada a escolha considerada como a mais compatível, segundo a aplicação do critério.

Assim, deve-se ressaltar que não foi possível estabelecer uma relação unívoca e exata subcritério-controle ou tática, mas uma abordagem da relação considerada a mais provável. Do observado pelo autor desta pesquisa, um fator de alta relevância para aumentar as chances de as escolhas desses relacionamentos serem pertinentes é reunir no aplicador do critério a familiaridade teórica com os *frameworks* escolhidos e a com a teoria de conhecimento organizacional, assim com suas aplicações reais, além de conhecer a organização onde o conjunto de será aplicado.

As únicas exceções consideradas pelo pesquisador no estabelecimento de uma relação um a um, entre aspectos da teoria adota de defesa cibernética e os elementos do *framework* de teoria adotada para defesa cibernética, foram as táticas 1, 2, 3 e 11 advindas do MITRE. O porquê dessas repetições esteve relacionado com o fato de essas táticas serem de tal natureza que sua consecução se estende num *continuum* pelas fases da teoria adotada para defesa cibernética. Tal fato ocorre tanto com controles do NIST CSF quanto táticas do MITRE, no entanto em graus

considerados menores para aplicação da pesquisa, prevalecendo, como explanado neste subtítulo, o critério de aplicabilidade mais compatível.

6.3. OBJETIVO ESPECÍFICO (c)

De modo a justificar e discutir a respeito da escolha do critério para relacionar os elementos do *framework* de teoria adotada para defesa cibernética e os estágios da consciência situacional, conforme estabelecido para a tarefa (c.1), faz-se necessário recordar o segundo recorte estabelecido no referencial teórico sobre os aspectos da consciência situacional que são compatíveis com a teoria adotada para defesa cibernética. Esse recorte estabeleceu o foco nos fatores individuais, em particular os elementos de pré-atenção e de memória de longo prazo, conforme as Figuras 28 e 29.

Mais especificamente, a pesquisa focalizou os insumos desses elementos que foram viáveis para observação e manuseio pela pesquisa, devido à sua natureza compatível com a teoria adotada para defesa cibernética. Esses elementos são os *schematas*, os quais, partindo de sua forma mais concreta e geral, podem se desdobrar desde o seu aspecto mais granular, ou seja, os *scripts*, até a sua forma mais subjetiva, ou seja, os modelos mentais. Assim, partindo-se desses elementos, elaborou-se o Quadro 8 para consecução da tarefa (c.1).

O Quadro 8 representa os critérios estabelecidos para relacionamento dos controles do *framework* de teoria adotada para defesa cibernética, partindo-se dos questionamentos estabelecidos como guias no referencial teórico, desdobrando-se destes os critérios buscados. Como se pode verificar da redação dos subcritérios, foi demandado que o controle, uma vez convertido em NIP, pudesse gerar um *schemata* correspondente às condições que satisfizessem à NIP. As únicas exceções a essa explicitação do *schemata* nos subcritérios foi quando estes se referiam aos insumos metas, objetivos e perspectivas, pois, pela sua natureza direcionadora e necessariamente, ao mesmo tempo, sintética e clara, esses insumos, em si, foram considerados *schematas*.

Cabe destacar, no Quadro 8, o critério 3. Nesse critério, buscou-se descrever o tipo de formato utilizado para representar a necessidade informacional primordial, optando-se pelo formato de questionamento, a partir de uma abordagem de Choo

(1998, p.26). Para a determinação de necessidades informacionais, Choo (1998, p.26), coloca um conjunto de seis perguntas como desdobramento de uma pergunta principal, “o que você quer saber?”. As seis perguntas desdobradas são: (i) “por que você precisa saber disso?”; (ii) “com o que o seu problema se parece?”; (iii) “o que você já sabe?”; (iv) “o que você pode antecipar?”; (v) “como isso pode ajudar você?”; (vi) “em que forma você precisa saber disso?”

Considerou-se que as perguntas de (i) a (v), além da própria pergunta principal conforme Choo propõe, estão totalmente contextualizadas e, em termos gerais, respondidas, dados os elementos de base da pesquisa, quais sejam, a escolha de *frameworks* de segurança e defesa cibernética, em particular pelo seu caráter de reunir as melhores práticas de cibernética, a organização dessas melhores práticas de acordo com a teoria do conhecimento organizacional para promoção de aprendizado organizacional, com ênfase na teoria adota, e, por fim, o foco na consciência situacional de defesa cibernética para operações dessa natureza.

Ressaltando que a expressão da necessidade informacional deve ser feita controle a controle e tática a tática, percebe-se que a pergunta principal “o que você quer saber?”, é a mais diretamente respondida nas condições da pesquisa, pois cada controle ou tática, em si, já constituem a resposta. Resta assim, determinar como esses controles e táticas devem ser adaptados à sua aplicação no ambiente organizacional.

Desse modo, resta responder a pergunta (vi), “em que forma você precisa saber disso?”. Assim, adotou-se o procedimento de adaptar a pergunta (vi) de tal modo que a necessidade informacional fosse expressa de modo a demandar de que forma o controle ou tática deveria ser adotado.

Os Quadros 9 e 10 cumprem a tarefa (c.2), sintetizando a aplicação dos critérios estabelecidos na tarefa (c.1), conforme Quadro 8, nos elementos do *framework* de teoria adotada para defesa cibernética, produzindo o resultado buscado na pesquisa: o *framework* de necessidades informacionais primordiais para consciência situacional de defesa cibernética (*framework* de NIP-CS-DC). Neste ponto do trabalho, pode-se afirmar que esse resultado, dado todo o trajeto metodológico realizado, produz um instrumento para o qual se espera que a sua aplicação gere o aumento da capacidade da formação de consciência situacional em uma operação de defesa cibernética. Para se aferir se essa expectativa extrapola o

meramente possível e o verossímil, chegando ao provável, os dois objetivos específicos finais, letras (d) e (e), são discutidos nos subtítulos a seguir.

6.4. OBJETIVO ESPECÍFICO (d)

As discussões a respeito do objetivo específico (d) estão focadas na complementação da tarefa (d.2), cuja solução, conforme disposta no capítulo 5, descreveu em valores a aplicação das NIP nos Grandes Eventos e nas operações do Ministério da Defesa. Assim, restou revelar como, além dos resultados observáveis em operações específicas, a aplicabilidade das NIP se mostra na linha do tempo, considerando o conjunto das operações estudadas. Para efetuar essa comparação, dois grupos foram discernidos: operações dos Grandes Eventos e operações de adestramento militar do Ministério da Defesa ou, simplesmente, operações do MD.

6.4.1. Operações de Grandes Eventos

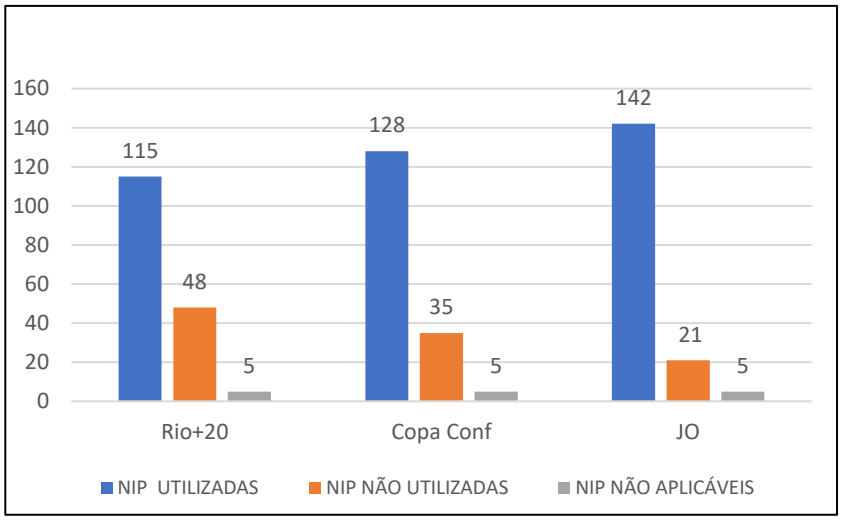
A sequência de informações para realizar as comparações entre as operações de grandes eventos seguiu a lógica dos dados apresentados no capítulo de resultados. Assim, foram explicitadas, entre as operações como um todo, os dados e gráficos das NIP utilizadas, em geral e por estágio de consciência situacional, assim como os números relativos à maturidade. A Tabela 52 inicia a sequência mostrando a progressão das NIP utilizadas por operação, cuja representação gráfica está nas Figuras 89 e 90.

Tabela 51 – Resultados gerais da aplicação das NIP nas Operação de Grandes Eventos

OPERAÇÃO	NIP UTILIZADAS	INCREM. NIP UTIL.	NIP NÃO UTILIZADAS	NIP NÃO APLICÁVEIS	% Total	TOTAL
Rio+20	115	0,0%	48	5	68,5%	168
Copa Conf	128	7,7%	35	5	76,2%	168
JO	142	8,3%	21	5	84,5%	168
Total Acum	-----	16,1%	-----	-----	-----	-----

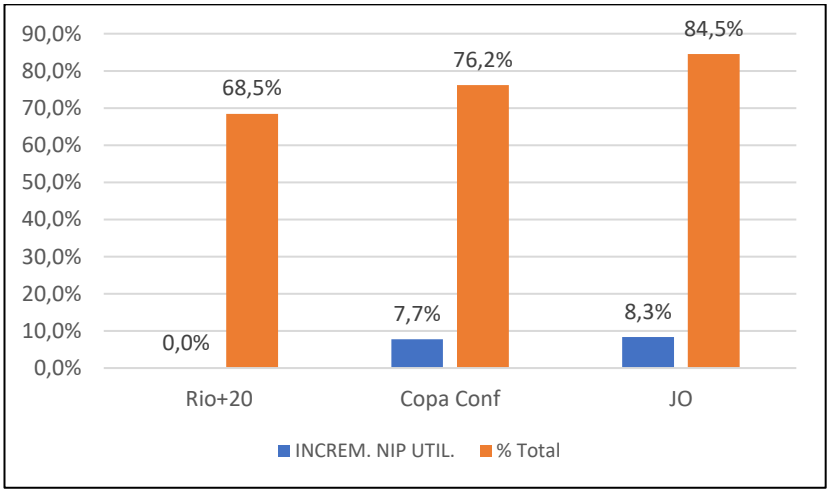
Fonte: Autor

Figura 90 – Operações Grandes Eventos - Resultados Gerais



Fonte: Autor

Figura 91 – Operações Grandes Eventos - Incrementos de NIP Utilizadas



Fonte: Autor

Da leitura da Tabela 52 e das Figuras 89 e 90, é possível constatar que a aplicação das NIP progrediu na linha do tempo, aumentando o número de NIP consideradas na operação, sugerindo, portanto, o incremento da capacidade de consciência situacional de defesa cibernética, conforme analisado nesta pesquisa.

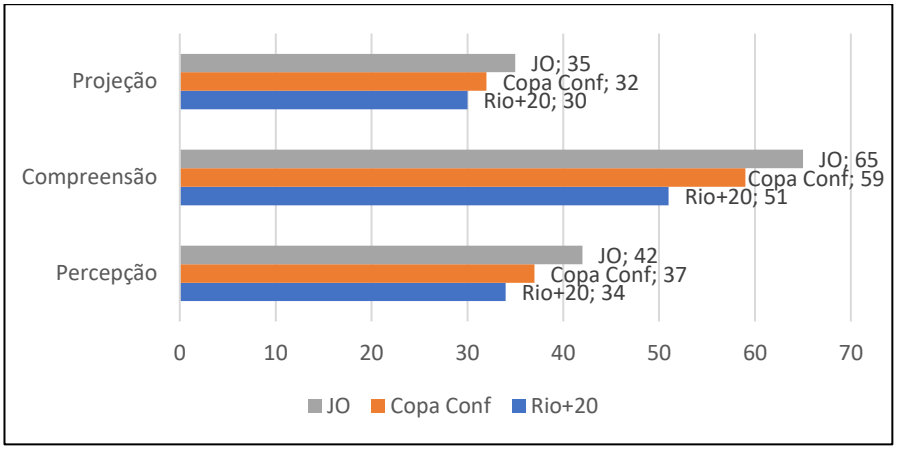
Repetindo-se o mesmo tipo de verificação, considerando-se agora cada estágio de consciência situacional, obtém-se a Tabela 53 e as Figuras 91 e 92.

Tabela 52 – NIP Utilizadas por estágio de CS para todas as Operações de Grandes Eventos

NIP UTILIZADAS							
Operação	**Percepção**	**Increm. Percepção**	**Compreensão**	**Increm. Compreensão**	**Projeção**	**Increm. Projeção**	**TOTAIS**
Rio+20	34	0%	51	0%	30	0%	115
Copa Conf	37	6%	59	10%	32	5%	128
JO	42	10%	65	8%	35	7%	142
Total Acum.	-----	17%	-----	18%	-----	12%	-----

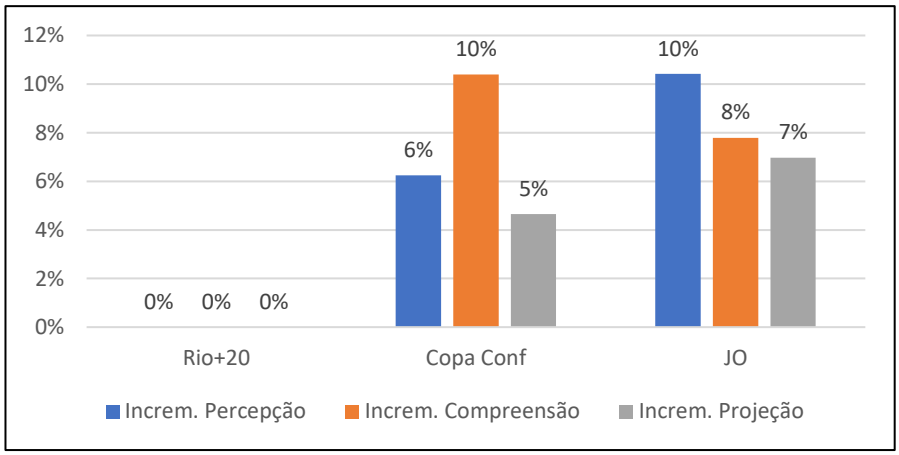
Fonte: Autor

Figura 92 – NIP Utilizadas por estágio de CS para todas as Operações



Fonte: Autor

Figura 93 – Incremento de NIP na Operações de Grandes Eventos por estágio de CS



Fonte: Autor

Observando-se a Tabela 53 e as Figuras 91 e 92, vê-se que a aplicação das NIP, por estágio de CS aumenta de operação para operação. Da Figura 92, percebe-se um incremento maior de compreensão na Copa das Confederações 2013, enquanto uma expressiva melhora na percepção durante os Jogos Olímpicos. Esses

incrementos de destaque vão ao encontro do testemunho do pesquisador, que, em ambas as operações, era o comandante do Destacamento de Defesa Cibernética, podendo, assim, complementar a interpretação desses incrementos.

Em relação à Copa das Confederações, durante o evento, houve uma inesperada troca no eixo das ameaças ao evento devido às grandes manifestações ocorridas no país no mesmo período. Embora o alvo inicial das manifestações não fosse o evento esportivo, a Copa das Confederações acabou por se tornar um foco adicional de interesse dos manifestantes. Assim, grupos *hackers* deflagaram operações contra o evento, assim como, nas mídias sociais como *FaceBook*[23] e, como era denominado à época, o *Twitter*[24], houve inúmeras mobilizações de manifestações, como desenvolvê-las, como enfrentar a polícia, onde eram os lugares melhores para deslocamento de pessoal que estivesse em pontos diferentes da cidade etc.

Com relação às atividades *hackers*, o Dst de Defesa Cibernética, por intermédio da sua equipe de operações, a qual contava com pessoal muito mais experiente em gestão de incidentes do que na Rio+20, elaborou *schematas*, em forma de manuais de procedimento, para gerir incidentes de rede, com classificação e tratamento específico da maioria dos ataques conhecidos, o que incrementava em muito a capacidade de análise de um evento anômalo e, em consequência, a sua compreensão.

A operação contra a Copa das Confederações por ataques cibernéticos foi pouco efetiva. Primeiro, por não haver alvos relacionados ao evento que fossem compensadores, ou seja, cujo comprometimento causasse impactos severos à realização da Copa as Confederações. Segundo, os atacantes pareceram menos organizados do que na Rio+20 e aparentemente dissuadidos de realizar ataques mais ousados, devido, provavelmente, a aprovação de lei que podia os incriminar[25], o que não ocorria na época do grande evento anterior, o que resultou em o Dst de Defesa Cibernética tratar eventos de menor impacto.

---

[23] https://www.facebook.com/
[24] https://twitter.com/
[25] Lei Nº 12.737, de 30NOV2012, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

Por outro lado, a Seção de Inteligência do Dst teve de desdobrar para tratar uma quantidade muito elevada de eventos captados nas mídias sociais e que colocavam, de um modo geral, a ordem em várias cidades do país em risco, filtrando os dados falso-positivos, especificando o interlocutor adequado para compartilhamento, além de outros tratamentos de informação, o que refinou sua capacidade interpretativa dos fatos e, por conseguinte, a capacidade de compreensão.

Quanto à melhoria expressiva no quesito de uso de NIP de percepção durante os Jogos Olímpicos, pode-se afirmar com precisão que a o incremento é condizente com a realidade observada, pois, nos JO, o Dst contava com um maior número de instrumentos e mecanismos para detecção de anomalias no espaço cibernético. Considerando apenas as ferramentas tecnológicas, próprias ou de parceiros associados, havia disponível mais que o triplo de ferramentas usadas na Copa das Confederações, focando em partes distintas do espaço cibernético de interesse da operação.

O próximo quesito a se discutir e interpretar é sobre a maturidade. Foram analisadas comparativamente as maturidades gerais dos três grandes eventos, assim como as maturidades por estágio de CS. O parâmetro de maturidade foi percebido como essencial à análise dos dados, uma vez constatado que uma mesma NIP poderia ser aplicada em ocasiões diferentes, porém com níveis de profundidade e complexidade diversos, exigindo cada vez maiores e melhores conhecimentos para sua gestão.

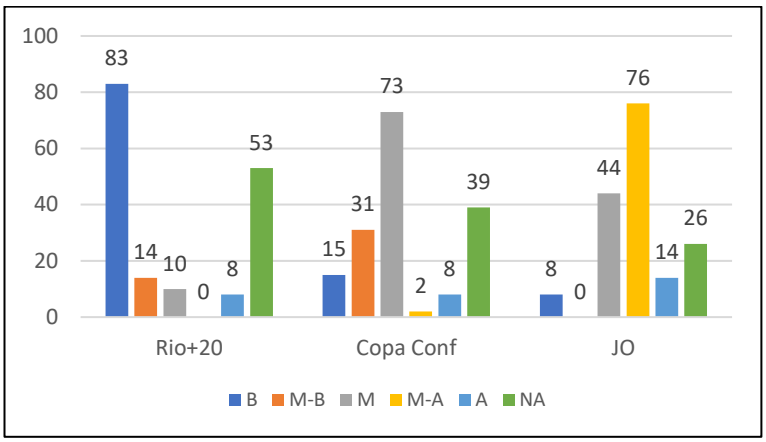
As discussões foram apresentadas por grupos de tabelas e gráficos, abordando-se assim, números gerais e por estágio de CS. Assim, são representadas nas Tabelas 54 a 51 com as respectivas Figuras, de 93 a 104, onde os parâmetros de maturidade estão dispostos e interpretados.

