



ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA  
COORDENADORIA ACADÊMICA  
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

**JAMES DE CASTRO MARTINS**, Ten Cel Av

**A teoria das estruturas organizacionais de Mintzberg e o modelo de Endsley: uma avaliação sobre os níveis de consciência situacional cibernética do Núcleo do Centro de Defesa Cibernética da Aeronáutica no contexto do projeto piloto Campo Grande**

Rio de Janeiro  
2022

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA  
COORDENADORIA ACADÊMICA  
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

**JAMES DE CASTRO MARTINS**, Ten Cel Av

**A teoria das estruturas organizacionais de Mintzberg e o modelo de Endsley: uma avaliação sobre os níveis de consciência situacional cibernética do Núcleo do Centro de Defesa Cibernética da Aeronáutica no contexto do projeto piloto Campo Grande**

Trabalho de conclusão de curso apresentado, como requisito parcial para aprovação, no Curso Avançado de Comando e Estado-Maior da Escola de Comando e Estado-Maior.  
Linha de Pesquisa: Poder Militar.  
Orientador: Heráclito Moreira de Souza.

## **AGRADECIMENTO**

Uma vez Albert Clarke disse que “nas nossas vidas diárias, devemos ver que não é a felicidade que nos faz agradecidos, mas a gratidão é que nos faz felizes.” e, neste momento, a felicidade faz parte dos meus sentimentos. Essa gratidão vem, pela sua suficiência e grandiosidade, de Deus, em nome de Jesus, que é e sempre será o nosso caminho e daqueles que estavam próximos durante a caminhada: minha família, pelo amor e suporte constantes no dia a dia e compreensão pelos diversos momentos distantes; Brigadeiro Intendente Luiz Fernando, pela referência profissional e inspiração dedicada à proposta de estrutura organizacional de defesa cibernética em prol de uma FAB mais eficiente e eficaz; Tenente Coronel Aviador Heráclito, companheiro de outras batalhas, pelo seu tempo e orientações sempre precisos e oportunos, características essenciais ao sucesso deste trabalho; aos amigos Diedrich, Júlio César, Julião e Motta, pelas contribuições e percepções relevantes e adequadas; finalmente, a nossa querida ECEMAR, “Escola de Guerra!”, pela oportunidade e confiança.

Todos por uma Força Aérea Brasileira Forte e Pujante!

“Asas que protegem o País!!”

## RESUMO

O Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAer), no âmbito do Plano Piloto Campo Grande (PPCG), ainda não possui uma estrutura organizacional aderente. Este fato aliado à importância da Consciência Situacional Cibernética (CSC) e às possibilidades oferecidas pela Teoria das Estruturas Organizacionais de Mintzberg subsidiam o objetivo geral desta pesquisa: “avaliar a influência de uma proposta de Estrutura Organizacional de Defesa Cibernética, baseada na Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, durante o processo de implantação do NuCDCAer, no contexto do PPCG.” Para tal, foram realizadas pesquisas exploratória, documental e de campo para, primeiramente, identificar uma proposta de Estrutura Organizacional de Defesa Cibernética, à luz da Teoria de Mintzberg; secundariamente, a concepção de métricas para os níveis de CSC e, finalmente, a estimativa quanto aos níveis de CSC. Como resultados, à luz de Mintzberg, foi identificada a burocracia mecanizada como proposta de estrutura organizacional mais aderente ao NuCDCAer e ao PPCG, onde o COMPREP apoiaria um Grupo de Defesa Cibernética e a BACG auxiliaria um Esquadrão de Defesa Cibernética. Em seguida, foram concebidas métricas para níveis de CSC. Essas métricas envolveram a técnica CS3, no âmbito do modelo de Endsley, aplicadas na proposta de estrutura organizacional identificada e suportada por um framework de CSC e por métricas internas de CSC. Ao final, os níveis de CSC foram estimados e avaliados em relação à esta estrutura, obtendo-se como resultado uma CSC variando entre ligeiramente alta e alta.

**Palavras-chave:** Teoria das Estruturas Organizacionais de Mintzberg; Consciência Situacional Cibernética; Modelo de Endsley; Estrutura Organizacional de Defesa Cibernética.