Tabela 53 – Quantitativo e % de aplicação de NIP por Maturidade nas Op Grandes Eventos

QUANTITATIVO DE NIP POR MATURIDADE													
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**	**Total**
Rio+20	83	49,4%	14	8,3%	10	6,0%	0	0,0%	8	4,8%	53	31,5%	168
Copa Conf	15	8,9%	31	18,5%	73	43,5%	2	1,2%	8	4,8%	39	23,2%	168
JO	8	4,8%	0	0,0%	44	26,2%	76	45,2%	14	8,3%	26	15,5%	168

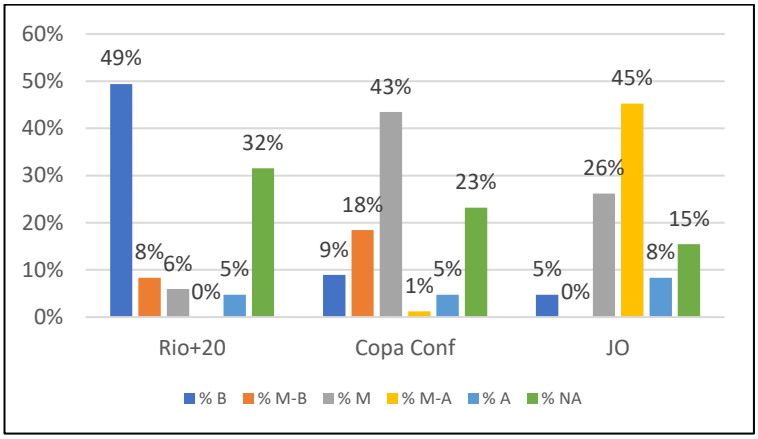
Fonte: Autor

Figura 94 – Quantitativo de aplicação de NIP por Maturidade nas Op Grandes Eventos



Fonte: Autor

Figura 95 – Percentual de aplicação de NIP por Maturidade nas Op Grandes Eventos



Fonte: Autor

Dentre as constatações possíveis de serem extraídas pela análise dos dados da Tabelas 53 e Figuras 93 e 94, dois conjuntos são de destaque. A primeiro é a observação dos seguintes fatos: (i) predominância da quantidade de NIP aplicadas com baixa maturidade na primeira operação estudada, a Rio+20, o que é coerente com o estágio de desenvolvimento incipiente da atividade de defesa cibernética no Brasil, em particular no CDCiber; (ii) a predominância da quantidade de NIP aplicadas de grau médio na Copa das Confederações e diminuição expressiva da quantidade de NIP de maturidade baixa, refletindo, a realidade de aprendizado das equipes envolvidas, pois, por ocasião da Copa das Confederações já havia sido acumulado um conjunto de lições aprendidas da Rio+20 e de duas operações de

treinamento do MD, além de o Dst contar com pessoal melhor capacitado, porém com poucos produtos de tecnologia e processos ainda em desenvolvimento; (iii) a predominância de quantitativo de NIP de maturidade médias-altas nos JO, o que vai ao encontro do observado na ocasião pelo pesquisador, pois à época dos JO, o CDCiber, portanto o Dst de Defesa Cibernética contava com um acumulado de LA e uma dezena de operações de maior importância, treinamento de maior nível e quantidade para o pessoal e aparato tecnológico de maior e melhor alcance e em quantidade muito superiores aos outros eventos.

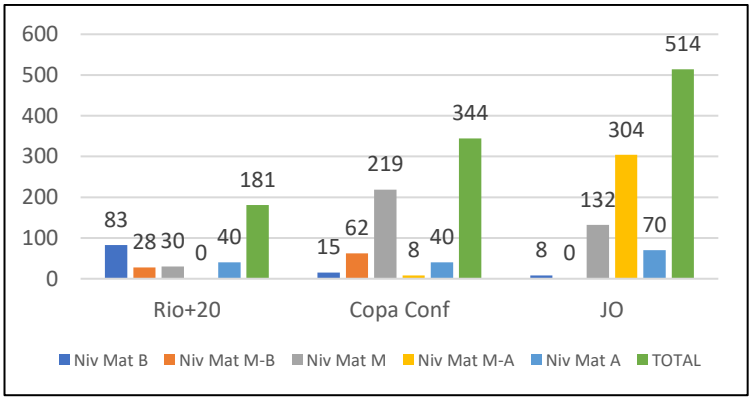
O segundo conjunto de fatos diz respeito a constatação de que a verificação dos quantitativos de aplicação de NIP em termos de maturidade, embora revelasse predominâncias de determinados tipos, não deixava claro o progresso como um todo da aplicação das NIP na linha do tempo, pois os quantitativos de aplicação de NIP dos graus observados variaram entre si, seja na mesma operação ou entre operações, dificultando apreender progressos globais. Em consequência, buscou-se consolidar os parâmetros de maturidade em valores que revelassem se houve ou não progresso geral na sua aplicação, o que leva ao representado na Tabela 55 e a Figura 95.

Tabela 54 – Grau de Maturidade da aplicação das NIP nas Op Grandes Eventos

	GRAU DE MATURIDADE										
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Rio+20	83	83	14	28	10	30	0	0	8	40	181
Copa Conf	15	15	31	62	73	219	2	8	8	40	344
JO	8	8	0	0	44	132	76	304	14	70	514

Fonte: Autor

Figura 96 – Grau de Maturidade da aplicação das NIP nas Op Grandes Eventos



Fonte: Autor

Para se verificar o progresso ou não da aplicação das NIP, o parâmetro de maturidade foi consolidado por evento como o somatório das maturidades dos diversos graus estimados. O resultado pode ser observado na Tabela 55 e a Figura 95. Na Figura 95, vê-se claramente a progressão em verde da maturidade da aplicação das NIP, o que é condizente com o progresso observado da organização CDCiber e seu desdobramento operacional, o Destacamento de Defesa Cibernética.

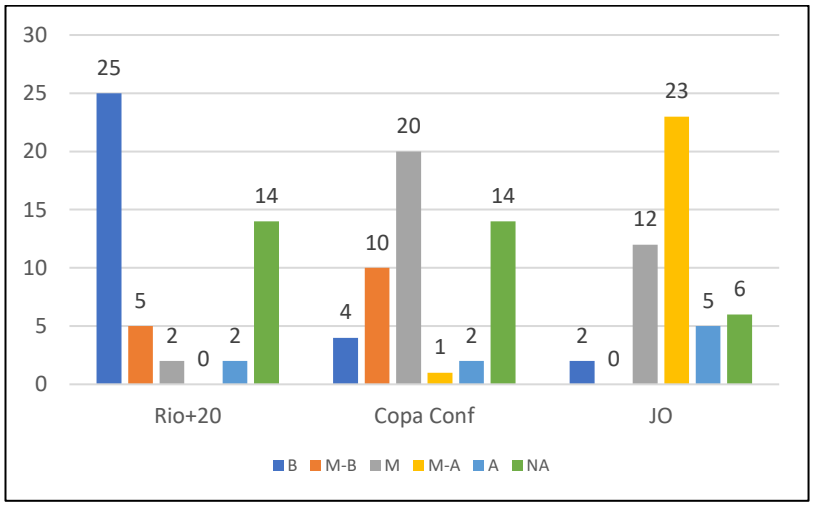
Para se observar como as constatações feitas até esse ponto tiveram evolução por estágio de CS, foram tabulados e representados os dados das Tabelas 56 a 6, com respectivos gráficos representados nas Figuras 96 a 104.

Tabela 55 - Quantitativo e % de aplicação de NIP por Maturidade de Percepção - Grandes Eventos

	MATURIDADE DE PERCEPÇÃO												
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**	**Total**
Rio+20	25	52,1%	5	10,4%	2	4,2%	0	0,0%	2	4,2%	14	29,2%	48
Copa Conf	4	7,8%	10	19,6%	20	39,2%	1	2,0%	2	3,9%	14	27,5%	51
JO	2	4,2%	0	0,0%	12	25,0%	23	47,9%	5	10,4%	6	12,5%	48

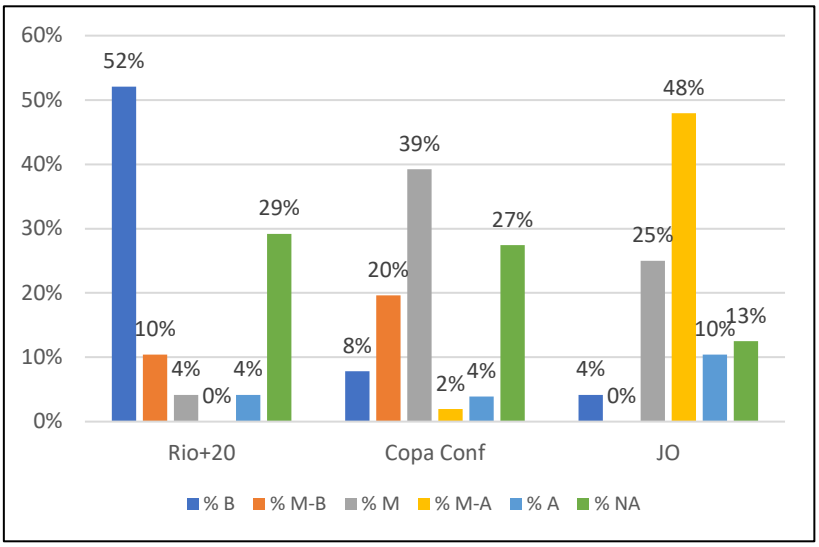
Fonte: Autor

Figura 97 – Quantitativo e % de aplicação de NIP por Maturidade de Percepção - Grandes Eventos



Fonte: Autor

Figura 98 – % de Quantitativo da aplicação das NIP por Maturidade de Percepção - Grandes Eventos



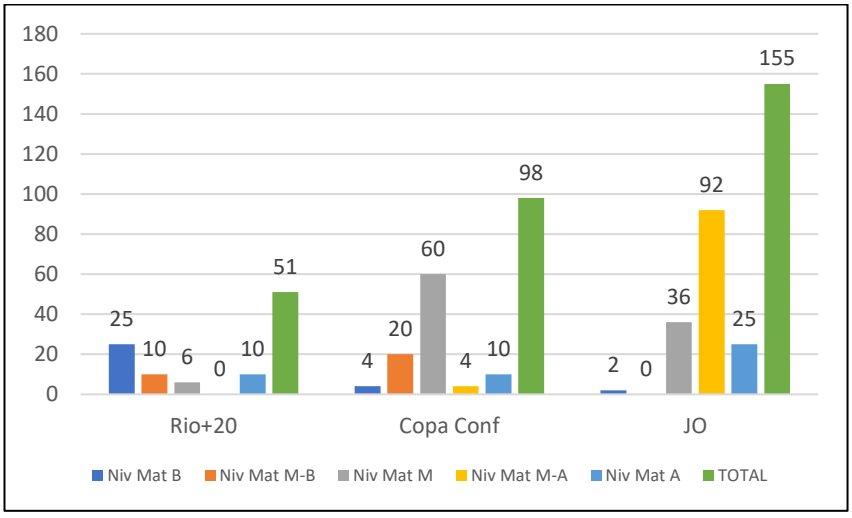
Fonte: Autor

Tabela 56 – Grau de Maturidade da aplicação das NIP de Percepção nas Op Grandes Eventos

GRAU DE MATURIDADE DE PERCEPÇÃO											
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Rio+20	25	25	5	10	2	6	0	0	2	10	51
Copa Conf	4	4	10	20	20	60	1	4	2	10	98
JO	2	2	0	0	12	36	23	92	5	25	155

Fonte: Autor

Figura 99 – Grau de Maturidade da aplicação das NIP de Percepção nas Op Grandes Eventos



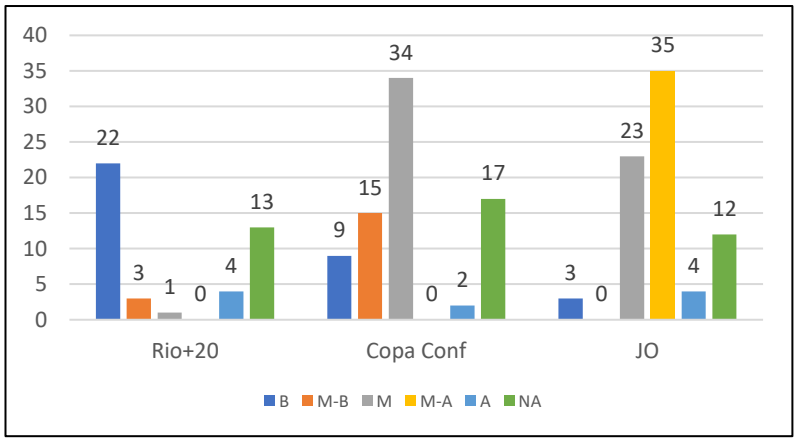
Fonte: Autor

Tabela 57 – Quantitativo e % de aplicação de NIP por Maturidade de Compreensão nas Op Grandes Eventos

MATURIDADE DE COMPREENSÃO												
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**
Rio+20	22	51,2%	3	7,0%	1	2,3%	0	0,0%	4	9,3%	13	30,2%
Copa Conf	9	11,7%	15	19,5%	34	44,2%	0	0,0%	2	2,6%	17	22,1%
JO	3	3,9%	0	0,0%	23	29,9%	35	45,5%	4	5,2%	12	15,6%

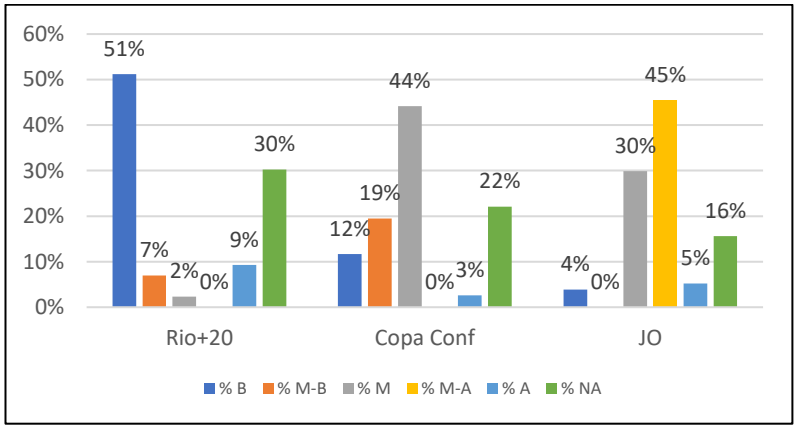
Fonte: Autor

Figura 100 – Quantitativo de aplicação de NIP por Maturidade de Compreensão - Grandes Eventos



Fonte: Autor

Figura 101 – % de aplicação de NIP por Maturidade de Compreensão nas Op Grandes Eventos



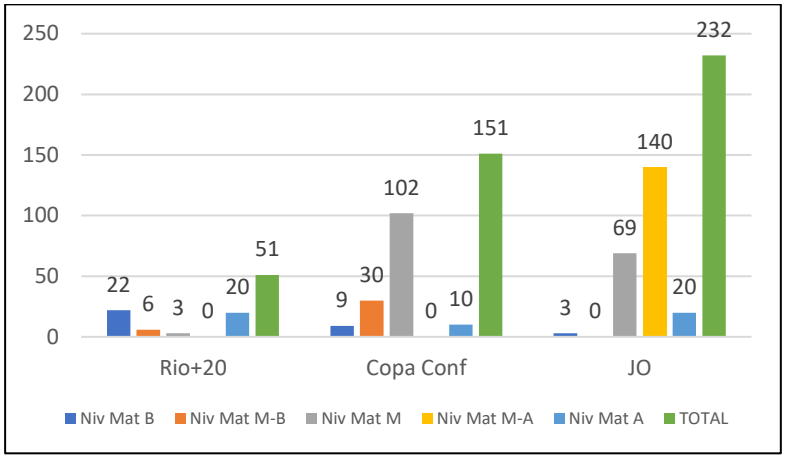
Fonte: Autor

Tabela 58 – Grau de Maturidade da aplicação das NIP de Compreensão nas Op Grandes Eventos

GRAU DE MATURIDADE DE COMPREENSÃO											
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Rio+20	22	22	3	6	1	3	0	0	4	20	51
Copa Conf	9	9	15	30	34	102	0	0	2	10	151
JO	3	3	0	0	23	69	35	140	4	20	232

Fonte: Autor

Figura 102 – Grau de Maturidade da aplicação das NIP de Compreensão nas Op Grandes Eventos



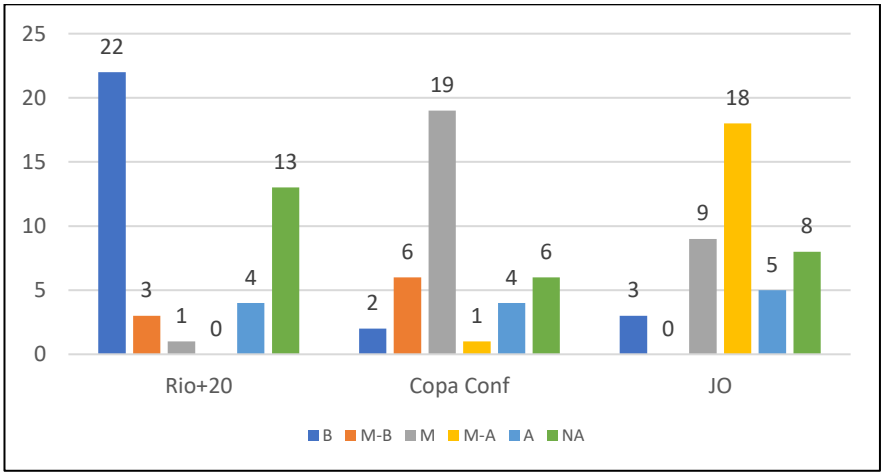
Fonte: Autor

Tabela 59 – Quantitativo e % de aplicação de NIP por Maturidade de Projeção - Grandes Eventos

	MATURIDADE DE PROJEÇÃO											
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**
Rio+20	22	51%	3	7%	1	2%	0	0%	4	9%	13	30%
Copa Conf	2	5%	6	16%	19	50%	1	3%	4	11%	6	16%
JO	3	7%	0	0%	9	21%	18	42%	5	12%	8	19%

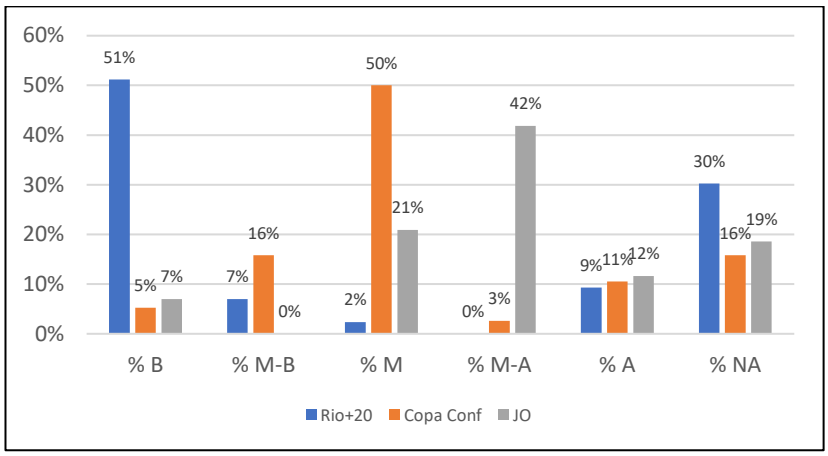
Fonte: Autor

Figura 103 – Quantitativo de aplicação de NIP por Maturidade de Projeção - Grandes Eventos



Fonte: Autor

Figura 104 – % de aplicação de NIP por Maturidade de Projeção - Grandes Eventos



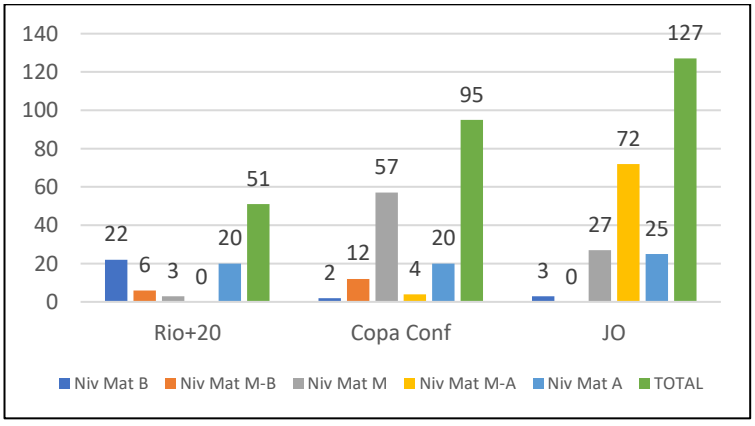
Fonte: Autor

Tabela 60 – Grau de Maturidade da aplicação das NIP de Projeção nas Op Grandes Eventos

GRAU DE MATURIDADE DE PROJEÇÃO											
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Rio+20	22	22	3	6	1	3	0	0	4	20	51
Copa Conf	2	2	6	12	19	57	1	4	4	20	95
JO	3	3	0	0	9	27	18	72	5	25	127

Fonte: Autor

Figura 105 – Grau de Maturidade da aplicação das NIP de Projeção nas Op Grandes Eventos



Fonte: Autor

As tabelas e gráficos de quantitativos de maturidade na aplicação de NIP por estágio de CS trouxeram resultados muito similares aos observados nos resultados gerais, tanto na distribuição dos valores por grande evento e por estágio de CS quanto nos valores de progresso global.

6.4.2. Operações de Adestramento do MD

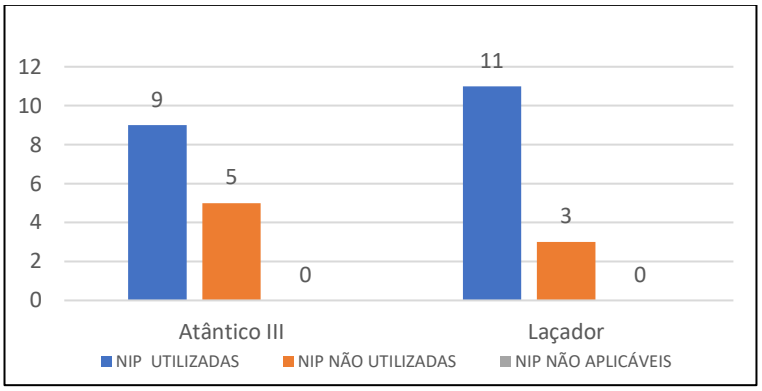
Analogamente à sequência seguida no registro das operações dos Grandes Eventos, este tópico aborda as operações Atlântico III 2012 e Laçador 2013, comparando-as por observação do que ocorre com a aplicação das NIP e sua maturidade. As Tabelas 62 e 63 as Figuras 105 a 108 mostram a aplicação das NIP utilizadas por operação, tanto no cômpito geral quanto por estágio da CS. São focadas as NIP de ataque e exploração cibernética, uma vez que essas operações são eminentemente de combate.

Tabela 61 – Resultados gerais da aplicação das NIP nas Operação do MD

OPERAÇÃO	NIP UTILIZADAS	INCREM. NIP UTIL.	NIP NÃO UTILIZADAS	NIP NÃO APLICÁVEIS	% Total	TOTAL
Atlântico III	9	0,0%	5	0	64,3%	14
Laçador	11	14,3%	3	0	78,6%	14
Total Acum.	-----	14,3%	-----	-----	-----	-----

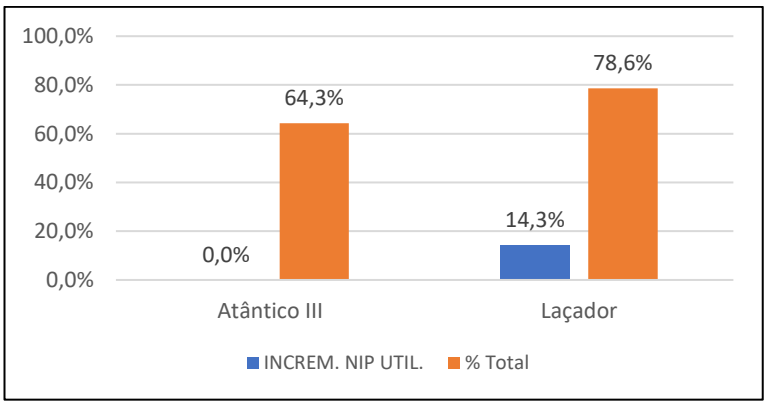
Fonte: Autor

Figura 106 – Operações do MD - Resultados Gerais



Fonte: Autor

Figura 107 – Operações do MD - Incrementos de NIP Utilizadas



Fonte: Autor

Da leitura da Tabela 62 e das Figuras 105 e 106, é possível constatar que a aplicação das NIP progrediu da operação Atlântico III 2012 para a operação Laçador 2013, sugerindo, como ocorreu no caso das operações dos Grandes Eventos, o incremento da capacidade de consciência situacional de defesa cibernética.

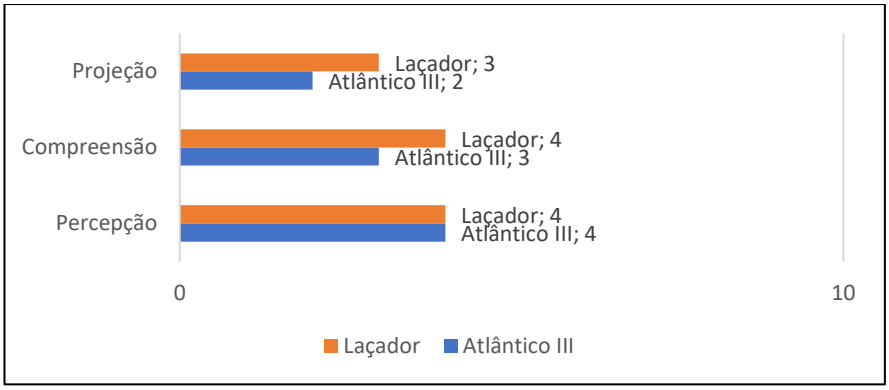
A Tabela 63 e as Figuras 107 e 108 estendem a verificação, considerando os estágios de consciência situacional.

Tabela 62 – NIP Utilizadas por estágio de CS para todas as Operações do MD

NIP UTILIZADAS							
Operação	**Percepção**	**Increm. Percepção**	**Compreensão**	**Increm. Compreensão**	**Projeção**	**Increm. Projeção**	**TOTAIS**
Atlântico III	4	0%	3	0%	2	0%	9
Laçador	4	0%	4	17%	3	33%	11
Total Acum.	-----	0%	-----	17%	-----	33%	-----

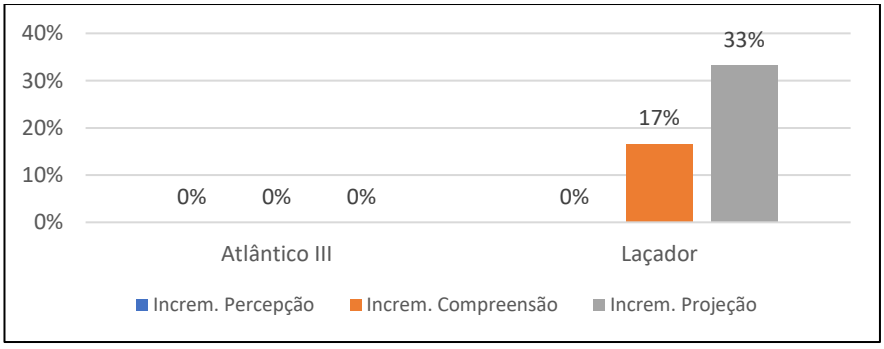
Fonte: Autor

Figura 108 – NIP Utilizadas por estágio de CS para todas as Operações do MD



Fonte: Autor

Figura 109 – Incremento de NIP na Operações do MD por estágio de CS



Fonte: Autor

Observando-se a Tabela 63 e as Figuras 107 e 108, vê-se que a aplicação das NIP, aumentou de uma operação para outra nos estágios de compreensão e projeção, permanecendo a mesma na percepção. Provavelmente, esses resultados estão associados, em primeiro lugar, tratando-se do estágio de percepção, ao fato de que as situações anômalas, nestas operações, serem “percebidas” por meio dos problemas militares simulados, padronizando, de uma certa forma, essa captação do problema.

À época dessas operações, foi proposta dentre as LA a elas relacionadas que se estabelecesse um time de técnicos real para fazer as vezes de equipe cibernética do país hostil do cenário fictício, além de as ações cibernéticas serem desenvolvidas em ambiente de TI real, porém específico e segregado para o exercício. Isso transformaria o processo de percepção. No entanto, por razões diversas, essas mudanças não foram implementadas no período estudado.

O incremento em relação às NIP de compreensão e projeção empregadas de um modo geral é coerente com o amadurecimento que ocorreu nas atividades do CDCiber, unidade da qual era desdobrado o Destacamento de Guerra Cibernética, unidade esta que, efetivamente, atuava nos exercícios operacionais. À época da operação Laçador, já havia ocorrido quatro operações de defesa cibernética, duas de grandes eventos e duas de treinamento militar, dentre elas a Atlântico III, e o aprendizado, em forma de lições aprendidas das operações, capacitações diversas e o incremento tecnológico e de pessoal especializado permitiu aventar mais e melhores itens de planejamento e preparação para a operação.

Cabe ressaltar que a verificação de uso das NIP reflete a preparação prévia para a operação e o amadurecimento dos conceitos e práticas envolvidos na atividade por parte do pessoal envolvido.

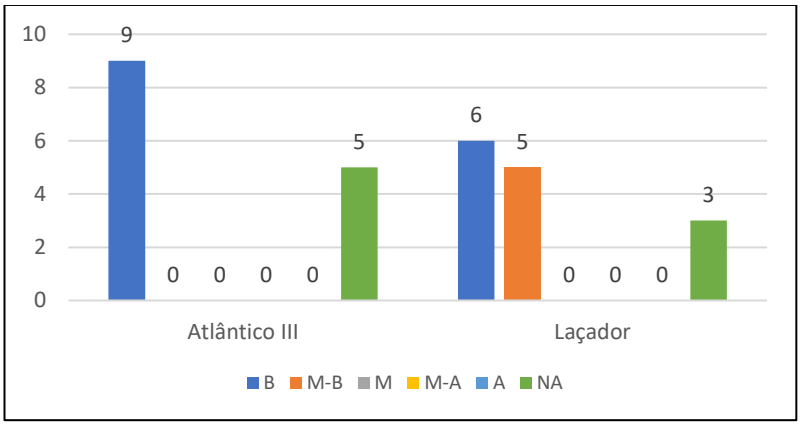
A seguir, analogamente ao procedimento seguido para as operações de grandes eventos, são apresentados a série de tabelas e gráficos correspondentes a avaliação de maturidade, após os quais, são tecidos os comentários que discutem os pontos de relevância.

Tabela 63 – Quantitativo e % da aplicação das NIP por Maturidade nas Op do MD

	MATURIDADE												
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**	**Total**
Atlântico III	9	64,3%	0	0,0%	0	0,0%	0	0,0%	0	0,0%	5	35,7%	14
Laçador	6	42,9%	5	35,7%	0	0,0%	0	0,0%	0	0,0%	3	21,4%	14

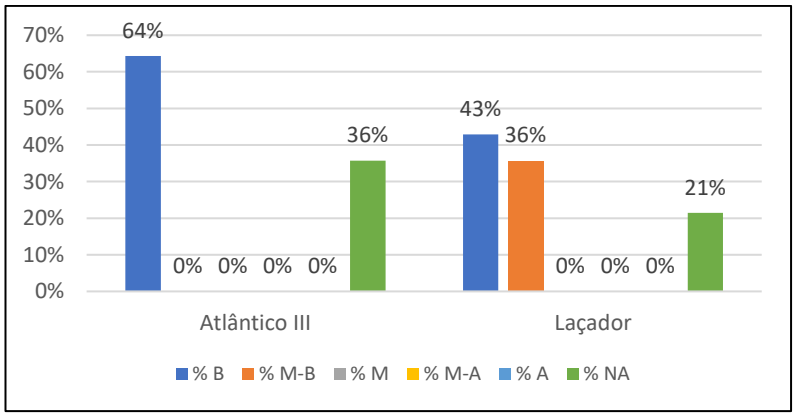
Fonte: Autor

Figura 110 – Quantitativo da aplicação das NIP por Maturidade nas Op do MD



Fonte: Autor

Figura 111 – % da aplicação das NIP por Maturidade nas Op do MD



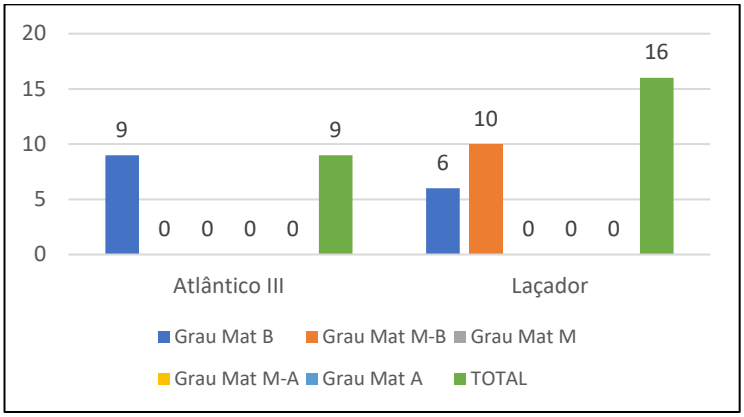
Fonte: Autor

Tabela 64 – Grau de Maturidade da aplicação das NIP nas Op do MD

	GRAU DE MATURIDADE										
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Atlântico III	9	9	0	0	0	0	0	0	0	0	9
Laçador	6	6	5	10	0	0	0	0	0	0	16

Fonte: Autor

Figura 112 – Grau de Maturidade da aplicação das NIP nas Op do MD



Fonte: Autor

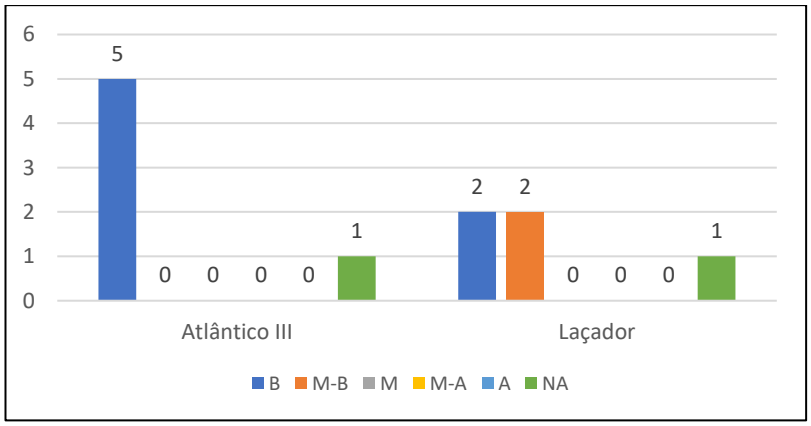
Analogamente ao ocorrido nas operações do Grande Eventos, as Tabelas 64 e 65 e gráficos das Figuras 110 e 111 revelam uma incipiência clara na Operação Atlântico e um progresso significativo na operação Laçador. No entanto, observou-se também um valor significativo de NIP não aplicadas, aproximadamente 36%, o que reforça constatação de que, apesar dos progressos de uma operação para outra, havia, à época das observações, uma maturidade menor nos aspectos das ações de exploração e ataque do que nas de proteção cibernética.

Tabela 65 – Quantitativo e % da aplicação das NIP por Maturidade de Percepção nas Op do MD

	MATURIDADE DE PERCEPÇÃO												
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**	**Total**
Atlântico III	5	83,3%	0	0,0%	0	0,0%	0	0,0%	0	0,0%	1	16,7%	6
Laçador	2	40,0%	2	40,0%	0	0,0%	0	0,0%	0	0,0%	1	20,0%	5

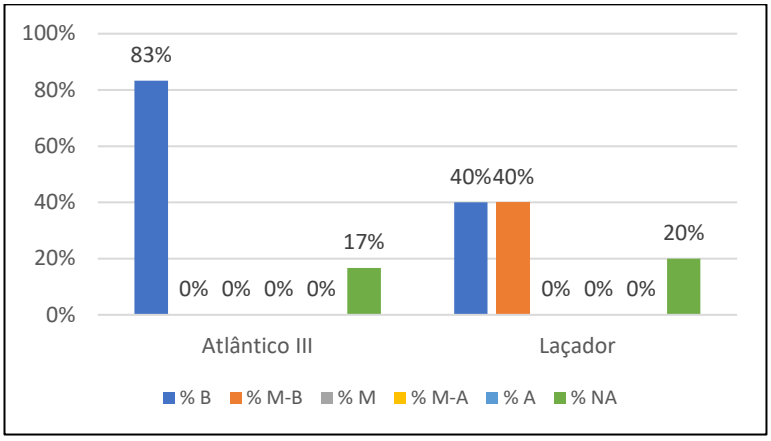
Fonte: Autor

Figura 113 – Quantitativo da aplicação das NIP por Maturidade de Percepção nas Op do MD



Fonte: Autor

Figura 114 – % de aplicação das NIP por Maturidade de Percepção nas Op do MD



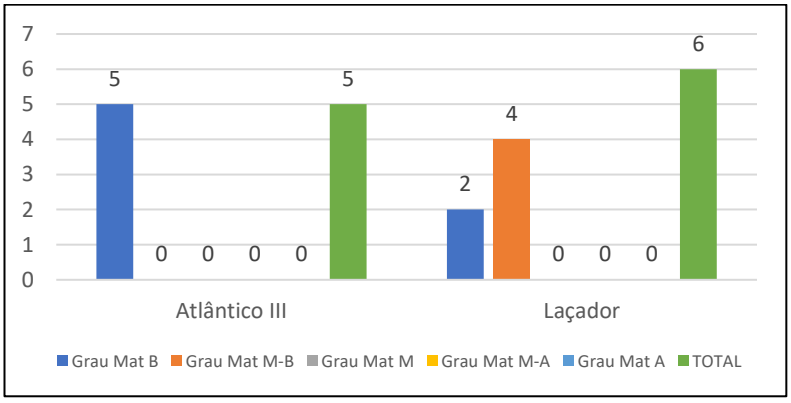
Fonte: Autor

Tabela 66 – Grau de Maturidade da aplicação das NIP de Percepção nas Op Grandes Eventos

GRAU DE MATURIDADE DE PERCEPÇÃO											
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Atlântico III	5	5	0	0	0	0	0	0	0	0	5
Laçador	2	2	2	4	0	0	0	0	0	0	6

Fonte: Autor

Figura 115 – Grau de Maturidade da aplicação das NIP de Percepção nas Op MD



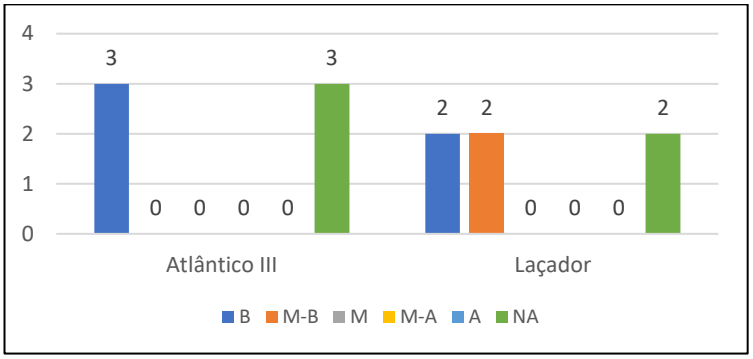
Fonte: Autor

Tabela 67 – Quantitativo e % de aplicação das NIP por Maturidade de Compreensão nas Op MD

MATURIDADE DE COMPREENSÃO												
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**
Atlântico III	3	50,0%	0	0,0%	0	0,0%	0	0,0%	0	0,0%	3	50,0%
Laçador	2	33,3%	2	33,3%	0	0,0%	0	0,0%	0	0,0%	2	33,3%

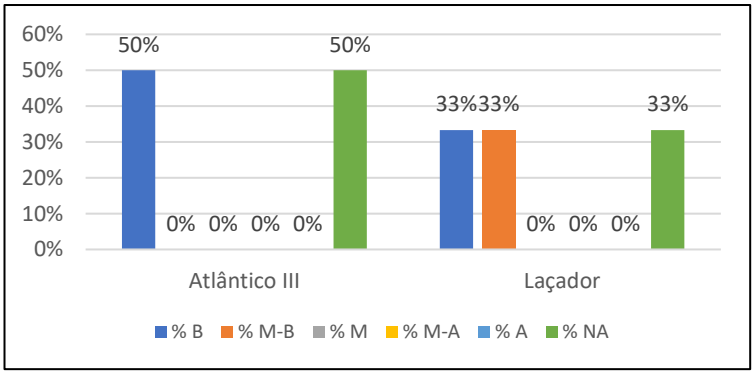
Fonte: Autor

Figura 116 – Quantitativo de aplicação das NIP por Maturidade de Compreensão nas Op MD



Fonte: Autor

Figura 117 – % de aplicação das NIP por Maturidade de Compreensão nas Op MD



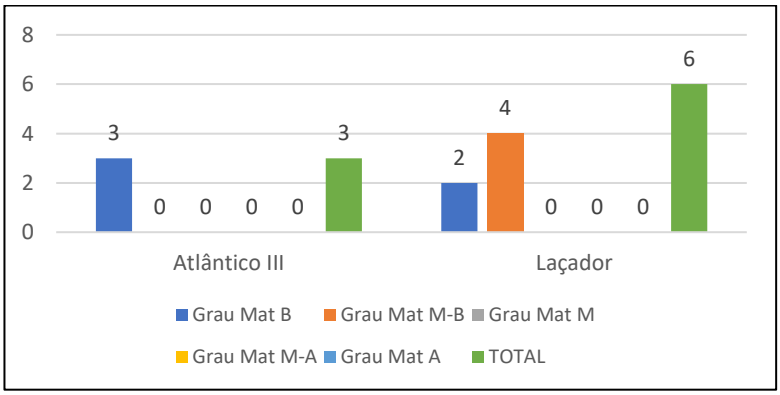
Fonte: Autor

Tabela 68 – Grau de Maturidade da aplicação das NIP de Compreensão nas Op MD

	GRAU DE MATURIDADE DE COMPREENSÃO										
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Atlântico III	3	3	0	0	0	0	0	0	0	0	3
Laçador	2	2	2	4	0	0	0	0	0	0	6