## ABSTRACT

*The Core of the Aeronautics Cyber Defense Center (NuCDCAer), under the scope of the Campo Grande Pilot Plan (PPCG), has yet to identify an adherent organizational structure. This fact, combined with the importance of Cyber Situational Awareness (CSA) and the possibilities offered by Mintzberg's Theory of Organizational Structures, drives the general objective of this research: to evaluate the influence of a proposal for an Organizational Structure of Cyber Defense based on Mintzberg's Theory of Organizational Structures using Cyber Situational Awareness (CSA) levels as a means of evaluation, during the NuCDCAer implementation process, in the context of the PPCG. To this end, exploratory, documentary, and field research were carried out to identify a proposal for an Organizational Structure of Cyber Defense utilizing Mintzberg's Theory; secondly, design metrics to measure situational awareness levels, and, finally, estimate CSA levels. Results identified mechanized bureaucracy as a proposal for an organization structure more adherent to NuCDCAer and PPCG, where COMPREP assists a Cyber Defense Group and BACG would assist a Cyber Defense Squadron. Additionally, metrics involving the CS3 technique in Endsley's model, were designed to measure CSA levels. As conclusion, the technique as applied in the proposed organizational structure supposed by a CSA framework and internal SSC metrics, revealed that estimated and evaluated CSA levels in relation to a mechanized bureaucracy structure ranged from slightly high to high.*

**Keywords:** *Mintzberg's Theory of Organizational Structures; Cyber Situational Awareness; Endsley's Model; Organizational Structure of Cyber Defense.*

## LISTA DE ILUSTRAÇÕES

Figura 1 – Cinco partes básicas e os mecanismos de coordenação de Mintzberg.....	12
Figura 2 – Síntese da Teoria das Estruturas Organizacionais de Mintzberg para a concepção de uma Estrutura Organizacional.....	13
Figura 3 – Os três níveis de Consciência Situacional do modelo de Endsley.....	14
Figura 4 – Framework apresentado por Tianfield (2016) envolvendo o modelo de Endsley.....	17
Figura 5 – Cinco partes básicas e os cinco mecanismos de coordenação da organização que compõem a Estrutura Organizacional de Defesa Cibernética do NuCDCAer envolvendo o PPCG.....	27
Figura 6 – Percepção dos entrevistados quanto aos níveis de CSC.....	29
Quadro 1 – Exemplos de métricas relacionadas à disponibilidade e à confiabilidade.....	20

## LISTA DE ABREVIATURAS E SIGLAS

BACG	Base Aérea de Campo Grande
CC-SART	<i>Cognitive Compatibility Situation Awareness Rating Technique</i>
CDCAer	Centro de Defesa Cibernética da Aeronáutica
COMAER	Comando da Aeronáutica
COMPREP	Comando de Preparo
CS3	Consciência Situacional – três níveis
CSC	Consciência Situacional Cibernética
CSSA	<i>Cyber Security Situational Awareness</i>
CTIR.AER	Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores do Comando Aeronáutica
DTIC	Divisão de Tecnologia da Informação e Comunicações
EB	Exército Brasileiro
EDC	Esquadrão de Defesa Cibernética
ETIR	Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores
FA	Força(s) Armada(s)
FAB	Força Aérea Brasileira
GDC	Grupo de Defesa Cibernética
HW	<i>Hardware</i>
IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Protection System</i>
NuCDCAer	Núcleo do Centro de Defesa Cibernética da Aeronáutica
OM	Organização Militar
ONG	Organização Não-Governamental
PPCG	Projeto Piloto Campo Grande
REGINT	Regulamento Interno
SAGAT	<i>Situational Awareness Global Assessment Technique</i>
SART	<i>Situational Awareness Rating Technique</i>
SW	<i>Software</i>
TI	Tecnologia da Informação
UFC	Universidade Federal do Ceará

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>9</b>
<b>2</b>	<b>REFERENCIAL TEÓRICO .....</b>	<b>11</b>
<b>2.1</b>	<b>Trabalhos Relacionados .....</b>	<b>15</b>
<b>3</b>	<b>METODOLOGIA.....</b>	<b>21</b>
<b>4</b>	<b>APRESENTAÇÃO DE DADOS E ANÁLISE DE RESULTADOS.....</b>	<b>23</b>
<b>5</b>	<b>CONCLUSÃO.....</b>	<b>31</b>
	<b>REFERÊNCIAS.....</b>	<b>34</b>
	<b>GLOSSÁRIO.....</b>	<b>36</b>
	<b>APÊNDICE A – Questionário para Coleta de Dados.....</b>	<b>37</b>
	<b>ANEXO A – Organograma da Estrutura Organizacional do COMPREP.....</b>	<b>41</b>

## 1 INTRODUÇÃO

A Força Aérea Brasileira - FAB, ao longo dos últimos anos, vem envidando esforços no sentido de melhorar sua capacidade de defesa cibernética e, recentemente, estabeleceu as premissas e as orientações norteadoras para a implantação do Núcleo do Centro de Defesa Cibernética da Aeronáutica – NuCDCAER (BRASIL, 2020b).

Esse processo foi planejado para ser desenvolvido em duas etapas: a primeira, que se encerrou em 30 de junho de 2022, dentre outras ações, incorporou o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores do Comando Aeronáutica - CTIR.AER e sua estrutura de defesa cibernética; e a segunda etapa, com prazo de conclusão em 31 de dezembro de 2023, marcará a ativação do próprio Centro de Defesa Cibernética da Aeronáutica - CDCAER.

Outrossim, voltando-se a outros esforços de reestruturação da FAB, foi apresentado também o Projeto Piloto Campo Grande - PPCG. No ínterim da implantação do PPCG, de acordo com Brasil (2021a), notou-se que apesar da importância dada pela FAB à defesa cibernética e de se buscar “consolidar as modificações na estrutura organizacional do Comando da Aeronáutica - COMAER [...] e finalizar as ações decorrentes do processo de reestruturação organizacional”, o PPCG ainda não contemplou em sua organização uma Estrutura Organizacional de Defesa Cibernética.

Da mesma forma, até agora, não se observou, no processo de implantação do NuCDCAer, conforme Brasil (2020b), uma Estrutura Organizacional de Defesa Cibernética que fosse aderente ao PPCG.

O desenvolvimento de Estruturas Organizacionais de Defesa Cibernética é desafiado pela volatilidade, agressividade, mutabilidade, permeabilidade e transversalidade presentes no espaço cibernético.

Na atual conjuntura mundial, caracterizada por incerteza, mutabilidade e volatilidade das ameaças potenciais, bem como pela presença de novos atores não estatais nos possíveis cenários de conflito, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. (BRASIL, 2014).

Não obstante a esses desafios, a atual Diretriz do Comandante da FAB 2021-2022, conforme Brasil (2021), também considera que as atuais e futuras Estruturas Organizacionais deverão primar pela eficiência e pela eficácia. “Os órgãos centrais de cada Sistema do Comando da Aeronáutica deverão rever suas respectivas normas, atualizando-as, reformulando-as ou

extinguindo-as, a fim de buscar a eficiência e a eficácia das atividades-meio e das atividades-fim da Força.” (BRASIL, 2021b).

Por esse contexto, a Teoria das Estruturas Organizacionais de Mintzberg apresentou-se como uma perspectiva de estudo e investigação. Conforme Aguiar e Martins (2006), a Teoria das Estruturas Organizacionais de Mintzberg é adequadamente aplicada, quando se deseja abordar a realidade da organização objetivando a eficiência e a eficácia de seus processos. Nesse viés, como eventual solução para a ausência de Estrutura Organizacional de Defesa Cibernética apresentada.

Essa ausência, dentre outros efeitos nocivos à Organização, também pode comprometer os níveis de consciência situacional em relação aos objetivos organizacionais (JÚNIOR, 2019). Fato que assevera ainda mais a ausência estrutural supracitada, pois, conforme Brasil (2020b), “o futuro CDCAER deverá possuir a consciência situacional das atividades realizadas no domínio cibernético”, pois as ações de proteção, defesa e ataque cibernéticos são comprometidas pela falta de Consciência Situacional Cibernética – CSC (BRASIL, 2014).

Dessa forma, a falta de uma Estrutura Organizacional de Defesa Cibernética e a análise de sua influência nos níveis de CSC, no contexto supracitado, apontam para a necessidade de pesquisas e estudos que proponham soluções para esse problema.

Destarte, este artigo científico possui como objetivo geral avaliar a influência de uma proposta de Estrutura Organizacional de Defesa Cibernética, baseada na Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, durante o processo de implantação do NuCDCAer, no contexto do PPCG.

Para o atingimento deste objetivo, as seguintes questões norteadoras foram formuladas: qual estrutura organizacional de defesa cibernética, à luz da Teoria das Estruturas Organizacionais de Mintzberg, é mais aderente ao NuCDCAER, no contexto do PPCG?; quais métricas são mais adequadas para se mensurar os níveis de CSC de uma Estrutura Organizacional de Defesa Cibernética?; e quais os níveis de CSC em relação a uma Estrutura Organizacional de Defesa Cibernética, concebida à luz da Teoria das Estruturas Organizacionais de Mintzberg, durante o processo de implantação do NuCDCAER, no contexto do PPCG?