Fonte: Autor

Figura 118 – Grau de Maturidade da aplicação das NIP de Compreensão nas Op MD



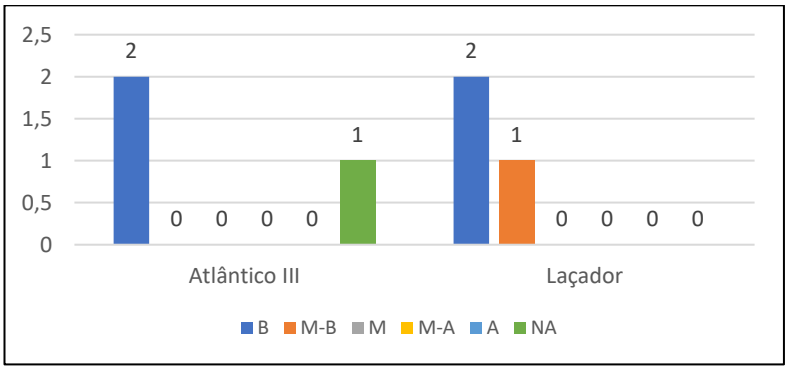
Fonte: Autor

Tabela 69 – Quantitativo de aplicação das NIP por Maturidade de Projeção nas Op MD

	MATURIDADE DE PROJEÇÃO											
Operação	**B**	**% B**	**M-B**	**% M-B**	**M**	**% M**	**M-A**	**% M-A**	**A**	**% A**	**NA**	**% NA**
Atlântico III	2	66,7%	0	0,0%	0	0,0%	0	0,0%	0	0,0%	1	33,3%
Laçador	2	66,7%	1	33,3%	0	0,0%	0	0,0%	0	0,0%	0	0,0%

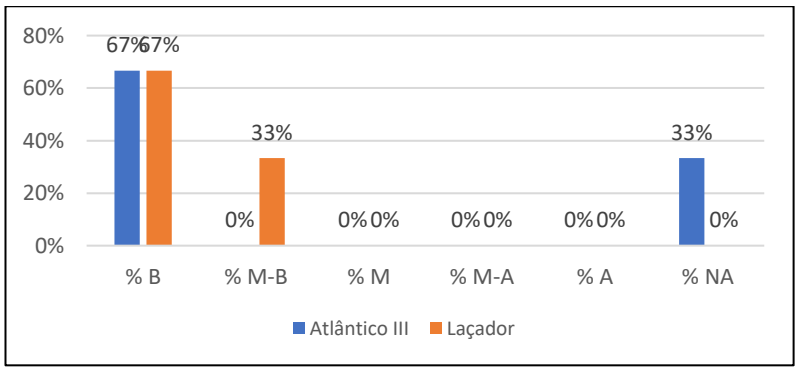
Fonte: Autor

Figura 119 – Quantitativo de aplicação das NIP por Maturidade de Projeção nas Op MD



Fonte: Autor

Figura 120 – % de aplicação das NIP por Maturidade de Projeção nas Op MD



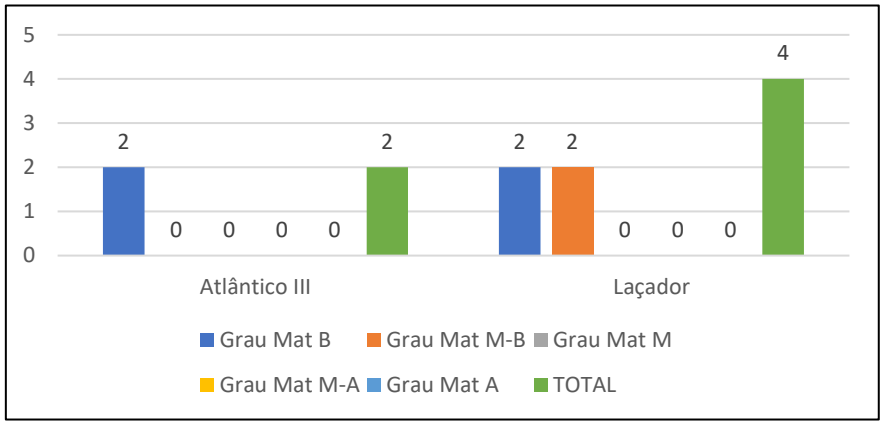
Fonte: Autor

Tabela 70 - Grau de Maturidade da aplicação das NIP de Projeção nas Op MD

	GRAU DE MATURIDADE DE PROJEÇÃO										
Operação	**B**	**Grau Mat B**	**M-B**	**Grau Mat M-B**	**M**	**Grau Mat M**	**M-A**	**Grau Mat M-A**	**A**	**Grau Mat A**	**TOTAL**
Atlântico III	2	2	0	0	0	0	0	0	0	0	2
Laçador	2	2	1	2	0	0	0	0	0	0	4

Fonte: Autor

Figura 121 - Grau de Maturidade da aplicação das NIP de Projeção nas Op MD



Fonte: Autor

O exame da aplicação das NIP por estágio de CS corroborou as constatações de caráter geral, destacando-se apenas que foi observado nenhuma aplicação de NIP de maturidade média ou superior. A razão dessa ausência encontra-se no fato de que o CDCiber, quando da coleta dos dados da pesquisa, além de recém-criado, estava majoritariamente voltado para coordenar a defesa cibernética dos Grandes Eventos ocorridos de 2012 a 2016, que eram operações de proteção cibernética, o que impactou muito o seu desenvolvimento em exploração e ataque cibernéticos nos primeiros anos de sua existência, o que ficou corroborado pelo estudo.

6.5. OBJETIVO ESPECÍFICO (e)

As discussões a respeito do objetivo específico (e) foram concentradas na tarefa (e.3), como mencionado no subtítulo 5.5 do capítulo 5, quando do relato dos resultados referentes ao objetivo específico (e). Com a realização da tarefa (e.3), procurou-se realizar qualitativamente uma análise comparativa entre os resultados da aplicação das NIP sobre a documentação das operações estudadas (objetivo (d)) e os resultados da análise dos registros de tratamento das anomalias captadas no espaço cibernético pelo Dst de Defesa Cibernética que atou na operação.

Em outras palavras, essa análise buscou averiguar que relação era possível perceber entre as expectativas geradas pelo efeito da aplicação das NIP-CS-DC na consciência situacional dos comandantes das operações estudadas e as reações

reais de consciência situacional ocorridas por esses comandantes resultante do tratamento dado aos eventos anômalos que ocorreram durante as operações.

Essa análise foi desenvolvida de modo indireto, pois, além de a CS ser um processo eminentemente subjetivo a cada ser humano que a realiza, o trabalho de defesa cibernética depende uma miríade de componentes instrumentais, processuais e de atividade humana efetuados em múltiplos níveis, desde a monitoração dos impulsos elétricos que transitam nas redes computacionais, abstraídos matematicamente em *bits* e *bytes*, até a relação homem-máquina em que o ser humano interage com mostradores do estado de segurança dos ativos de informação a serem protegidos ou combatidos, conforme a situação de emprego da defesa cibernética.

Logo, como solução para essa abordagem indireta, três fatores foram utilizados. O primeiro, em relação à aplicação das NIP, foi a viabilização de um modo de medir a sua utilização e, portanto, ainda que de modo indireto, estimar o seu provável aproveitamento para formação da consciência situacional dos envolvidos na cadeia de decisões até o comandante de uma operação. Dois parâmetros foram usados: o número de NIP utilizadas e a maturidade estimada na sua utilização. Este último parâmetro se demonstrou de importância central para esta última tarefa da pesquisa, sendo a forma de sua contabilização e interpretação expostos no subtítulo 5.4.2.3.

O segundo fator esteve relacionado à estimativa de quão maduros foram os posicionamentos advindos da tomada de consciência situacional de defesa cibernética nos eventos reais com os quais a equipe dos Destacamentos, em particular o seu comandante, tiveram de lidar. Para realizar essa estimativa, em tese, seria necessário analisar um a um os eventos anômalos ocorridos, identificar qual o processo específico foi escolhido para o seu tratamento e os relacionar, cada um, aos estágios da CS. Esse processo seria excessivamente complexo, além de haver a necessidade de documentar na pesquisa eventos reais considerados sigilosos, o que poderia restringir o acesso aos resultados e métodos do trabalho.

A análise dos registros de eventos anômalos ocorridos nas operações revelou como essa dificuldade poderia ser contornada. Conforme resolução da tarefa (e.2) mostrou, constatou-se que todos os eventos de segurança podiam ser enquadrados em três categorias principais, havendo, para todas, métodos de tratamentos bem

definidos (gestão de riscos, tratamento de incidentes de segurança computacional e ciclo de Inteligência), os quais podem ser relacionados aos estágios da CS com relativa simplicidade. Esses métodos se repetiam em todos as operações, sendo diferenciados apenas pela maturidade de sua aplicação. Novamente o parâmetro de maturidade se mostrou capital para a análise, restando resolver como essa estimativa poderia ser minimamente confiável, que leva ao terceiro fator que definiu a abordagem para resolver a tarefa (e.3).

O terceiro fator foi o fato de o pesquisador, autor desta tese, ter sido protagonista em todos os eventos estudados, sendo comandante de destacamento nas operações Atlântico III, Copa das Confederações 2013 e Jogos Olímpicos 2016, e exercendo funções assessoramento direto aos comandantes nas operações Laçador e Rio+20, tendo referências diretas do exercício da consciência situacional de defesa cibernética.

Além disso, o autor exerceu diversos cargos de chefia ligadas as operações do CDCiber, dentre eles o cargo de chefe da seção de doutrina do CDCiber, a quem coube coordenar a compilação das LA das operações e aplicação de *frameworks* de segurança e defesa cibernética, o que vai ao encontro da vivência, ainda que não de forma metódica e explicitamente reconhecida na instituição, da aplicação do ciclo de gestão do conhecimento organizacional como alicerce e pavimento das condições de uma tomada de consciência situacional com chances significativas de ter direcionamento adequado. Assim, com tais vivências e conhecimentos, o exercício da observação participante por parte do autor da pesquisa tende a permitir a formulação de juízos de valores razoáveis para a estimar graus para o parâmetro de maturidade.

Isso posto, procedeu-se o desenvolvimento da tarefa de discussão (e.3), o que foi segmentado em três fases. Na primeira, foi realizada a compactação das informações dos Quadros 10 e 11, relativos à resolução da tarefa (e.2), nas Tabelas 73, 74, 75, 78 e 79, discriminadas por operação, acrescentando-se as estimativas de maturidade e respectivos valores numéricos, conforme a mesma escala utilizada nos mapeamentos de maturidade do objetivo (d), assim como os valores totais de *schematas* e de maturidade, sendo este discriminado por evento anômalo e obtido por soma dos valores intermediários estimados por estágio de CS.

A segunda fase consistiu em uma nova compactação, agora, dos valores totais de maturidade e *schematas*, distribuídos por categoria de evento anômalo, e compilados em um valor geral obtido por soma simples. Essas informações estão nas Tabelas 76 e 77 e Figuras 120 e 121 para os Grandes Eventos e Tabelas 80 e 81 b e Figuras 122 e 123 para as operações do MD.

A terceira fase foi a análise comparativa propriamente dita entre os resultados do objetivo (d), mais especificamente a tarefa (d.2) e as informações geradas nas duas primeiras fases supras explanadas da tarefa (e.3). Essas análises estão registradas nos subtítulos 6.5.2 e 6.5.4.

Para realizar a análise comparativa dos resultados dos objetivos específicos (d) e (e), deve-se partir de uma base de comparação que precisa estar bem estabelecida e caracterizada. Nesse sentido três premissas precisaram ser estipuladas de modo a referenciar a análise.

O resultado da aplicação das NIP para potencializar a tomada de consciência situacional gera uma expectativa de um exercício dessa CS em nível de maturidade superior ao de experiências similares anteriores. Essa expectativa se baseia no fato de que as NIP, por definição, constituem um comportamento informacional cuja realização se dá nos estágios iniciais dos ciclos de gestão da informação e do conhecimento, direcionando as ações decorrentes dos demais estágios.

Ao se verificar a aplicação das NIP-CS-DC em situações passadas, mediante mecanismos metodológicos bem estabelecidos, tal qual se buscou estruturar nesta pesquisa, o resultado alcançado revela, de forma indireta e de modo lógico dedutivo, tendências da evolução do exercício da consciência situacional na linha do tempo. Assim, a primeira premissa da análise comparativa realizada nesta tarefa (e.3) da pesquisa é:

1) A aplicação das NIP revela tendências de evolução no exercício da consciência situacional de defesa cibernética.

Nos primeiros passos da tarefa (e.2), foi buscado um modo de verificar de forma mais próxima possível do que seria uma a verificação direta a progressão da consciência situacional no decorrer da realização das operações de defesa cibernética estudas. A forma encontrada foi a de lançar mão do testemunho do pesquisador e participante dos eventos em termos de estimativa de maturidade do

exercício da consciência situacional nas operações sob análise. Tomou-se o cuidado de tomar esse testemunho de modo sistematizado, lançando-se mão do modelo de Barford (2010, p. 3-5), e em consonância com os processos reais ocorridos e que fundamentaram a tomada de consciência situacional em todas as categorias de eventos anômalos observados. Assim a segunda premissa para a análise comparativa realizada nesta tarefa (e.3):

2) A estimativa da maturidade do exercício da consciência situacional nas operações estudadas, por meio do testemunho do pesquisador participante a respeito da qualidade dos processos usados para tratar os eventos anômalos, revela tendências da sua evolução nos eventos estudados.

Outro fato importante a destacar neste preâmbulo para a comparação efetuada é que a aplicação das NIP pressupõe, ainda que não de forma sistemática e metodológica, algum grau de desenvolvimento de conhecimento organizacional para que seu sucesso seja significativo e não apenas fortuito, o que converge com a estruturação desta pesquisa de doutorado que, para propor o *framework* de NIP-CS-DC, o fez derivar de um *framework* anterior para aprendizado organizacional resultante da adaptação de *frameworks* originais de segurança e defesa cibernética escolhidos para a pesquisa. Logo, se, por definição, as NIP são as origens do ciclo de conhecimento organizacional, os resultados desse ciclo, produtos informacionais com valor agregado e conhecimentos, devem ser adequadamente consumidos no comportamento informacional de uso da informação, que no caso desta pesquisa é o próprio exercício da consciência situacional. Assim, uma terceira premissa é estabelecida:

3) A realização do efeito desejado na aplicação das NIP-CS-DC depende do amadurecimento do conhecimento organizacional em defesa cibernética de modo que seja viabilizado o exercício de consciência situacional de DC.

Por fim, considerando o uso de *schematas* como elemento potencializador da consciência situacional, em termos teoria adotada para defesa cibernética, a verificação contida na tarefa (e.3) também destacou esse elemento para fins de verificação se existe algum indício de relação entre a evolução de sua utilização e o a evolução do exercício da CS.

6.5.1. Estimativas de Maturidade para as Operações dos Grandes Eventos

Neste tópico são apresentadas as estimativas de maturidade para os Grandes Eventos cobertos pela pesquisa e a contabilização da quantidade de *schematas* utilizados. Nas tabelas 73, 74 e 75, as designações Pe1, Pe2, Co1, Co2, Co3, Pr1 e Pr2 representam os sete aspectos do modelo de Barford (2010, p.3-5), adaptados para questionamentos, conforme referencial teórico e apresentados no Quadro 2, correspondendo aos estágios de CS perceber (Pe), compreender (Co) e projetar (Pr).

Tabela 71 – Estimativa de Maturidade e *Schematas* na Op Rio+20

Categorias de Eventos Anômalos	PE1	PE2	Matur. de Perceção	Vlr Mat Pe	CO1	CO2	CO3	Matur. de Compreensão	Vlr Mat Co	PR1	PR2	Matur. de Projeção	Vlr Mat Pr	Total Mat	Total *Schemata*
Riscos de Ativos	1	1	M-B	2	1	NA	1	M-B	2	1	1	B	2	6	6
Eventos de segurança	3	1	B	1	1	1	2	M-B	2	2	1	B	2	5	11
Canal de Inteligência	3	1	M	3	1	1	1	M	3	3	NA	M	3	9	10

Fonte: Autor

Tabela 72 – Estimativa de Maturidade e *Schematas* na Op Copa das Confederações 2013

Categorias de Eventos Anômalos	PE1	PE2	Matur. de Perceção	Vlr Mat Pe	CO1	CO2	CO3	Matur. de Compreensão	Vlr Mat Co	PR1	PR2	Matur. de Projeção	Vlr Mat Pr	Total Mat	Total *Schemata*
Riscos de Ativos	1	1	M	3	1	NA	1	M	3	1	1	M	3	9	6
Eventos de segurança	3	1	M	3	2	1	2	M	3	2	1	M	3	9	12
Canal de Inteligência	3	1	M-A	4	1	1	1	M-A	4	3	NA	M-A	4	12	10

Fonte: Autor

Tabela 73 – Estimativa de Maturidade e *Schematas* na Op dos JO

Categorias de Eventos Anômalos	PE1	PE2	Matur. de Perceção	Vlr Mat Pe	CO1	CO2	CO3	Matur. de Compreensão	Vlr Mat Co	PR1	PR2	Matur. de Projeção	Vlr Mat Pr	Total Mat	Total *Schemata*
Riscos de Ativos	1	1	M-A	4	3	NA	1	M-A	4	1	1	M-A	4	12	8
Eventos de segurança	3	1	M-A	4	2	2	2	M-A	4	3	1	M	3	11	14
Canal de Inteligência	3	1	M-A	4	1	1	1	M-A	4	3	NA	M-A	4	12	10

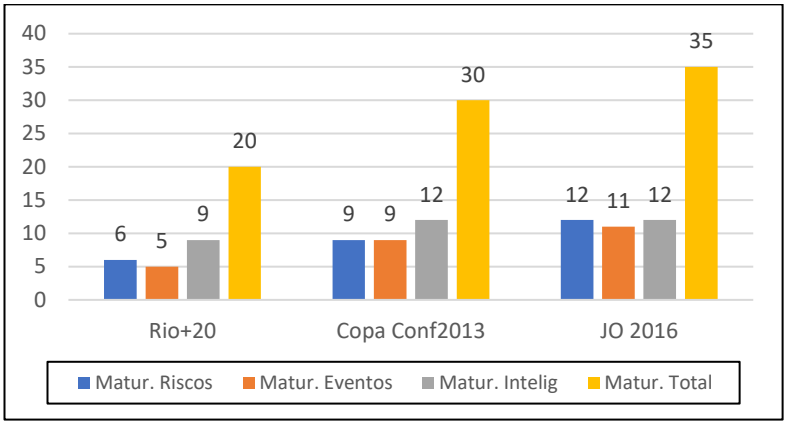
Fonte: Autor

Tabela 74 – Estimativa de Maturidade por Operação de Grandes Eventos

Operação	Matur. Riscos	Matur. Eventos	Matur. Intelig	Matur. Total
Rio+20	**6**	**5**	**9**	**20**
Copa Conf2013	9	**9**	**12**	**30**
JO 2016	12	**11**	**12**	**35**

Fonte: Autor

Figura 122 – Estimativa de Maturidade por Operação de Grandes Eventos



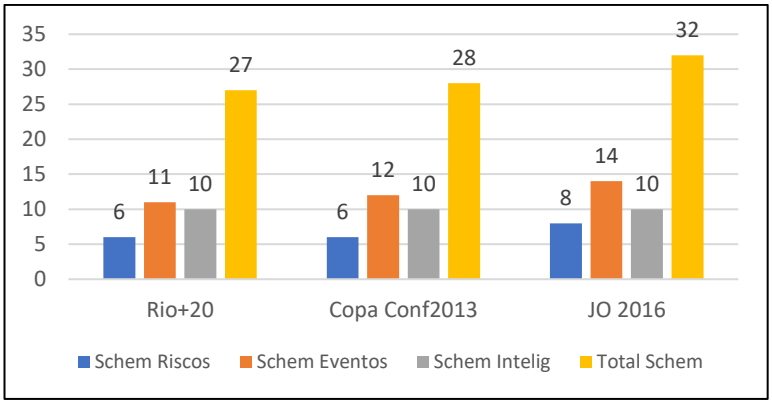
Fonte: Autor

Tabela 75 – Quantitativo de Schematas por Operação de Grandes Eventos

Operação	Schem Riscos	Schem Eventos	Schem Intelig	Total Schem
Rio+20	6	11	10	27
Copa Conf2013	6	12	10	28
JO 2016	8	14	10	32

Fonte: Autor

Figura 123 – Quantitativo de *Schematas* por Operação de Grandes Eventos



Fonte: Autor

6.5.2. Comparação entre resultados das tarefas (d.2) e (e.3) – Grandes Eventos

A análise comparativa entre os resultados da aplicação das NIP e a averiguação pelo modelo Barford (2010, p. 3-5) deve ter por base as tabelas 55 e 76 e Figuras 95 e 120. Da Figura 95, vê-se que os valores globais de maturidade de aplicação de NIP chegam a duplicar da Rio +20 para a Copa das Confederações e

têm um incremento de pouco mais de 60% desta para os Jogos Olímpicos. Já na Figura 120, vê-se um incremento de 50% entre as duas primeiras operações e de aproximadamente 17% da segunda para a terceira.