Conducente respectivamente aos seguintes objetivos específicos: identificar, à luz da Teoria das Estruturas Organizacionais de Mintzberg, uma proposta de Estrutura Organizacional de Defesa Cibernética, que seja mais aderente ao NuCDCAER, no contexto do PPCG; conceber métricas que sejam mais adequadas para os níveis de CSC de uma Estrutura Organizacional de Defesa Cibernética; e estimar os níveis de CSC em relação a proposta de Estrutura

Organizacional de Defesa Cibernética, concebida à luz da Teoria das Estruturas Organizacionais de Mintzberg, durante o processo de implantação do NuCDCAER, no contexto do PPCG.

## 2 REFERENCIAL TEÓRICO

Esta seção se propõe a identificar o estado do problema a ser pesquisado sob o aspecto teórico e de outros trabalhos e pesquisas realizados (LAKATOS; MARCONI, 2003).

Nesse contexto, com vistas a oferecer uma melhor compreensão sobre o problema de pesquisa, primeiramente, apresentou-se uma breve fundamentação teórica envolvendo as duas variáveis: Estrutura Organizacional de Defesa Cibernética e CSC. Após, apresentou-se os principais trabalhos encontrados na literatura que abordaram a Teoria de Mintzberg e CSC mais aderentes à construção dos objetivos específicos desta pesquisa.

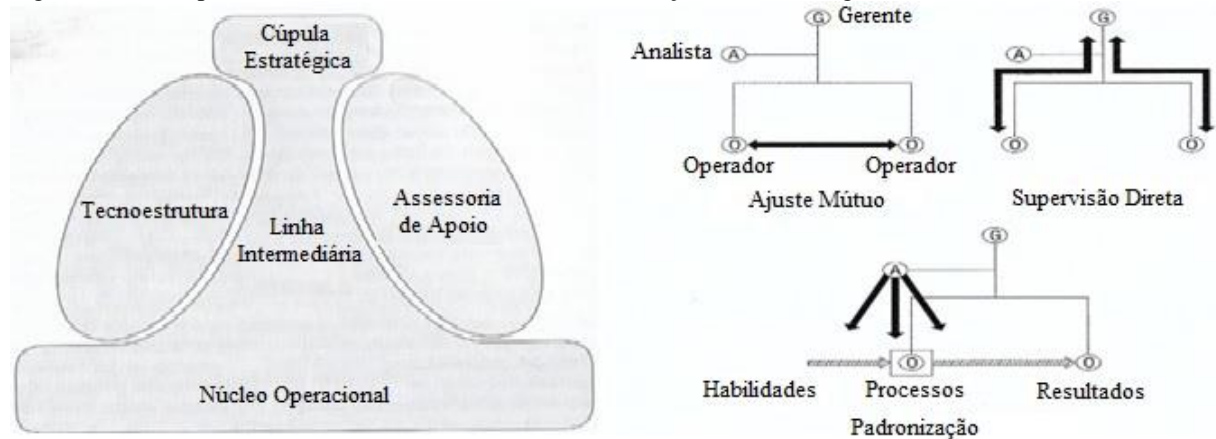
“A estrutura de uma organização pode ser definida simplesmente como a soma total das maneiras pelas quais o trabalho é dividido em tarefas distintas e, depois, como a coordenação é realizada entre essas tarefas.” (MINTZBERG, 2006). Essa estrutura, basicamente, compreende um construto, formado pela identificação das partes básicas de uma organização e de seus mecanismos de coordenação, para a consecução das tarefas contextualizadas pela influência da relação entre os parâmetros de *design* e fatores situacionais.

Mintzberg (2006, p. 22-30) divide uma estrutura organizacional em cinco partes básicas: (a) núcleo operacional – “elementos que executam o trabalho básico diretamente relacionado à fabricação de produtos e à prestação de serviços, sendo considerada a parte que produz os *outputs* essenciais”; (b) cúpula estratégica - “encarregada de assegurar que a organização cumpra sua missão de modo eficiente e eficaz e também que atenda às necessidades dos que a controlam ou que detêm poder sobre ela”; (c) linha intermediária - cadeia de gerentes intermediários que conecta a cúpula estratégica ao núcleo operacional; (d) tecnoestrutura – estrutura composta por analistas responsáveis na adaptação, “transformando a organização para enfrentar as mudanças ambientais e preocupados com o *design* e o funcionamento da estrutura”; e, finalmente, (e) a assessoria de apoio – estrutura de apoio e suporte que se localiza fora do fluxo operacional do trabalho.