Cabe lembrar que a comparação aqui não busca proximidades numéricas, seja de valores absolutos ou proporcionais. O que se busca verificar nessas comparações é se há coerências entre as tendências das duas estimativas de maturidade. Essa escolha de procedimento advém do fato de se estar estimando a aplicação de objetos diferentes. No primeiro caso, a aplicação das NIP; no segundo, a aplicação dos processos de gestão de riscos, gestão de incidentes e canal de Inteligência. No entanto, ambos os objetos têm como ponto comum a contribuição para o exercício da consciência situacional de defesa cibernética. Daí a escolha de examinar a tendência e não a proporcionalidade numérica. No caso específico dos Grandes Eventos, observa-se uma coerência de tendências entre os resultados, sugerindo a pertinência do *framework* proposto na pesquisa. Um fator adicional que sugere a coerência dos resultados é o aumento, ainda que modesto, de *schematas* usados de uma operação para outra, conforme Figura 121.

6.5.3. Estimativas de Maturidade para as Operações do MD

Neste tópico são apresentadas as estimativas de maturidade para as operações de adestramento militar cobertas pela pesquisa e a contabilização da quantidade de *schematas* utilizados.

Tabela 76 – Estimativa de Maturidade e *Schematas* na Op Atlântico III

Categorias de Eventos Anômalos	PE1	PE2	Matur. de Perceção	Vlr Mat Pe	CO1	CO2	CO3	Matur. de Compreensão	Vlr Mat Co	PR1	PR2	Matur. de Projeção	Vlr Mat Pr	Total Mat	Total Schcemata
Riscos de Ativos	1	NA	M	3	NA	NA	NA	NA	0	NA	NA	NA	0	3	1
Eventos de segurança	1	2	M	3	3	3	3	M	3	3	3	M	3	9	18
Canal de Inteligência	1	2	M	3	3	3	3	M	3	3	3	M	3	9	15

Fonte: Autor

Tabela 77 – Estimativa de Maturidade e *Schematas* na Op Laçador

Categorias de Eventos Anômalos	PE1	PE2	Matur. de Perceção	Vlr Mat Pe	CO1	CO2	CO3	Matur. de Compreensão	Vlr Mat Co	PR1	PR2	Matur. de Projeção	Vlr Mat Pr	Total Mat	Total Schcemata
Riscos de Ativos	1	NA	M	3	1	NA	1	B	2	NA	NA	NA	0	5	3
Eventos de segurança	1	2	M-B	2	2	2	2	M-B	2	2	2	M-B	2	6	13
Canal de Inteligência	1	2	M	3	2	2	2	M-B	2	2	2	M-B	2	7	11

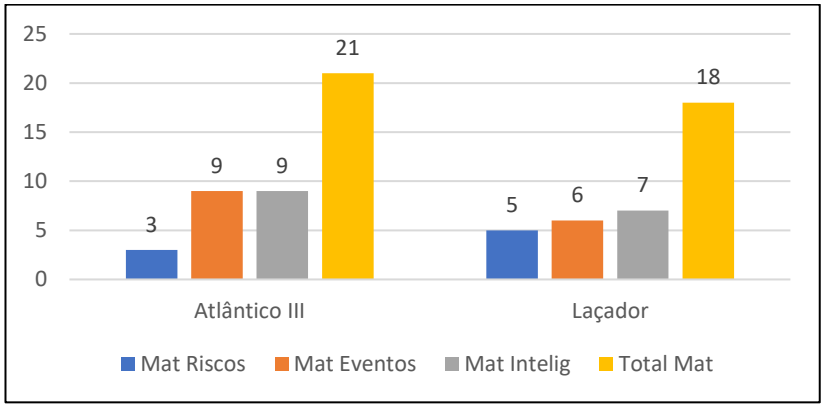
Fonte: Autor

Tabela 78 – Estimativa de Maturidade por Operação do MD

Operação	Mat Riscos	Mat Eventos	Mat Intelig	Total Mat
Atlântico III	3	9	9	21
Laçador	5	6	7	18

Fonte: Autor

Figura 124 – Estimativa de Maturidade por Operação do MD



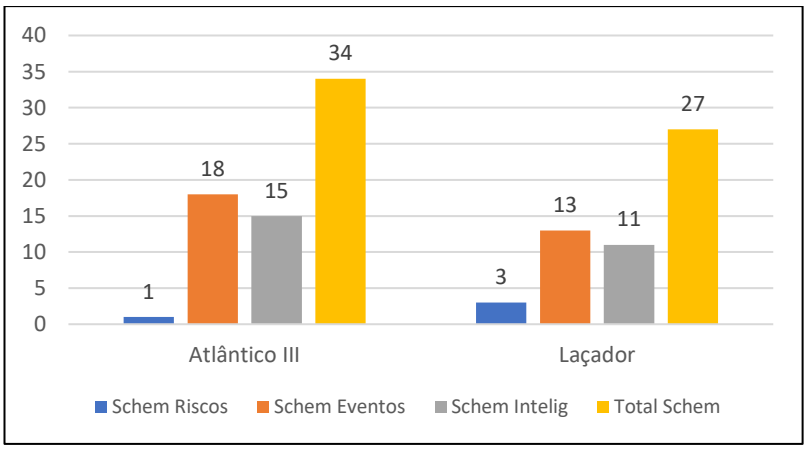
Fonte: Autor

Tabela 79 – Quantitativo de *Schemata* por Operação do MD

Operação	Schem Riscos	Schem Eventos	Schem Intelig	Total Schem
Atlântico III	**1**	**18**	**15**	**34**
Laçador	**3**	**13**	**11**	**27**

Fonte: Autor

Figura 125 – Quantitativo de *Schemata* por Operação do MD



Fonte: Autor

6.5.4. Comparação entre resultados das tarefas (d.2) e (e.3) – Operações do MD

Tal qual desenvolvido para os Grandes Eventos, apresenta-se neste ponto a análise comparativa entre as operações do MD Atlântico III e Laçador 2013. Para

esse fim, foram estudadas as Tabelas 65 e 80 e as Figuras 111 e 122. Neste caso, da Figura 111, constata-se um incremento da maturidade na aplicação das NIP de quase 80%. No entanto, da Figura 122, contata-se uma retração de aproximadamente 21% uma operação para outra. Refeitas as estimativas e cálculos, constatou-se que não houve erros de aplicação do método, logo, a explicação deveria pertencer a algum fator externo ao recorte ou condicionantes da pesquisa.

Assim, procedeu-se o reestudo das operações, constatando-se que a equipe formou o Dst que atuou na operação Laçador era menor e bem menos experiente do que a equipe da operação Atlântico. O chefe da equipe era um oficial de destaque no Centro de Defesa Cibernética, mas fora transferido para o CDCiber no ano anterior à operação e não tinha histórico prévio de trabalho no âmbito da defesa cibernética. Dos seus três membros de equipe, dois eram profissionais de tecnologia da informação, mas sem experiência de defesa cibernética e o último era um militar de Inteligência com experiência das operações anteriores, porém mais restrito aos níveis operacional e tático. Em contraste, a equipe da operação Atlântico III contava com um comandante e dois de seus oficiais com experiência de operações e anos de exercício de segurança e defesa cibernética, além de dois outros membros poucos experientes.

Relembrando a terceira premissa estabelecida para realizar essa análise, ou seja, “A realização do efeito desejado na aplicação das NIP para CS em DC depende do amadurecimento do conhecimento organizacional em defesa cibernética de modo que seja viabilizada o exercício de consciência situacional de DC”, é pertinente supor que a inexperiência da equipe do Destacamento de Guerra Cibernética da operação Laçador tenha se refletido na maturidade apresentadas na Figura 122.

Em suma, é pertinente afirmar que a retração de maturidade constatada na Tabela 80 e Figura 122, na operação Laçador, ainda que não coerente com a constatação de aumento de maturidade observada na aplicação das NIP, conforme Tabela 65 e Figura 111, não refuta a pertinência do framework de consciência situacional de defesa cibernética, mas sim o reforça, pois a aplicação das NIP são prévias à operação e sua prosperidade depende de pessoal com conhecimento sedimentado compatível com as NIP para usar a informações.

6.5.5. Síntese do Resultado da Pesquisa

Neste tópico, é apresentado o modelo final a que se chegou na pesquisa, ou seja, o *Framework* de Necessidades Informacionais Primordiais para Consciência Situacional de Defesa Cibernética. Essa informação já fora apresentada nos Quadros 9 e 10, no Capítulo 5, por meio do realce das colunas com fonte em vermelho, mas sem o destaque próprio que é necessário. Logo, o *Framework* de NIP-CS-DC está disposto de forma específica nos Quadros 13 e 14, assim como as Figuras 124 e 125 representam, respectivamente, a sequência de produção e a organização das categorias das NIP.

Primeiramente, na Figura 124, é apresentada a sequência que foi utilizada para produzir o *Framework* de NIP-CS-DC, a qual é a mesma sequência que se espera da sua implementação real em um ambiente organizacional. Foi usada uma representação piramidal na qual se adotou uma convergência que se irradia da base para o topo.

Assim, como primeiro estágio, estão as “matérias-primas”, ou seja, os *frameworks* que podem ser utilizados para delimitar o conjunto universo do que se deve saber. No estágio intermediário está o *framework* de teoria adotada para defesa cibernética, no qual a matéria-prima dos *frameworks* originais é rearranjada para servir de guia para produzir, preferencialmente de modo sistemático e metodológico, os efeitos de interpretações, conhecimentos explícitos e regras de defesa cibernética no ambiente organizacional a que for aplicado. Por fim, a partir de um ambiente organizacional em que o conhecimento de defesa cibernética prospera e amadurece, é possível, a partir do *framewor*k de teoria adotada para defesa cibernética do segundo nível, formular o *framework* de NIP-CS-DC como ápice do processo. A partir deste ponto, as ações decorrentes tendem a prover incrementos significativos à capacidade de exercitar a consciência situacional por parte de comandantes e gestores, em seus níveis diversos de decisão.

A Figura 125 mostra uma forma estilizada do *Framework* de NIP-CS-DC num conjunto organizado nas categorias que definem os estágios da consciência situacional, ou seja, percepção, compreensão e projeção, e nos conjuntos das ações cibernéticas de proteção, exploração e ataque. As NIP, por sua vez, estão identificadas pela designação adotada desde os Quadro 9 e 10 e reproduzidas nos Quadros 13 e 14.

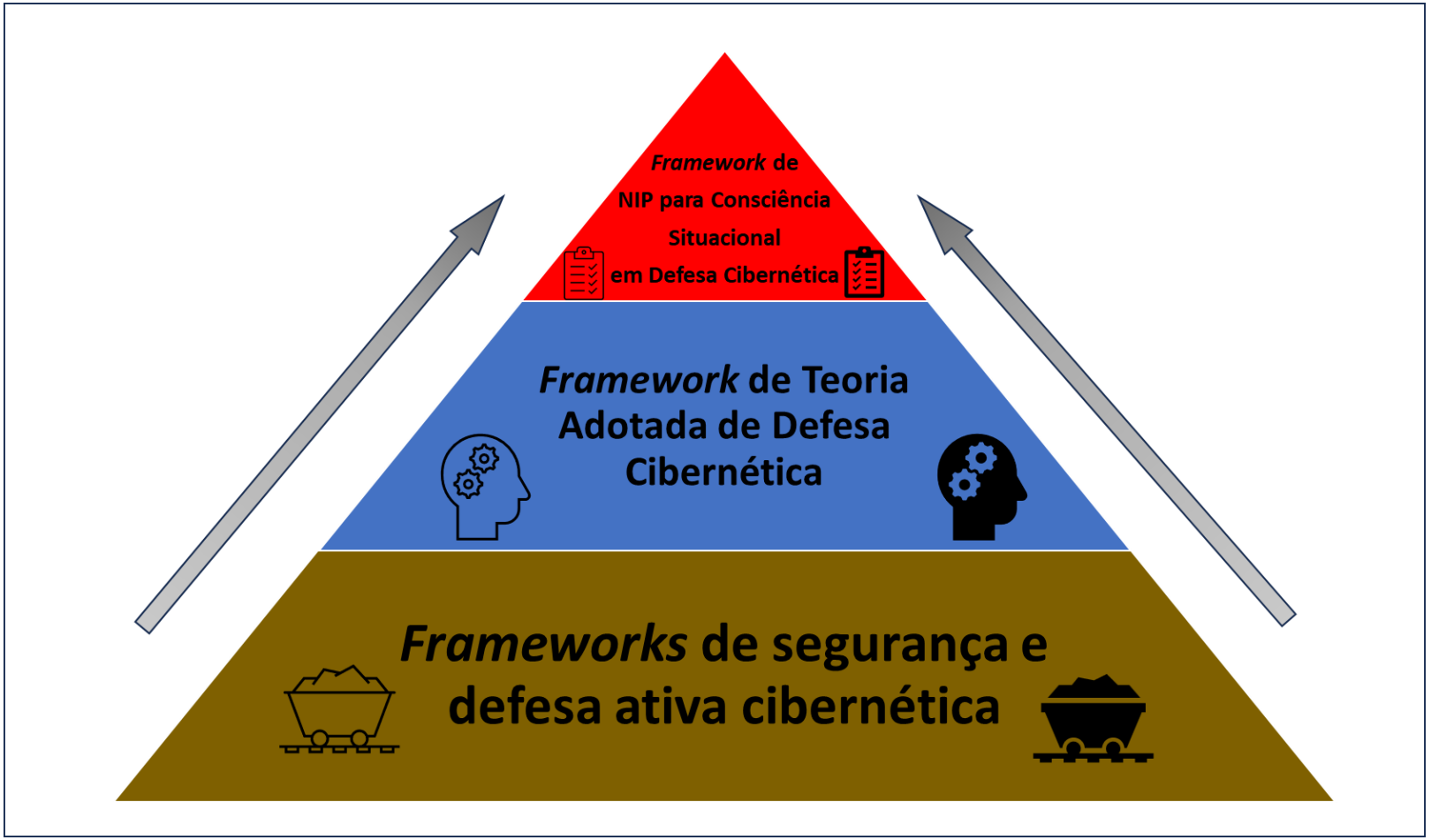
Considerando que as NIP-CS-DC são elementos de consulta e ponto de partida para uma série de possibilidades de como as informações correspondentes deverão ser buscadas e usadas para produzir os resultados que se esperam, foi adotada na Figura 125 uma representação do *Framework* de NIP-CS-DC que lembra uma estante de livros. Essa “estante” tem três módulos, correspondentes a cada estágio de consciência situacional, onde estão organizados os “livros”.

Na primeira “prateleira” estão os volumes relativos às ações de exploração e ataque, tendo sido a cor vermelha adotada por lembrar os *red teams*, designação utilizada no campo da cibernética para as equipes que são empregadas para realizar explorações e ataques durante exercícios controlados de defesa cibernética.

Nas três “prateleiras” seguintes estão os volumes relativos às ações de proteção cibernética, tendo sido a cor azul adotada por lembrar os *blue teams*, designação utilizada no campo da cibernética para as equipes que são empregadas para proteger e responder a incidentes advindos de explorações e ataques durante exercícios controlados de defesa cibernética. As tonalidades de azul apenas foram utilizadas para diferenciar os “livros” de proteção, conforme estágio de CS.

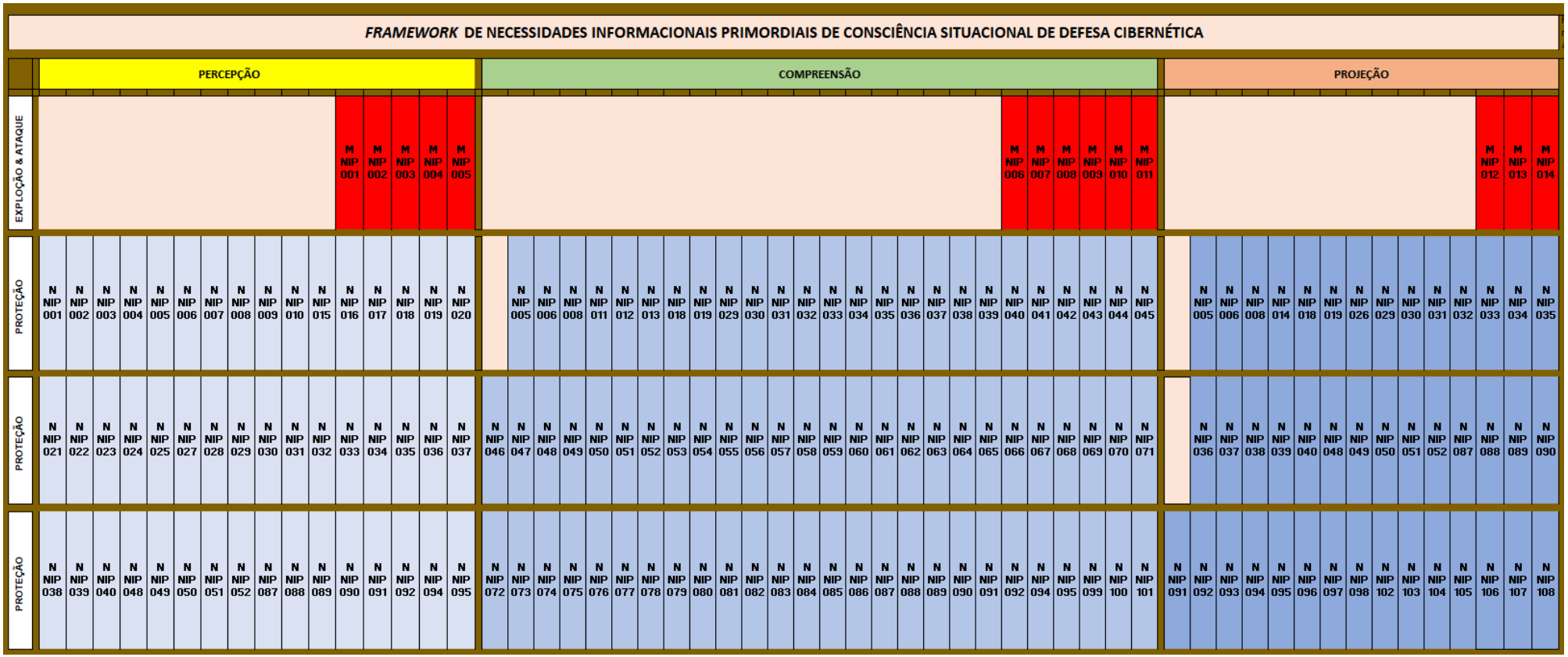
Por fim, cabe ressaltar que algumas repetições de “livros” entre os módulos de consciência situacional são em razão da mesma NIP se desdobrar de modos diferentes conforme o estágio de CS em que está.