Conforme a Teoria das Estruturas Organizacionais, essas partes básicas de uma organização sofrem a influência de cinco mecanismos de coordenação: (a) ajuste mútuo: obtenção da coordenação do trabalho pelo simples processo de comunicação entre os operadores; (b) supervisão direta “assume a coordenação quando existe um responsável pelo

trabalho de outras, passando-lhes instruções e monitorando suas ações; (c) padronização dos resultados: quando na percepção de saídas padronizadas, a coordenação entre as tarefas é predeterminada - ênfase no resultado esperado; (d) padronização dos processos: processos de trabalho são padronizados quando o conteúdo do processo for especificado - ênfase em como o trabalho será realizado; e (e) padronização das habilidades: trabalhadores são contratados por suas habilidades e conhecimentos e, neste caso, padroniza-se o treinamento a ser realizado pelo operador - ênfase nas capacidades necessárias para realizar o trabalho. A Figura 1 ilustra a disposição das cinco partes básicas juntamente com os mecanismos de coordenação.

Figura 1 – Cinco partes básicas e os mecanismos de coordenação de Mintzberg



Fonte: Adaptada de Mintzberg (2006)

Assim, a partir da construção das partes básicas de uma organização e da representação dos mecanismos de coordenação, a proposta de Mintzberg (2006) visa compreender como os fatores situacionais – idade e tamanho, ambiente, sistema técnico e poder – e os parâmetros de *design* - especialização da tarefa, formalização do comportamento, treinamento, agrupamento em unidades, tamanho de unidade, sistemas de planejamento e controle, instrumentos de vínculo, descentralização vertical e descentralização horizontal – se relacionam e indicam qual destas seis estruturas organizacionais básicas - estrutura simples, burocracia mecanizada, burocracia profissional, forma divisionalizada, “adhocracia” e missionária - seria a mais adequada a uma determinada estrutura organizacional ou até mesmo um híbrido em relação a elas.

Mintzberg (2006) define cada uma das estruturas organizacionais da seguinte forma: (a) estrutura simples é caracterizada por possuir poucos assessores de apoio, pouca distinção entre unidades e discreta hierarquia gerencial, divisão do trabalho não rigorosa e comportamento pouco formalizado; (b) burocracia mecanizada: estrutura que predominam as tarefas operacionais rotineiras e altamente especializadas, procedimentos demasiadamente

formalizados no núcleo operacional, proliferação de normas e comunicação rígida em toda a organização; (c) burocracia profissional é caracterizada pelo trabalho operacional estável e complexo, sendo o parâmetro de treinamento amplamente utilizado para se padronizar as habilidades dos profissionais e a doutrinação de forma complementar; (d) forma divisionalizada possui grande atenção no agrupamento por mercado na linha intermediária, ocorrendo assim descentralização do poder de tomada de decisão com o sistema de controle de desempenho bastante desenvolvido, pouca padronização do comportamento e pouco planejamento de ações; (e) “adhocracia” apresenta pouca formalização do comportamento e com especialização do trabalho em sua dimensão horizontal, possuindo o treinamento formal como meio para tal; e (f) missionária: organizações que possuem ênfase em sua ideologia e fazem uso amplo do parâmetro da doutrinação. O poder de tomada de decisão é dividido entre todos os membros e com grande apresentação da descentralização. Há pouca divisão do trabalho e pouca especialização de tarefas.

A Figura 2 apresenta uma síntese das relações apresentadas por Mintzberg (2006) no contexto da Teoria das Estruturas Organizacionais para a concepção de uma proposta de estrutura organizacional, em que, primeiramente, parte-se de uma missão organizacional definida; após a definição das partes básicas juntamente com a construção dos mecanismos de coordenação presentes e, finalmente, após estes construtos, estabelece-se os fatores situacionais/parâmetros de *design* e suas relações conducentes ao tipo de Estrutura Organizacional mais adequada a determinada organização.

Figura 2 – Síntese da Teoria das Estruturas Organizacionais de Mintzberg



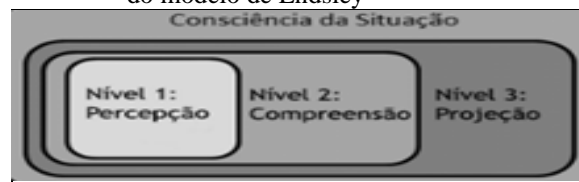
Fonte: Adaptada de Mintzberg (2006)

Já quanto à CSC, o modelo de Endsley apresenta características e conceitos que melhor contribuem quanto à definição de níveis de consciência situacional. Segundo Staton, Chambers e Piggott (2001), o conceito de consciência situacional, ainda que possua diferentes interpretações na literatura, possui como definição mais amplamente utilizada, em função da sua divisão em níveis, o modelo de Endsley, que descreve a consciência situacional como uma

percepção dos elementos no ambiente, dentro de um volume de tempo e espaço, a compreensão de seu significado e a projeção da condição no futuro próximo.

Endsley (1995) apresenta um modelo teórico de consciência da situação que é baseado na importância da tomada de decisão humana dinâmica, que se apresenta em um ambiente multi-domínios. A partir de uma visão descritiva da tomada de decisão, a consciência situacional representa a preocupação presente na operação do sistema. A autora classifica consciência situacional em três níveis: percepção, compreensão e projeção, como apresentado na Figura 3.

Figura 3 – Os três níveis de Consciência Situacional do modelo de Endsley



Fonte: Adaptada de Endsley (1995)

O nível que diz respeito à percepção é relacionado aos fatores críticos no ambiente que são importantes para um determinado tomador de decisão. Esse engloba a valorização e a identificação da dinâmica dos fatores relevantes ao longo do tempo e do espaço, envolvendo seus *status* e atributos, com base nas informações coletadas de diferentes fontes no ambiente.

A compreensão traz o significado dos fatores encontrados no nível de percepção, envolvendo a integração e a correlação de elementos desconexos que precisam ser entendidos no contexto do papel do decisor para a tomada de decisão.

Já o nível de projeção trabalha no entendimento futuro da situação para prever o impacto desses elementos no contexto da visão do tomador de decisão. A projeção gerencia o conhecimento do estado, da dinâmica de fatores e da compreensão de elementos que caracterizam a situação dos níveis 1 e 2 para prever acontecimentos no ambiente dentro de um período.

O modelo de Endsley estabelece uma estrutura dividida em camadas e interdependentes, que constrói uma consciência situacional para apoiar diretamente a tomada de decisão, recebendo informações do ambiente externo e sistemas ligados à organização. Neste sentido, no contexto de um ambiente de defesa cibernética, como é o caso da proposta de Estrutura Organizacional de Defesa Cibernética a qual o NuCDCAer está inserido, percebeu-se a oportunidade de pesquisar sua influência nos níveis de CSC.

## 2.1 Trabalhos Relacionados

Esta subseção traz pesquisas e trabalhos relacionados à Teoria das Estruturas Organizacionais de Mintzberg, de modo a possibilitar a construção de uma proposta de Estrutura Organizacional de Defesa Cibernética para o NuCDCAer e, desse modo, criar um ambiente cuja influência possa ser avaliada em relação aos níveis de CSC, conforme o modelo de Endsley. Da mesma maneira, apresenta pesquisas e trabalhos, envolvendo CSC e o modelo de Endsley, que possibilitem a identificação do estado do problema pesquisado e ofereçam subsídios para a mensuração dos respectivos níveis de CSC.

Aguiar e Martins (2006), sob a ótica da Teoria de Mintzberg, buscaram identificar as implicações que as estruturas organizacionais predominantes nas Organizações Não-Governamentais – ONGs do Estado de São Paulo poderiam causar na gestão estratégica de custos. Os autores constataram que as ONGs apresentaram, como estrutura organizacional predominante, a burocracia profissional.

Para Aguiar e Martins (2006), a gestão estratégica de custos precisa ser consistente com as características organizacionais determinantes da estrutura administrativa para se tornar capaz de maximizar os recursos aplicados em entidades dessa natureza.

A importância e a relevância oferecidos pelos autores, quanto à gestão estratégica de custos nas ONGs de São Paulo, assemelham-se ao valor institucional presente na atual Diretriz do Comandante da FAB, Brasil (2021), quanto à eficiência e à eficácia das atividades-meio e das atividades-fim da Força. No caso desta pesquisa, as atividades de defesa cibernética.