Figura 126 - Sequência de ações seguidas na pesquisa para produzir o *Framework* de NIP-CS-DC



Fonte: Autor

Figura 127 - Representação das NIP por estágio de CS e tipos de ações cibernética



Fonte: Autor

Quadro 13 - Framework de NIP de Consciência Situacional para Defesa Cibernética – proteção cibernética (continua)

ESTÁGIO DE CS	Id NIP_CS_DC	NECESSIDADES INFORMACIONAIS PRIMORDIAIS DE CS PARA DC (Proteção Cibernética)
PERCEPÇÃO	N-NIP001	*Quais os ativos informacionais internos físicos e de sistemas relevantes para a operação a serem inventariados?*
PERCEPÇÃO	N-NIP002	*Quais os ativos informacionais internos de aplicações e de software relevantes para a operação a serem inventariados?*
PERCEPÇÃO	N-NIP003	*Quais são as comunicações e fluxos informacionais a serem mapeados?*
PERCEPÇÃO	N-NIP004	*Quais os sistemas de informação externos a serem catalogados?*
PERCEPÇÃO	N-NIP005	*Qual o papel da organização na cadeia de suprimentos envolvida na operação e para quem deve ser comunicado?*
PERCEPÇÃO	N-NIP006	*(Apenas para organizações consideradas IEC) Qual a posição da organização na infraestrutura crítica e em seu setor industrial e para quem deve ser comunicada?*
PERCEPÇÃO	N-NIP007	*Quais são as vulnerabilidades dos ativos que devem ser identificadas e documentadas?*
PERCEPÇÃO	N-NIP008	*Quais os foruns e fontes de compartilhamento de informações sobre ameaças cibernéticas são relevantes para a missão?*
PERCEPÇÃO	N-NIP009	*Quais são as ameaças internas e externas a serem identificadas e documentadas?*
PERCEPÇÃO	N-NIP010	*Quais as linhas de base das operações de rede e fluxos de dados esperados para usuários e sistemas devem ser estabelecidas e gerenciadas?*
PERCEPÇÃO	N-NIP015	*Que redes devem ser monitoradas para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?*
PERCEPÇÃO	N-NIP016	*Que ambientes físicos devem ser monitorados para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?*
PERCEPÇÃO	N-NIP017	*Que tipo de atividade de pessoal deve ser monitorado para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?*
PERCEPÇÃO	N-NIP018	*Que métodos e tecnologias devem ser empregadas para detecção de código malicioso?*
PERCEPÇÃO	N-NIP019	*Que métodos e tecnologias devem ser empregadas para detecção de código móvel não autorizado?*
PERCEPÇÃO	N-NIP020	*Que tipo de atividade de provedor de serviços externos deve ser monitorado para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?*
PERCEPÇÃO	N-NIP021	*Que tipo de atividade de monitoração de pessoal, conexões, dispositivos e software não autorizados deve ser realizada para detectar possíveis eventos de segurança cibernética e que tipos de monitoração devem ser realizadas?*
PERCEPÇÃO	N-NIP022	*Que tipo de varreduras de vulnerabilidade devem ser realizadas?*
PERCEPÇÃO	N-NIP023	*Que tipo de funções e atribuições para detecção devem ser definidas para garantir responsabilidade?*
PERCEPÇÃO	N-NIP024	*Que critérios de conformidade devem ser adotados para se verificar se as atividades de detecção estão em conformidade com todos os requisitos aplicáveis?*
PERCEPÇÃO	N-NIP025	*Que tipo de testes devem ser aplicados e mantidos para os processos de detecção?*
PERCEPÇÃO	N-NIP027	*Como os processos de detecção devem ser continuamente melhorados?*
PERCEPÇÃO	N-NIP028	*Como deve ser organizada uma sistemática de priorização de recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software), tendo por base a sua classificação, criticidade e valor para o negócio?*
PERCEPÇÃO	N-NIP029	*Que funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros devem ser estabelecidas?*
PERCEPÇÃO	N-NIP030	*Quais são as prioridades para a missão, objetivos e atividades organizacionais a serem estabelecidas e comunicadas?*
PERCEPÇÃO	N-NIP031	*Quais são os serviços essenciais que sustentam a infraestrutura da operação e quais sãos as dependências e funções críticas para o seu provimento?*
PERCEPÇÃO	N-NIP032	*A política organizacional de cibersegurança está estabelecida e comunicada?*
PERCEPÇÃO	N-NIP033	*Quais as funções e responsabilidades de cibersegurança, funções internas e parceiros externos devem ser coordenadas e alinhadas?*
PERCEPÇÃO	N-NIP034	*Quais são os requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis devem ser compreendidos e gerenciados?*
PERCEPÇÃO	N-NIP035	*Quais os riscos de cibersegurança são abordados nos processos de governança e gerenciamento de riscos?*
PERCEPÇÃO	N-NIP036	*Quais os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais e quais outras são necessários?*
PERCEPÇÃO	N-NIP037	*Quais os processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais e quais outros são necessários?*
PERCEPÇÃO	N-NIP038	*Quais fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos e quais outros também o devem ser?*
PERCEPÇÃO	N-NIP039	*Os objetivos do programa de cibersegurança da organização envolvida na operação e Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos são atendidos nos contratos com fornecedores e parceiros terceirizados?*
PERCEPÇÃO	N-NIP040	*Que avaliações por meio de auditorias, resultados de testes ou outras formas de avaliação, fornecedores e parceiros terceirizados devem ser rotineiramente avaliados para confirmar que estão cumprindo suas obrigações contratuais?*
PERCEPÇÃO	N-NIP048	*Quais informações e treinamentos devem ser dados aos usuários?*
PERCEPÇÃO	N-NIP049	*Usuários privilegiados entendam seus papéis e responsabilidades?*
PERCEPÇÃO	N-NIP050	*O que deve se realizado para que as partes interessadas de terceiros entendam seus papéis e responsabilidades?*
PERCEPÇÃO	N-NIP051	*O que deve se realizado para que executivos seniores entendam seus papéis e responsabilidades?*
PERCEPÇÃO	N-NIP052	*O que deve se realizado para que o pessoal de segurança física e cibernética entendem seus papéis e responsabilidades?*
PERCEPÇÃO	N-NIP087	*Quais são os requisitos de resiliência que devem ser estabelecidos para todos os estados operacionais para apoiar a entrega de serviços críticos (por exemplo, sob pressão/ataque, durante a recuperação, operações normais)?*
PERCEPÇÃO	N-NIP088	*Que impactos e probabilidades potenciais nos negócios podem ser identificados?*
PERCEPÇÃO	N-NIP089	*Que ameaças, vulnerabilidades, probabilidades e impactos devem ser considerados são utilizados para determinar o risco?*
PERCEPÇÃO	N-NIP090	*O que é necessário para identificar e priorizar as respostas ao risco?*
PERCEPÇÃO	N-NIP091	*O que é necessário para determinar a tolerância organizacional aos riscos e claramente a expressar?*
PERCEPÇÃO	N-NIP092	*O que é necessário para informar a determinação da tolerância a riscos da organização, considerando o seu papel na infraestrutura crítica e na análise de riscos específicos do setor?*
PERCEPÇÃO	N-NIP094	*O que é necessário para executar o plano de resposta durante ou após um incidente?*
PERCEPÇÃO	N-NIP095	*O que é necessário para que o pessoal conheça suas funções e ordem de operações quando uma resposta é necessária?*

Fonte: Autor

Quadro 13 - *Framework* de NIP de Consciência Situacional para Defesa Cibernética – proteção cibernética (continua)

ESTÁGIO DE CS	Id NIP_CS_DC	NECESSIDADES INFORMACIONAIS PRIMORDIAIS DE CS PARA DC (Proteção Cibernética)
COMPREENSÃO	N-NIP005	*Qual o papel da organização na cadeia de suprimentos envolvida na operação e para quem deve ser comunicado?*
COMPREENSÃO	N-NIP006	*(Apenas para organizações consideradas IEC) Qual a posição da organização na infraestrutura crítica e em seu setor industrial e para quem deve ser comunicada?*
COMPREENSÃO	N-NIP008	*Quais os foruns e fontes de compartilhamento de informações sobre ameaças cibernéticas são relevantes para a missão?*
COMPREENSÃO	N-NIP011	*Que requisitos são necessários para especificar uma estrutura para detectar e analisar eventos para entender os alvos e métodos de ataque?*
COMPREENSÃO	N-NIP012	*Que tipos de dados de eventos devem ser coletados e correlacionados e quais as fontes e sensores devem ser usadas?*
COMPREENSÃO	N-NIP013	*Que critérios de impacto dos eventos são adequados para a operação?*
COMPREENSÃO	N-NIP018	*Que métodos e tecnologias devem ser empregadas para detecção de código malicioso?*
COMPREENSÃO	N-NIP019	*Que métodos e tecnologias devem ser empregadas para detecção de código móvel não autorizado?*
COMPREENSÃO	N-NIP029	*Que funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros devem ser estabelecidas?*
COMPREENSÃO	N-NIP030	*Quais são as prioridades para a missão, objetivos e atividades organizacionais a serem estabelecidas e comunicadas?*
COMPREENSÃO	N-NIP031	*Quais são os serviços essenciais que sustentam a infraestrutura da operação e quais sãos as dependências e funções críticas para o seu provimento?*
COMPREENSÃO	N-NIP032	*A política organizacional de cibersegurança está estabelecida e comunicada?*
COMPREENSÃO	N-NIP033	*Quais as funções e responsabilidades de cibersegurança, funções internas e parceiros externos devem ser coordenadas e alinhadas?*
COMPREENSÃO	N-NIP034	*Quais são os requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis devem ser compreendidos e gerenciados?*
COMPREENSÃO	N-NIP035	*Quais os riscos de cibersegurança são abordados nos processos de governança e gerenciamento de riscos?*
COMPREENSÃO	N-NIP036	*Quais os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais e quais outras são necessários?*
COMPREENSÃO	N-NIP037	*Quais os processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais e quais outros são necessários?*
COMPREENSÃO	N-NIP038	*Quais fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos e quais outros também o devem ser?*
COMPREENSÃO	N-NIP039	*Os objetivos do programa de cibersegurança da organização envolvida na operação e Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos são atendidos nos contratos com fornecedores e parceiros terceirizados?*
COMPREENSÃO	N-NIP040	*Que avaliações por meio de auditorias, resultados de testes ou outras formas de avaliação, fornecedores e parceiros terceirizados devem ser rotineiramente avaliados para confirmar que estão cumprindo suas obrigações contratuais?*
COMPREENSÃO	N-NIP041	*Quais são as identidades e credenciais a serem emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados?*
COMPREENSÃO	N-NIP042	*Quais são os acessos físicos aos ativos a serem gerenciados e protegidos?*
COMPREENSÃO	N-NIP043	*Quais serão os acessos remotos necessários e qual a forma de gerenciamento deve ser empregada?*
COMPREENSÃO	N-NIP044	*Quais as permissões e autorizações de acesso incorporando os princípios de privilégio mínimo e separação de funções devem ser estabelecidas e gerenciadas?*
COMPREENSÃO	N-NIP045	*Quais ações para proteger a integridade da rede devem ser realizadas?*
COMPREENSÃO	N-NIP046	*Quais as ações para verificar as identidades e as vincular às respectivas credenciais?*
COMPREENSÃO	N-NIP047	*O que é necessário para autenticar usuários, dispositivos e outros ativos proporcionalmente ao risco da transação?*
COMPREENSÃO	N-NIP048	*Quais informações e treinamentos devem ser dados aos usuários?*
COMPREENSÃO	N-NIP049	*Usuários privilegiados entendam seus papéis e responsabilidades?*
COMPREENSÃO	N-NIP050	*O que deve se realizado para que as partes interessadas de terceiros entendam seus papéis e responsabilidades?*
COMPREENSÃO	N-NIP051	*O que deve se realizado para que executivos seniores entendam seus papéis e responsabilidades?*
COMPREENSÃO	N-NIP052	*O que deve se realizado para que o pessoal de segurança física e cibernética entendem seus papéis e responsabilidades?*
COMPREENSÃO	N-NIP053	*Quais ações devem ser realizadas para proteger dados em repouso?*
COMPREENSÃO	N-NIP054	*Quais ações devem ser realizadas para proteger dados em trânsito?*
COMPREENSÃO	N-NIP055	*O que é necessário para formalmente gerenciar os ativos de dados durante a remoção, transferências e disposição?*
COMPREENSÃO	N-NIP056	*O que é necessário para manter a capacidade adequada para garantir a disponibilidade?*
COMPREENSÃO	N-NIP057	*Que proteções contra vazamentos de dados devem ser implementadas?*
COMPREENSÃO	N-NIP058	*Quais mecanismos de verificação de integridade são usados para verificar a integridade do software, firmware e informações?*
COMPREENSÃO	N-NIP059	*Que é necessário realizar para criar e manter ambientes de desenvolvimento e teste separados do ambiente de produção?*
COMPREENSÃO	N-NIP060	*Que mecanismos de verificação de integridade devem ser usados para verificar a integridade do hardware?*
COMPREENSÃO	N-NIP061	*O que é necessário para criar e manter uma configuração básica de sistemas de tecnologia da informação/sistemas de controle industrial, incorporando princípios de segurança?*
COMPREENSÃO	N-NIP062	*Qual deve ser o Ciclo de Vida de Desenvolvimento de Sistemas empregado na gerência de sistemas empregados na operação?*
COMPREENSÃO	N-NIP063	*Quais pocessos de controle de mudanças de configuração devem estar em vigor?*
COMPREENSÃO	N-NIP064	*Quais informações devem possuir backups e que processos devem ser realizados para mantê-los testá-los?*
COMPREENSÃO	N-NIP065	*Que ações são necessárias para que políticas e regulamentos referentes ao ambiente operacional físico de ativos organizacionais sejam atendidos?*
COMPREENSÃO	N-NIP066	*Que processo deve ser realizado para que os dados sejam destruídos de acordo com a política?*
COMPREENSÃO	N-NIP067	*O que é necessário para aprimorar os processos de proteção?*
COMPREENSÃO	N-NIP068	*Como compartilhar a eficácia das tecnologias de proteção?*

Fonte: Autor

Quadro 13 - *Framework* de NIP de Consciência Situacional para Defesa Cibernética – proteção cibernética (continua)

ESTÁGIO DE CS	Id NIP_CS_DC	NECESSIDADES INFORMACIONAIS PRIMORDIAIS DE CS PARA DC (Proteção Cibernética)
COMPREENSÃO	N-NIP069	*O que é necessário para manter em vigor e gerenciar os Planos de Resposta a Incidentes e Continuidade de Negócios e os planos de Recuperação de Incidentes e Recuperação de Desastres?*
COMPREENSÃO	N-NIP070	*O que é necesário para testear os planos de resposta e recuperação?*
COMPREENSÃO	N-NIP071	*O que é necessário para incluir a cibersegurança nas práticas de recursos humanos?*
COMPREENSÃO	N-NIP072	*O que é necessário para desenvolver e implementar um plano de gerenciamento de vulnerabilidades?*
COMPREENSÃO	N-NIP073	*O que é necessário para que a manutenção e reparo de ativos organizacionais sejam realizados e registrados, utilizando ferramentas aprovadas e controladas?*
COMPREENSÃO	N-NIP074	*O que é necessário para aprovar, registrar e realizar a manutenção remota de ativos organizacionais, evitando acesso não autorizado?*
COMPREENSÃO	N-NIP075	*O que é necessário para determinar, documentar, implementar e revisar registros de auditoria/sistema de acordo com a política?*
COMPREENSÃO	N-NIP076	*O que é necessário para proteger mídias removíveis e restringir o seu uso de acordo com a política?*
COMPREENSÃO	N-NIP077	*O que é necessário para incorporar o princípio da menor funcionalidade configurando sistemas para fornecer apenas as capacidades essenciais?*
COMPREENSÃO	N-NIP078	*O que é necessário para proteger as redes de comunicação e controle da operação?*
COMPREENSÃO	N-NIP079	*Quais devem ser os requisitos de resiliências e os respectivos mecanismos (por exemplo, failsafe, balanceamento de carga, hot swap) a serem implementados para utilização em situações normais e adversas?*
COMPREENSÃO	N-NIP080	*O que é necessário para investigar as notificações dos sistemas de detecção?*
COMPREENSÃO	N-NIP081	*O que é necessário para realizar a perícia?*
COMPREENSÃO	N-NIP082	*O que é necessário para sistematicamente receber, analisar e responder a vulnerabilidades informadas à organização de fontes internas e externas?*
COMPREENSÃO	N-NIP083	*O que é necessário para incorporar lições aprendidas aos planos de resposta?*
COMPREENSÃO	N-NIP084	*O que é necessário para atualizar as estratégias de respostas?*
COMPREENSÃO	N-NIP085	*O que é necessário para incorporar lições aprendidas aos planos de recuperação?*
COMPREENSÃO	N-NIP086	*O que é necessário para atualizar as estratégias de recuperação?*
COMPREENSÃO	N-NIP087	*Quais são os requisitos de resiliência que devem ser estabelecidos para todos os estados operacionais para apoiar a entrega de serviços críticos (por exemplo, sob pressão/ataque, durante a recuperação, operações normais)?*
COMPREENSÃO	N-NIP088	*Que impactos e probabilidades potenciais nos negócios podem ser identificados?*
COMPREENSÃO	N-NIP089	*Que ameaças, vulnerabilidades, probabilidades e impactos devem ser utilizados para determinar o risco?*
COMPREENSÃO	N-NIP090	*O que é necessário para identificar e priorizar as respostas ao risco?*
COMPREENSÃO	N-NIP091	*O que é necessário para determinar a tolerância organizacional aos riscos e claramente a expressar?*
COMPREENSÃO	N-NIP092	*O que é necessário para informar a determinação da tolerância a riscos da organização, considerando o seu papel na infraestrutura crítica e na análise de riscos específicos do setor?*
COMPREENSÃO	N-NIP094	*O que é necessário para executar o plano de resposta durante ou após um incidente?*
COMPREENSÃO	N-NIP095	*O que é necessário para que o pessoal conheça suas funções e ordem de operações quando uma resposta é necessária?*
COMPREENSÃO	N-NIP099	*O que é necessário para realizar um compartilhamento voluntário de informações com as partes interessadas externas para alcançar uma compreensão mais ampla da situação de segurança cibernética?*
COMPREENSÃO	N-NIP100	*O que é necessário para compreender o impacto de um incidente?*
COMPREENSÃO	N-NIP101	*O que é necessário para categorizar os incidentes de acordo com os planos de resposta?*

Fonte: Autor

Quadro 13 - *Framework* de NIP de Consciência Situacional para Defesa Cibernética – proteção cibernética (conclusão)

ESTÁGIO DE CS	Id NIP_CS_DC	NECESSIDADES INFORMACIONAIS PRIMORDIAIS DE CS PARA DC (Proteção Cibernética)
PROJEÇÃO	N-NIP005	*Qual o papel da organização na cadeia de suprimentos envolvida na operação e para quem deve ser comunicado?*
PROJEÇÃO	N-NIP006	*(Apenas para organizações consideradas IEC) Qual a posição da organização na infraestrutura crítica e em seu setor industrial e para quem deve ser comunicada?*
PROJEÇÃO	N-NIP008	*Quais os foruns e fontes de compartilhamento de informações sobre ameaças cibernéticas são relevantes para a missão?*
PROJEÇÃO	N-NIP014	*Que critérios devem ser usados para estabelecer um esquema de categorias de alertas de incidentese com respectivos limites e ações?*
PROJEÇÃO	N-NIP018	*Que métodos e tecnologias devem ser empregadas para detecção de código malicioso?*
PROJEÇÃO	N-NIP019	*Que métodos e tecnologias devem ser empregadas para detecção de código móvel não autorizado?*
PROJEÇÃO	N-NIP026	*Que processos de compartilhamento da informação devem ser realizados sobre eventos detectados no espaço cibernético da operação?*
PROJEÇÃO	N-NIP029	*Que funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros devem ser estabelecidas?*
PROJEÇÃO	N-NIP030	*Quais são as prioridades para a missão, objetivos e atividades organizacionais a serem estabelecidas e comunicadas?*
PROJEÇÃO	N-NIP031	*Quais são os serviços essenciais que sustentam a infraestrutura da operação e quais sãos as dependências e funções críticas para o seu provimento?*
PROJEÇÃO	N-NIP032	*A política organizacional de cibersegurança está estabelecida e comunicada?*
PROJEÇÃO	N-NIP033	*Quais as funções e responsabilidades de cibersegurança, funções internas e parceiros externos devem ser coordenadas e alinhadas?*
PROJEÇÃO	N-NIP034	*Quais são os requisitos legais e regulatórios relacionados à cibersegurança, incluindo obrigações de privacidade e liberdades civis devem ser compreendidos e gerenciados?*
PROJEÇÃO	N-NIP035	*Quais os riscos de cibersegurança são abordados nos processos de governança e gerenciamento de riscos?*
PROJEÇÃO	N-NIP036	*Quais os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelos stakeholders organizacionais e quais outras são necessários?*
PROJEÇÃO	N-NIP037	*Quais os processos de gestão de riscos cibernéticos na cadeia de suprimentos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders organizacionais e quais outros são necessários?*
PROJEÇÃO	N-NIP038	*Quais fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de riscos cibernéticos na cadeia de suprimentos e quais outros também o devem ser?*
PROJEÇÃO	N-NIP039	*Os objetivos do programa de cibersegurança da organização envolvida na operação e Plano de Gestão de Riscos Cibernéticos na Cadeia de Suprimentos são atendidos nos contratos com fornecedores e parceiros terceirizados?*
PROJEÇÃO	N-NIP040	*Que avaliações por meio de auditorias, resultados de testes ou outras formas de avaliação, fornecedores e parceiros terceirizados devem ser rotineiramente avaliados para confirmar que estão cumprindo suas obrigações contratuais?*
PROJEÇÃO	N-NIP048	*Quais informações e treinamentos devem ser dados aos usuários?*
PROJEÇÃO	N-NIP049	*Usuários privilegiados entendam seus papéis e responsabilidades?*
PROJEÇÃO	N-NIP050	*O que deve se realizado para que as partes interessadas de terceiros entendam seus papéis e responsabilidades?*
PROJEÇÃO	N-NIP051	*O que deve se realizado para que executivos seniores entendam seus papéis e responsabilidades?*
PROJEÇÃO	N-NIP052	*O que deve se realizado para que o pessoal de segurança física e cibernética entendem seus papéis e responsabilidades?*
PROJEÇÃO	N-NIP087	*Quais são os requisitos de resiliência que devem ser estabelecidos para todos os estados operacionais para apoiar a entrega de serviços críticos (por exemplo, sob pressão/ataque, durante a recuperação, operações normais)?*
PROJEÇÃO	N-NIP088	*Que impactos e probabilidades potenciais nos negócios podem ser identificados?*
PROJEÇÃO	N-NIP089	*Que ameaças, vulnerabilidades, probabilidades e impactos devem ser considerados são utilizados para determinar o risco?*
PROJEÇÃO	N-NIP090	*O que é necessário para identificar e priorizar as respostas ao risco?*
PROJEÇÃO	N-NIP091	*O que é necessário para determinar a tolerância organizacional aos riscos e claramente a expressar?*
PROJEÇÃO	N-NIP092	*O que é necessário para informar a determinação da tolerância a riscos da organização, considerando o seu papel na infraestrutura crítica e na análise de riscos específicos do setor?*
PROJEÇÃO	N-NIP093	*O que é necessário para planejar e testar as resposta e procedimentos de recuperação com fornecedores e provedores terceirizados?*
PROJEÇÃO	N-NIP094	*O que é necessário para executar o plano de resposta durante ou após um incidente?*
PROJEÇÃO	N-NIP095	*O que é necessário para que o pessoal conheça suas funções e ordem de operações quando uma resposta é necessária?*
PROJEÇÃO	N-NIP096	*O que é necessário para relatar os incidentes de acordo com os critérios estabelecidos?*
PROJEÇÃO	N-NIP097	*O que é necessário para compartilhar as informações de acordo com os planos de resposta?*
PROJEÇÃO	N-NIP098	*O que é necessário para coordenar com as partes interessadas de acordo com os planos de resposta?*
PROJEÇÃO	N-NIP102	*O que é necessário para conter um incidentes?*
PROJEÇÃO	N-NIP103	*O que é necessário para mitigar um incidentes?*
PROJEÇÃO	N-NIP104	*O que é necessário para mitigar as vulnerabilidades recém-identificadas ou documentá-las como riscos aceitos?*
PROJEÇÃO	N-NIP105	*O que é necessário para a execução de um plano de recuperação durante ou após um incidente de cibersegurança?*
PROJEÇÃO	N-NIP106	*O que é necesário para gerenciar as relações públicas?*
PROJEÇÃO	N-NIP107	*O que é necessário para restaurar a reputação após um incidente.*
PROJEÇÃO	N-NIP108	*O que é necessário para comunicar as atividades de recuperação às partes interessadas internas e externas, bem como às equipes executivas e de gerenciamento?*

Fonte: Autor

Quadro 14 - Framework de NIP de Consciência Situacional para Defesa Cibernética – proteção cibernética

ESTÁGIO DE CS	Nr NIP	NECESSIDADES INFORMACIONAIS PRIMORDIAIS DE CS PARA DC (Exploração e Ataque Cibernéticos)
PERCEPÇÃO	M-NIP001	*Quais informações do alvo se deve tentar coletar que possam ser usadas para planejar operações futuras?*
PERCEPÇÃO	M-NIP002	*Que recursos se deve obter e estabelecer que possam ser usados para apoiar operações para alcançar o alvo?*
PERCEPÇÃO	M-NIP003	*Quais as formas para se tentar entrar na sua rede do alvo?*
PERCEPÇÃO	M-NIP004	*Quais e de que forma devem ser obtidas nomes de conta e senhas do alvo?*
PERCEPÇÃO	M-NIP005	*Quais dados de interesse para seu objetivo específico na rede do alvo devem ser reunidos?*
COMPREENSÃO	M-NIP006	*De que forma e quais códigos maliciosos se deve tentar executar em locais específicos da rede do alvo?*
COMPREENSÃO	M-NIP007	*O que é necesário para se tentar manter a posição na rede do alvo?*
COMPREENSÃO	M-NIP008	*O que é necessário para se obter permissões de nível mais alto na rede do alvo?*
COMPREENSÃO	M-NIP009	*O que é necessário para evitar ser detectado?*
COMPREENSÃO	M-NIP010	*O que é necessário para se entender o ambiente atacado?*
COMPREENSÃO	M-NIP011	*O que é necessário para realizar o deslocamento através do ambiente da rede do alvo?*
PROJEÇÃO	M-NIP012	*O que é necessário para se comunicar com os sistemas comprometidos na rede do alvo para controlá-los?*
PROJEÇÃO	M-NIP013	*O que é necessário para se apoderar de dados do alvo?*
PROJEÇÃO	M-NIP014	*O que é necessário para tentar manipular, interromper ou destruir os sistemas e dados do alvo?*

Fonte: Autor

6.5.6. Aplicação do *Framework* de NIP-CS-DC

Este tópico buscou descrever de forma simples como aplicar o *framework* de NIP-CS-DC, viabilizando assim o seu uso sem que haja a necessidade de reproduzir toda a sistemática seguida na pesquisa.

Considerando que o *framework* de NIP-CS-DC é um produto acabado e pronto para aplicação, o seu emprego pode ser direto em uma situação concreta, conforme a validação preliminar da pesquisa sugere.

No entanto, cabe ressaltar que, de acordo com as discussões dos resultados da pesquisa, o sucesso da aplicação do *framework* de NIP-CS-DC se baseia no nível de conhecimento organizacional em defesa cibernética alcançado no ambiente dos decisores pertencentes à cadeia de decisão e de consciência situacional que atuarão em operações de defesa cibernética. Esse conhecimento pode ser consolidado sem o emprego de uma sistemática formalmente adotada pela instituição para a gestão do conhecimento, como os dados da pesquisa demonstraram indiretamente, embora essa condição não seja desejável, pois isso tende a comprometer significativamente o emprego das NIP, como a pesquisa também identificou quando da análise comparativa entre as operações Atlântico III e Laçador 2013.

Logo, o *framework* pode ser aplicado diretamente, sendo que seus aplicadores devem estar cientes das nuances ressaltadas neste tópico. No entanto, recomenda-se uma preparação contínua para seu sucesso, acrescentando os estágios do ciclo de conhecimento organizacional para defesa cibernética e de modo sistemático.

Assim, neste tópico são apresentadas duas possibilidades de aplicação do *framework* de NIP-CS-DC. A primeira, aplicada por ocasião de uma necessidade específica e pontual, e a segunda, aplicada de modo contínuo e permanente. Esses dois modos estão explicados nos subitens 6.5.6.1 e 6.5.6.2. Para tal, foi adotada uma abordagem de processo, de modo a facilitar a apreensão da aplicação do *framework* de NIP-CS-DC. Esses processos estão representados nas Figuras 127 e 128.

Deve-se ter claro em mente que **a finalidade do *framework* de NIP-CS-DC é gerar o conjunto de necessidades informacionais particulares que impliquem em ações que criem as condições para que os decisores envolvidos**

alcancem uma consciência situacional adequada sobre o espaço cibernético de interesse da missão, seja essa missão a constituição de uma estrutura de defesa cibernética temporária, como uma operação militar, ou um centro de monitoração permanente.

Por fim, é de grande relevância lembrar que o emprego do *framework* de NIP-CS-DC não foi concebido para planejamento de operações ou implementação de centros de monitoração de defesa cibernética como um todo, mas sim para deflagração de ações para potencializar a consciência situacional de defesa cibernética a ser realizada nessas estruturas. Apesar dessa especificidade inerente a sua estruturação, o fato de as NIP serem resultantes diretas dos controles e táticas dos *frameworks* estudados faz como que seu emprego, de forma inevitável e desejável, se reflita nos requisitos de implementação das infraestruturas que abrangerão os ativos que viabilizarão o exercício da consciência situacional de defesa cibernética.

6.5.6.1. Aplicação por ocasião específica e temporária

Para a aplicação por ocasião específica e temporária, propõe-se uma estrutura de processo, conforme a Figura 127.

O primeiro estágio é o da identificação de todos os elementos direcionadores da missão, podendo ser objetivos, metas, planejamentos de ordens superiores, diretrizes, políticas, normas, regras, saídas de processos ou outro elemento de valor equivalente. Isso estabelece o que deve abranger e direcionar as ações correspondentes de cada estágio da consciência situacional. Nesse estágio, as NIP ainda não são consultadas, mas sim os documentos orientadores aplicáveis à missão.

O segundo estágio, ainda relacionado ao aspecto de direcionamento inicial, é subdividido em três subprocessos: (i) seleção, no *framework* de NIP-CS-DC, das NIP que são aplicáveis às três fases da CS e que são ligadas às metas, objetivos e perspectivas, conforme modelo de Endsley (1995); (ii) para cada uma das NIP selecionadas, deve-se analisar se na situação específica ela é ou não aplicável, desconsiderando-se as não aplicáveis; (iii) analisar cada NIP e particularizá-la para a situação específica da missão (pode não haver a necessidade de particularização).

Estabelecidos os estágios direcionadores, seguem-se os estágios correspondentes às fases da consciência situacional: percepção, compreensão e projeção. A abordagem dessas três fases de CS é integralmente similar ao realizado no segundo estágio, havendo os mesmos tipos de subprocessos, podendo ser aplicado tanto na porção do *framework* baseado em NIP de proteção cibernética quanto na porção baseada em ataque e exploração cibernéticas. três as ações de defesa cibernética, ou seja, proteção, exploração e ataque cibernético, conforme a natureza da missão.

No terceiro estágio, correspondente à percepção, são os seguintes os subprocessos: (i) seleção no *framework* das NIP que são aplicáveis à fase da percepção da CS, inclusive aquelas cuja aplicação se repete nas outras fases de CS; (ii) para cada uma das NIP selecionadas, deve-se analisar se na situação específica ela é ou não aplicável, desconsiderando-se as não aplicáveis; (iii) analisar cada NIP e particularizá-la para a situação específica da missão (pode não haver a necessidade de particularização).

No quarto estágio, correspondente à compreensão, são os seguintes os subprocessos: (i) seleção no *framework* das NIP que são aplicáveis à fase da compreensão da CS, inclusive aquelas cuja aplicação se repete nas outras fases de CS; (ii) para cada uma das NIP selecionadas, deve-se analisar se na situação específica ela é ou não aplicável, desconsiderando-se as não aplicáveis; (iii) analisar cada NIP e particularizá-la para a situação específica da missão (pode não haver a necessidade de particularização).

No quinto estágio, correspondente à projeção, são os seguintes os subprocessos: (i) seleção no *framework* das NIP que são aplicáveis à fase da projeção da CS, inclusive aquelas cuja aplicação se repete nas outras fases de CS; (ii) para cada uma das NIP selecionadas, deve-se analisar se na situação específica ela é ou não aplicável, desconsiderando-se as não aplicáveis; (iii) analisar cada NIP e particularizá-la para a situação específica da missão (pode não haver a necessidade de particularização).

No sexto e último estágio, deve-se compilar as Necessidade Informacionais produzidas para a situação específica. A partir desse ponto, tem-se os elementos informacionais de partida para busca e uso da informação a serem empregados em

planejamentos, compras, projetos, processos ou outras sistemáticas similares para aplicação à missão.

6.5.6.2. Aplicação contínua e permanente

Para a aplicação por ocasião específica e temporária, propõe-se uma estrutura de processo, conforme a Figura 128.

A aplicação contínua e permanente do *framework* de NIP-CS-DC se difere da aplicação por ocasião específica e temporária pelo acréscimo de outro processo que a antecede. Esse processo prévio diz respeito a aplicação do *framework* de teoria adotada para defesa cibernética e tem por finalidade aprimorar e aprofundar o conhecimento organizacional sobre defesa cibernética, pelo viés do conhecimento explícito, conforme o ciclo de conhecimento organizacional de Choo (1998).

Assim, o processo como um todo para aplicação das NIP-CS-DC para médio e longo prazo é composto por um primeiro processo a ser definido neste subtítulo conjuntamente como o processo para ocasião específica e temporária definido no subtítulo 6.5.6.1.

O processo prévio mencionado conta com cinco estágios: (i) direcionadores gerais da organização; (ii) capacitação dos integrantes da cadeia de decisão e consciência situacional sobre o que são e como se aplicam os controles e táticas dos *frameworks* **originais**; (iii) identificação e execução das ações relativas à organização das interpretações de defesa cibernética; (iv) identificação e execução das ações relativas ao conhecimento explícito de defesa cibernética; (v) identificação e execução das ações relativas à organização das regras de decisão de defesa cibernética.

O primeiro estágio é o da identificação de todos os elementos direcionadores da missão da organização, podendo ser objetivos, metas, planejamentos, diretrizes, políticas, normas, regras, saídas de processos ou outro elemento de valor equivalente. Isso estabelece o que deve abranger e direcionar a ação organizacional para defesa cibernética.

O segundo estágio é o da capacitação dos integrantes da cadeia de decisão e consciência situacional nos controles e táticas dos *frameworks*. Essa

capacitação pode ser uma ou mais dentre aquelas que, sendo de boa qualidade, são oferecidas no mercado. Um elemento de capacitação de importância significativa deve ser acrescido a essas capacitações comuns de mercado: exercícios de simulação de tomada de decisão e consciência situacional de defesa cibernética.

O terceiro estágio é da produção contínua de elementos específicos de interpretação de defesa cibernética, conforme rearranjo dos elementos dos *frameworks* estudados e a partir da infraestrutura de ativos disponíveis ou em implementação.

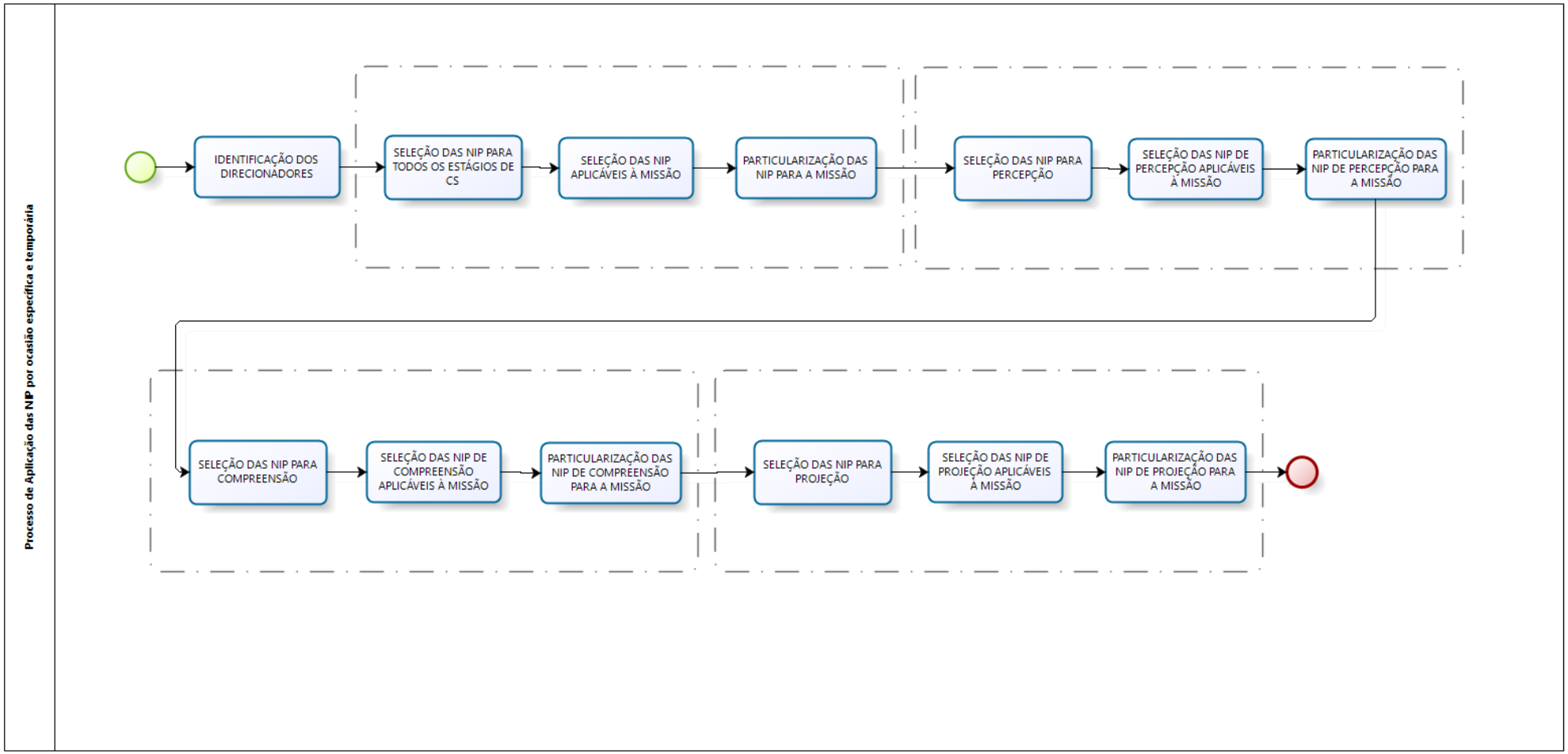
O quarto estágio é da produção contínua de elementos específicos de conhecimento explícito de defesa cibernética, conforme rearranjo dos elementos dos *frameworks* estudados e a partir da infraestrutura de ativos disponíveis ou em implementação.

O quinto estágio é da produção contínua de elementos específicos de regras de defesa cibernética, conforme rearranjo dos elementos dos *frameworks* estudados e a partir da infraestrutura de ativos disponíveis ou em implementação.

Para os estágios 2 a 5 é altamente recomendável a existência de uma estrutura de simulação de operações de defesa cibernética para encenação da aplicação da ação organizacional de defesa cibernética para avaliar a efetividade das interpretações, conhecimento explícito e regras de defesa cibernética.

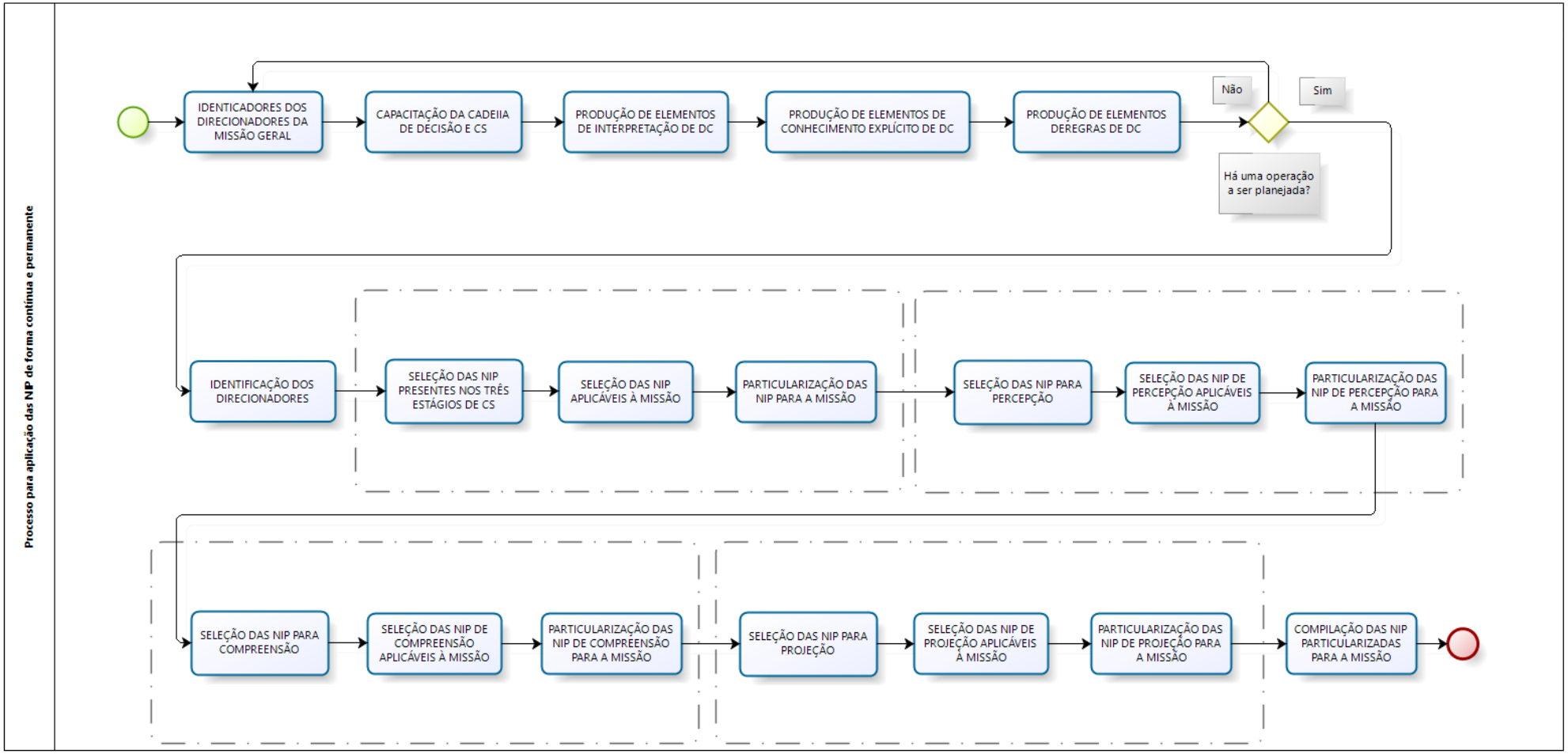
Assim, a Figura 128 retrata o processo completo, sendo a primeira parte o processo prévio descrito neste subtítulo e a segunda parte o processo de ocasião específica e temporária da Figura 127.

Figura 128 - Representação da aplicação das NIP-CS-DC em curto prazo



Fonte: Autor

Figura 129 - Representação da aplicação das NIP-CS-DC em médio e longo prazo



Fonte: Autor

7. CONCLUSÕES

Este capítulo apresenta o fecho desta pesquisa de doutorado, rememorando os passos principais, desde o questionamento central, até os resultados, acrescentando-se sugestões para pesquisas futuras.