Os autores, primeiramente, trataram de identificar, por meio de entrevistas direcionadas ao pessoal envolvido, as estruturas organizacionais predominantes nas ONGs do Estado de São Paulo para analisar suas implicações no desenvolvimento de sistemas de gestão estratégica de custos. Em seguida, buscaram atender suas premissas de pesquisa: “a gestão estratégica de custos das ONGs deve ser consistente com os parâmetros de *design* e fatores situacionais que determinam a estrutura organizacional de entidades, conforme a teoria de Mintzberg.” (AGUIAR e MARTINS, 2006).

Da mesma forma que Aguiar e Martins (2006), Martin e Guimarães (2018) abordaram a Teoria das Estruturas Organizacionais de Mintzberg, porém no contexto de *Startup*. A proposta foi “analisar de que forma as estruturas organizacionais propostas por Henry Mintzberg poderiam contribuir na *Startup* Target e no processo de tomada de decisão em nível gerencial.”

Segundo esses autores, foi realizada uma pesquisa com os colaboradores da organização por meio de um questionário fechado com o objetivo de analisar as percepções dos mesmos e compreender qual seria o modelo de estrutura organizacional ideal para a Target, constando-se que a estrutura organizacional mais adequada à *Startup*, segundo a Teoria de Mintzberg, foi a “adhocracia”.

Já Moreira *et al.* (2019), ainda no âmbito da Teoria de Mintzberg, buscaram “analisar de que modo a configuração organizacional predominante da Universidade Federal do Ceará - UFC contribuiu na consecução de seus objetivos institucionais.”, concluindo que a configuração organizacional predominante na UFC é um híbrido entre burocracia mecanizada e burocracia profissional. Os autores, dentro da metodologia proposta, utilizaram a “entrevista semiestruturada, cujo roteiro foi elaborado a partir da teoria das configurações de Mintzberg, com foco nos objetivos específicos propostos pelo trabalho.”

Moreira *et al.* (2019), ao contrário dos trabalhos de Aguiar e Martins (2006) e Martin e Guimarães (2018), por meio de uma pesquisa documental realizada na UFC, identificaram o principal mecanismo de coordenação e sua relação com os parâmetros de *design* e fatores situacionais.

Assim, nesse ínterim, percebeu-se que a Teoria das Estruturas Organizacionais de Mintzberg foi aplicada em cada estrutura organizacional, estabelecendo, em cada uma das pesquisas, propostas diferentes em relação à teoria: Aguiar e Martins (2006) identificaram a predominância da burocracia profissional entre as ONGs de São Paulo; Martin e Guimarães (2018) a estrutura organizacional adhocracia para a *startup* Target e, finalmente, Moreira *et al.* (2019) obtiveram uma configuração híbrida entre burocracia mecanizada e burocracia profissional mais adequada à UFC.

Por essas pesquisas, observou-se suporte teórico que colaborou com a identificação de uma proposta de estrutura organizacional, à luz da Teoria das Estruturas Organizacionais de Mintzberg, que fosse mais aderente ao NuCDCAer. Outrossim, além da possibilidade de identificação da estrutura organizacional, Moreira *et al.* (2019) e Martin e Guimarães (2018) acrescentaram, como ferramentas de coleta de dados, a pesquisa documental e entrevistas semiestruturadas e a realização de questionários fechados junto à alta gestão da *startup* Target, respectivamente.

Do outro lado, agora abordando as pesquisas e trabalhos envolvendo o modelo de Endsley para CSC, ainda que não tenham sido encontrados trabalhos diretamente relacionados com a influência de uma Estrutura Organizacional de Defesa Cibernética, à luz da Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, Tianfield (2016), Lötjönen

(2017), Guimarães (2019) e Satuf (2016) abordaram o tema. Essas duas últimas pesquisas foram abordadas por tratarem de métricas para CSC.