7.1. PERGUNTA DE PESQUISA E OBJETIVOS

Este documento de tese partiu da seguinte pergunta de pesquisa: "*Como estruturar um framework que, baseado no ciclo de conhecimento organizacional, forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética no contexto da Defesa Nacional Brasileira no seu nível estratégico?"* Para abordar a questão, a pergunta foi convertida em objetivo geral, o que foi desdobrado em cinco objetivos específicos, quais sejam:

Objetivo geral: Propor um *framework*, baseado no ciclo de conhecimento organizacional de Choo (1998, p. 240), que forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética, conforme definida por Endsley (1995, p.35), no contexto da Defesa Nacional Brasileira no seu nível estratégico.

Objetivos específicos: (a) Identificar *frameworks* consagrados internacionalmente para segurança cibernética, segurança da informação e de ataque cibernético que serão úteis à pesquisa; (b) Identificar e aplicar critérios para seleção de elementos presentes nos *frameworks* escolhidos que sejam compatíveis com os aspectos do ciclo de gestão do conhecimento de Choo (1998, p. 240); (c) Identificar e aplicar critérios para relacionar os elementos de *frameworks* selecionados em relação ao ciclo de gestão do conhecimento de Choo (1998, p. 240) com os estágios de consciência situacional de Endsley (1995, p. 35) para primeira consolidação do *framework* a ser produzido na pesquisa; (d) Aplicar o *framework* consolidado nas documentações regulatórias e doutrinárias do Setor Cibernético da Defesa brasileira, assim como nos planejamentos das operações de defesa cibernética ocorridas no período de 2011 a 2017 para identificar as necessidades informacionais de cada evento ocorrido no período; (e) Discutir e concluir a

pertinência do *framework* proposto por meio do relacionamento entre as necessidades informacionais primordiais mapeadas para cada operação de defesa cibernética e os respectivos registros das lições aprendidas análises pós-ação realizadas no período estudado.

O objetivo geral demandou a articulação de três entes que, a princípio, pareceram pertencer a três contextos de aplicação absolutamente separados: o ciclo de conhecimento organizacional de Choo (1998, p. 240), o modelo de consciência situacional em defesa cibernética, conforme definido por Endsley (1995, p.35) e os *frameworks* de segurança e defesa cibernética.

Os objetivos específicos foram planejados para viabilizar a prospecção e identificação de pontos de convergência e articulação entre os modelos de Choo (1989) e Endsley (1995) e os instrumentos de gestão de segurança e defesa cibernética em que se constituem os *frameworks*. Essas integrações foram resolvidas pelos objetivos específicos a, b e c, conforme recortes e adaptações definidos no referencial teórico.

O maior desafio dessa pesquisa foi a aplicação do *framework* proposto, resultante da consecução do objetivo específico (c), na documentação das operações de defesa cibernética, assim como aferir sua pertinência, ou seja, a execução dos objetivos (d) e (e). O desafio residiu majoritariamente em se contar com conhecimentos teóricos e práticos prévios envolvendo o objeto da pesquisa e aplicar esses conhecimentos de forma coerente com os aspectos metodológicos exigidos no trabalho, de modo a apresentar uma forma válida de aferir o modelo.

Cabe ressaltar que a condução da pesquisa foi tal que o *framework* proposto, por ser de caráter primordial, pelo viés das necessidades informacionais de defesa cibernética, tem flexibilidade suficiente para ser aplicado tanto no nível estratégico quanto níveis intermediários de gestão ou puramente operacionais.

Em consequência da realização de todos os objetivos, consideram-se os objetivos alcançados e a pergunta de pesquisa respondida, cabendo ressaltar que a pesquisa não produziu um resultado definitivo e rígido, podendo haver atualizações, extensões ou outras adaptações para o caso de novos estudos que explorem o tema.

7.2. CONTRIBUIÇÕES DO TRABALHO

Este trabalho de pesquisa abrangeu os contextos de defesa cibernética, consciência situacional, conhecimento organizacional, necessidades informacionais e *frameworks*, provendo, sob diversos aspectos, contribuições para cada dessas áreas.

Defesa Cibernética

No campo da defesa cibernética, dentre as possíveis contribuições advindas da pesquisa, destaca-se a possibilidade de utilização do *framework* como instrumento de delimitação e especificação dos temas de relevância a serem considerados para planejamento de uma operação de defesa cibernética em seus aspectos de tecnologia da informação, gestão de riscos, processos de preparação, proteção, monitoração respostas e recuperação de incidentes e seus aspectos ofensivos.

Consciência Situacional

No campo da consciência situacional, o destaque maior é o próprio resultado da pesquisa que proveu um modo de potencializar a consciência situacional de defesa cibernética por meio de dois estágios. O primeiro é o da sedimentação e atualização do conhecimento organizacional de defesa cibernética como instrumento para alçar as habilidades, treinamentos e consolidação das experiências. O segundo trata do uso do *framework* proposto nesse terreno organizacional fertilizado para aumentar as chances de o ciclo do conhecimento chegar ao seu auge, que é o uso de qualidade das informações e conhecimentos ou, em outras palavras convergentes com o objeto da pesquisa, exercitar uma consciência situacional de defesa cibernética satisfatória.

Conhecimento Organizacional

Por força da necessidade imposta pelas decisões de condução da pesquisa, o referencial teórico estabeleceu um recorte de trabalho no ciclo do conhecimento organizacional proposto por Choo (1998) de modo que o trabalho tivesse o foco na teoria adotada, ainda que sem prejuízo para as áreas da teoria em uso e a cultura organizacional, pois, como Choo (1998) demonstrou, há uma influência mútuas entre essas áreas. Assim, a pesquisa proveu às organizações que trabalham voltadas para a defesa cibernética ou com ela podem interagir, um instrumento indutor da evolução

do conhecimento organizacional de defesa cibernética como um todo a partir da teoria adotada.

Necessidades Informacionais

Apesar da obviedade do caráter imprescindível da determinação das necessidades informacionais para desenvolver praticamente qualquer atividade gerencial complexa, como, por exemplo, uma operação de defesa cibernética, não foram localizados métodos gerais para determinação de necessidades informacionais, e sim métodos específicos em diversas áreas de conhecimento, ou ainda métodos com outros objetivos, mas que incidentalmente realizam, em algum grau, a descoberta de necessidades informacionais, sendo um exemplo, no campo da cibernética, a gestão de riscos. Assim, uma contribuição para o campo das necessidades informacionais foi o método utilizado na pesquisa, no qual os aspectos da teoria adotada foram usados como delimitadores e referências para rearranjar os elementos dos mecanismos de melhores práticas de mercado em um conjunto de necessidade informacionais, ao mesmo tempo que os aspectos de consciência situacional foram usados para colimar as necessidades informacionais geradas com precisão para o seu uso.

Frameworks

A contribuição para o contexto dos *frameworks*, considerados como mecanismos facilitadores de procedimentos gerenciais complexos, é o próprio resultado da pesquisa, pelo qual foi elaborado um *framework* de necessidades informacionais de defesa cibernética, o qual pode ser útil para organizações do setor.

7.3. LIMITAÇÕES DO TRABALHO

O desenvolvimento da pesquisa mostrou muitas possibilidades de desenvolvimento ao mesmo tempo que diversas necessidade de delimitações, simplificações e escolhas metodológicas. Dentre as decisões tomadas em meio a execução dos procedimentos metodológicos, três foram de maior dificuldade e riscos de execução inadequada ou imprecisa. Foram elas: (i) a escolha de quais controles e táticas dos *frameworks* escolhidos correspondiam a que aspecto da teoria adotada de defesa cibernética; (ii) a escolha de quais controles e táticas dos *frameworks*

escolhidos correspondiam a que estágio da consciência situacional de defesa cibernética; (iii) estimativa do grau de maturidade da aplicação das NIP (tarefa d.2) ou da qualidade dos estágios de consciência situacional para lidar com eventos anômalos (tarefas e.2 e e.3).

A dificuldade para lidar com esses elementos era a necessidade de filtrar de modo suficiente deficiências de conhecimento, vieses pessoais ou outro aspecto subjetivo do pesquisador que comprometesse o juízo necessário às escolhas de cada processo. A atenuação desse risco foi contornada se estabelecendo critérios que condicionasse a escolha objetivamente, além da própria experiência vivida pelo pesquisador no objeto da pesquisa e de conhecimentos prévios sobre o tema sedimentados em contexto organizacional.

7.4. SUGESTÕES PARA TRABALHOS FUTUROS

As características da pesquisa permitem diversas possibilidades de extensão, complemento, alternativas, além de outras possibilidades. Dentre essas diversas possibilidades, sugere-se as seguintes:

- Extensão do *framework* de NIP-CS-DC por meio de outros *frameworks* de segurança cibernética ou de ataque cibernético.
- Substituição de um ou dos dois *frameworks* de segurança cibernética ou de ataque cibernético para produzir uma outra versão do *framework* de NIP-CS-DC.
- Estudo de caso da aplicação do *framework* de NIP-CS-DC em ambiente organizacional compatível.
- Extensão do *framework* de NIP-CS-DC, considerando as outras áreas do ciclo do conhecimento de Choo (1998).
- Enriquecer o *framework* com elementos de teoria de superioridade informacional.
- Extensão do *framework* de NIP-CS-DC, considerando aspectos de ambiguidade no ciclo do conhecimento de Choo (1998).

7.5. PALAVRAS FINAIS

Este estudo buscou produzir não só um conhecimento de caráter inovador, como se espera de uma tese de doutoramento, como também procurou gerar um

instrumento de produção de novos conhecimentos. Nesse sentido, a escolha de pesquisa com foco em necessidades informacionais teve especial significado.

Nos ciclos de gestão da informação ou no ciclo conhecimento organizacional, os primeiros passos são dados por meio da descoberta do que se precisa saber, acompanhado de todos os questionamentos complementares que enriquecem a resposta da pergunta “o que é necessário?”.

Assim, aprimorar os instrumentos que aumentam as chances de o uso da informação ser adequado às necessidades humanas, sejam internas ou externas, individuais, coletivas ou organizacionais, é um aspecto potencializador da própria evolução do indivíduo e, em última instância, da sociedade. Um desses instrumentos são os mecanismos de determinação das necessidades informacionais.

Tal qual uma flexa que é disparada para o alvo, a determinação das necessidades informacionais é a seta sem a qual não se pode alcançar o objetivo organizacional. Ainda que exista a possibilidade dessa flexa ser desviada ou encontrar um obstáculo inesperado no trajeto, como se constatou numa das operações estudadas, se ela não for adequadamente construída para, aí sim, ser posicionada com técnica no arco da busca da informação e disparada com destreza para o alvo do uso da informação, não será possível realizar ações de sucesso.

Deste modo, este trabalho de pesquisa é encerrado, sendo posicionado, ao mesmo tempo como um conhecimento que agrega novos conhecimentos aos campos da defesa cibernética, consciência situacional e conhecimento organizacional e como um conhecimento social aplicável em ambientes organizacionais compatíveis com o objeto de estudo.

REFERÊNCIAS

ALBERTS, David S., GARSTKA Jonh J., HAYES, Richard E., SIGNORI, David T. **Understanding information age warfare**. Washington-DC: DoD Command and Control Research Program (CCRP). Washington DC: CCRP Publications, 3 rd printing: 2004. 312 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001:2020.** Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002:2022.** Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005:2023.** Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação. Rio de Janeiro, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27032:** Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética. Rio de Janeiro, 2015.

BARFORD, Paul, DACIER, Marc, DIETTERICH, Thomas G., FREDRIKSON, Matt, GIFFIN, Jon, JAJODIA, Sushil, JHA, Somesh, LI, Jason, LIU, Peng, NING, Peng, OU, Xinming, SONG, Dawn, STRATER, Laura, SWARUP, Vipin, TADDA, George, WANG, Cliff, YEN, Jonh. Cyber SA: Situational Awareness for Cyber Defense. *In*: JAJODIA Sushil, LIU Peng, SWARUP Vipin, WANG Cliff. (Editors). **Cyber Situational Awareness**: Issues and Research. Springer, 2010. p. 3-13.

BEUREN, I. M. **Gerenciamento estratégico da informação**: um recurso estratégico no processo de gestão empresarial. São Paulo: Atlas, 2000.

BORKO, Harold. **Information Science**: What is it? American Documentation, v.19, n.1, p.3-5, Jan. 1968.

BOYD, John Richard. A **Discourse on Winning and Losing**. Montgomery: Air University Press, 2018. 392 p.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 de maio de 2023.

BRASIL, **Decreto n. 6.703**, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em 16/12/2023.

BRASIL. Presidência da República, Gabinete de Segurança Institucional da Presidência da República. Portaria n. 45, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. **Diário Oficial da União:** seção 1**,** Brasília, DF, n. 172, p.2, 09 Set. 2009. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/09/2009&jornal=1&pagina=2&totalArquivos=80. Acesso em: 20 dez.2023.

BRASIL, **Livro Branco de Defesa Nacional**. Brasília, 2012a. Ministério da Defesa. Disponível em < https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 30jul.2018.

BRASIL, **Política Nacional de Defesa**. Brasília, 2012b. Ministério da Defesa. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 30jul.2018.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3389, de 21 de dezembro de 2012. Dispõe sobre a Política Cibernética de Defesa. **Diário Oficial da União:** seção 1**,** Brasília, DF, n. 249, p. 11, 27 Dez. 2012. Disponível em: https://www.jusbrasil.com.br/diarios/44578940/dou-secao-1-27-12-2012-pg-11. Acesso em: 20 dez. 2023.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3010, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/comando_controle/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf/view. Acesso em: 20 dez. 2023.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3010, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas. **Glossário das Forças Armadas** (**MD35-G-01).** Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf/view. Acesso em: 20 dez. 2023.

BRASIL. Exército Brasileiro, Estado-Maior do Exército. Portaria n. 002-EME, de 5 de janeiro de 2015. Aprova o Manual de Campanha Comando e Controle. **Comando e Controle (EB20-MC-10.205)**, Brasília, DF. 2018.

CAMELO, José Ricardo Souza.; CARNEIRO, João Marinonio Enke. A Atuação do Centro de Defesa Cibernética na Copa das Confederações FIFA/2013. *In*: MEDEIROS FILHO, O. (organizador); FERREIRA NETO, W. B.(organizador); GONZALES, S. L. M. (organizador). **Segurança e Defesa Cibernética**: da fronteira física aos muros virtuais. Recife: Editora UFP, 2014. 196 p.

CARDOSO, Alberto M., **Os treze momentos da arte da guerra**: Uma visão brasileira da obra de Sun Tsu. Rio de Janeiro: Editora Record, 2005. 321p.

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética**: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. 2012. Tese (Doutorado em Ciências Militares) – Escola de Estado-Maior do Exército-ECEME, Rio de Janeiro, 2012. p. 203. Disponível em: http://www.eceme.eb.mil.br/images/IMM/producao_cientifica/teses/joao-marinonio-enke-carneiro.pdf. Acesso em: 20 dez. 2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA (CERT.br). **CSIRT FAQ**. São Paulo, 2002. Disponível em: https://www.cert.br/certcc/csirts/csirt_faq-br.html. Acesso em: 20 dez. 2023.

CHOO, Chun Wei. **Information Management for the Inteligent Organization**. Medford, NJ: Information Today, 1998. 272 p.

CHOO, Chun. Wei. **The knowing organization:** How organizations use information to construct meaning, create knowledge and make decisions. New York, NY: Oxford University Press, 1998. 298 p.

CLARKE, Richard Alan.; KNAKE Robert. **Cyber War: The Next Threat to National Security and What to Do About It**. New York: Harper Collins Publishers, 2010. 290 p.

CLAUSEWITZ, Carl V. **Da Guerra.** São Paulo: Editora Universidade de Brasília, 1979. 787 p.

ENDSLEY, Mica. R. Design and evaluation for situation awareness enhancement. *In*: Human Factors Society 32nd Annual Meeting, p. 97-101, 1988, Santa Monica. **Proceedings of the Human Factors Society**. Santa Monica: Human Factors and Ergonomics Society, 1988.

ENDSLEY, Mica R. **Situation awareness in dynamic human decision making:** Theory and measurement. Doctoral Dissertation (Industrial and Systems Engineering) – University of Southern California, Los Angeles, 1990.

ENDSLEY, Mica R.; Bolstad, Cheryl. Human capabilities and limitations in situation awareness. *In*: Combat automation for airborne weapon systems: Manlmachine interface trends and technologies, AGARD-CP-520; p. 19/1-19/10, 1993, Neuilly-

Sur-Seine. **Proceedings of the Human Factors Society**. Neuilly-Sur-Seine: NATO—Advisory Group for Aerospace Research and Development 1993.

ENDSLEY, Mica R. Situation Models: An Avenue to the Modeling of Mental Models. *In*: 14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society, p. 61-64, 2000, San Diego. **Proceedings of the Human Factors Society Annual Meeting**. San Diego: Human Factors and Ergonomics Society 2000.

ENDSLEY, Mica R. Toward a theory of situation awareness in dynamic systems. *In*: **Human Factors Journal**, volume 37(1) p. 32–64, 1995.

ESCOLA SUPERIOR DE GUERRA (Brasil). **Manual básico.** Rio de Janeiro, 2013. 3 v. Disponível em:< https://adesgce.org/wp-content/uploads/2021/05/Manual_Basico_V_I_2009-ADESGCE.pdf >. Acesso em: 12 nov. 2023.

FERNANDES, Jorge H. C. O Espectro de Atuação do Centro de Defesa Cibernética (CDCiber) sob o Enfoque de uma Integração Sistêmica Baseada nos Campos do Poder Nacional. *In*: Gilberto Fernando Gheller; Selma Lúcia de Moura Gonzales; Laerte Peotta de Melo. (Org.). **Amazônia e Atlântico Sul**: desafios e perspectivas para a defesa no Brasil. 1ed.Brasília: IPEA, 2015, v. 1, p. 507-558.

JONHSON, L. **Handbook of Intelligence Studies**. New York: Routledge, 2007. 382 p.)

MARCONI, Marina de A.; Eva M. LAKATOS. **Fundamentos de Metodologia Científica**. São Paulo: Editora Atlas S.A. 2003, 311 p.

MANDARINO Jr, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010. 182 p.

MITRE. MITRE ATT&CK: **Adversarial Tactics, Techniques, and Common Knowledge**. Bedford, MA: MITRE, 2023. Disponível em: https://attack.mitre.org/. Acesso em: 25 jun. 2023.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for improving critical infrastructure cybersecurity**: version 1.1. Gaithersburg, MD: NIST, 2018.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication 800-115**: Technical Guide to Information Security Testing and Assessment. Gaithersburg, MD: NIST, 2008.

OLIVEIRA, Silvio L. **Tratado de Metodologia Científica**: Projetos de Pesquisa, TGI, TCC, Monografias, Dissertações e Teses. São Paulo: Editora Pioneira. 2001, 320 p.

OLIVEIRA, Marcos Aurélio G., PAGLIARI, Graciela C., MARQUES, Adriana A., PORTELA, Lucas S., FERREIRA NETO, Walfredo B. **Guia de Defesa Cibernética na América do Sul**. Recife: Editora UFPE. 2017, 162 p.

ROBREDO, Jaime. **Da Ciência da Informação Revisitada aos Sistemas Humanos de Informação**. Brasília: Thesaurus, 2003. 245 p.

SYAFRIZAL, Melwin, SELAMAT, Siti R., e Zakaria, Nurul A. Analysis of cybersecurity standard and *framework* components. **International Journal of Communication Networks and Information Security** (IJCNIS), 12(3), 2022. Disponível em https://doi.org/10.17762/ijcnis.v12i3.4817

TADDA, George, SALERNO, Jonh S. Cyber SA: Overview of Cyber Situation Awareness. *In*: JAJODIA Sushil, LIU Peng, SWARUP Vipin, WANG Cliff. (Editors). **Cyber Situational Awareness**: Issues and Research. Springer, 2010. p. 15-34.

TAHERDOOST, Hamed. Understanding cybersecurity *frameworks* and information security standards - A Review and Comprehensive Overview. **Electronics**. Basel: MDPI, 2022. Disponível em SSRN: https://ssrn.com/abstract=4178718.

TAYLOR, Robert S. Information Use Environments: *In*: **Progress in Communication Science**. Norwood: Ablex Publishing, 1991. P. 217-54.

VIANNA, Eduardo W. A Segurança Cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável – Rio+20. *In*: NAKAYAMA, Marina K., PIMENTEL, Luiz O., ZIBETI, Fabíola W., ZIEGLER FILHO, João A. (Org). **Pontes para a Segurança Pública**. Florianópolis: FUNJAB, 2013. p. 127-156.

WEICK, Karl E. **Sensemaking in Organizations**. Thousand Oaks: Sage Publication Inc, 1995, 231p.