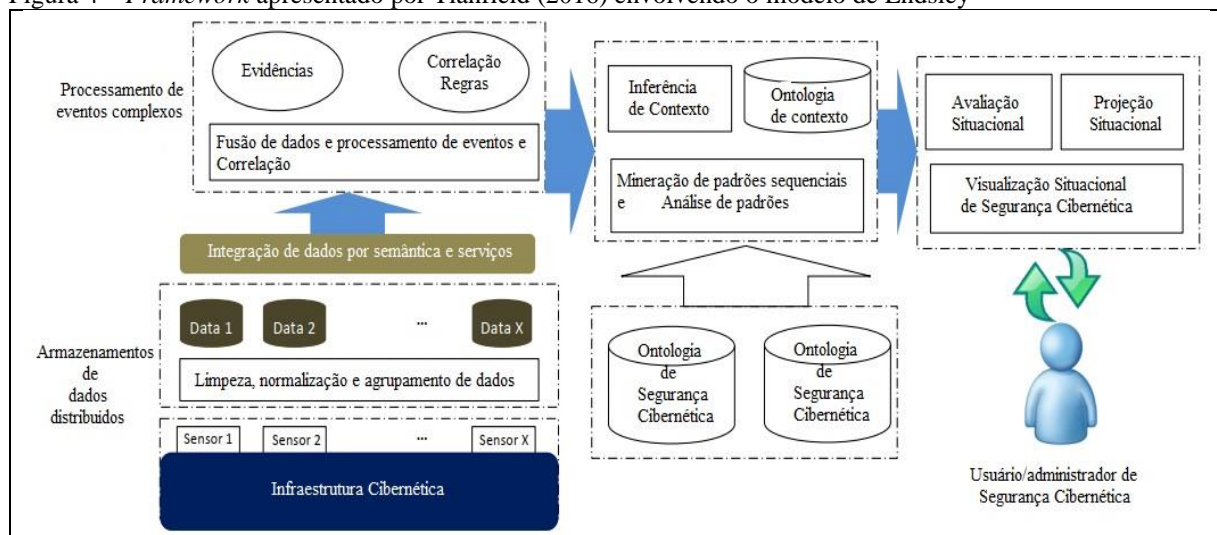
Tianfield (2016) apresentou a concepção e uma estrutura denominada *Cyber Security Situational Awareness - CSSA*, utilizando o modelo proposto por Endsley e envolvendo desde o nível de percepção até o nível de projeção.

De acordo com Tianfield (2016), a percepção envolve a coleta de evidências na infraestrutura cibernética, visando obter o conhecimento dos elementos do ambiente de rede, como alertas relatados por sistemas de detecção de intrusão, *logs de firewall*, relatórios de varredura, oferecendo, assim, informações significativas que servirão de base para a compreensão e projeção; a compreensão envolve a análise de evidências que objetivam identificar o nível exato de ameaça, tipo de ataque e riscos associados.

Ainda conforme o autor, a compreensão utiliza um conjunto de técnicas e procedimentos relevantes para analisar, sintetizar, correlacionar e agregar dados de evidências percebidos na infraestrutura cibernética; e a projeção envolve avaliação preditiva com vistas a abordar futuros incidentes e apoio para a mitigação de ataques cibernéticos. A projeção é a capacidade de fazer previsão ou previsão futura com base no conhecimento extraído da dinâmica dos elementos da rede e da compreensão da situação.

Para Tianfield (2016), a ideia da consciência situacional no campo cibernético foi analisar os entornos da infraestrutura cibernética e criar determinados eventos e visualizações com o objetivo de tomar decisões rápidas e eficientes. Em palavras simples, CSSA poderia ser descrito como a consciência situacional aplicada à segurança cibernética em uma infraestrutura cibernética. A Figura 4 apresenta o *framework* apresentado por Tianfield (2016).

Figura 4 – *Framework* apresentado por Tianfield (2016) envolvendo o modelo de Endsley



Fonte: Adaptada de Tianfield (2016, tradução nossa)

Esse autor afirmou que as “especificações sobre consciência situacional devem ser muito mais amplas do que consciência situacional de segurança, simplesmente porque a infraestrutura cibernética está muito além da rede.”, sugerindo a importância de uma estrutura organizacional por trás deste *framework*.

Já Lötjönen (2017) propôs a criação de requisitos para sistemas de CSC. Esses sistemas foram projetados para serem utilizados em exercícios de segurança cibernética por equipes responsáveis pela defesa de ambientes cibernéticos. Similar a Tianfield (2016), o autor explicou em sua tese que existe “uma clara necessidade de sistemas que reúnam informações para que o especialista em incidentes possa apoiar mais rapidamente a tomada de decisões.”

Os sistemas de CSC foram definidos por Lötjönen (2017), conforme o modelo de Endsley, onde o nível percepção significa como a equipe/indivíduo percebe o *status*, os atributos e a dinâmica dos elementos relevantes para alcançar a consciência situacional, por exemplo: alertas em sistemas defensivos, como *firewalls* ou sistemas de detecção/proteção contra intrusão IDS/IPS.

Ainda conforme esse autor, o nível compreensão trata das possibilidades de correlações e entendimentos possíveis a serem realizados com os dados e informações gerados no primeiro nível; e o nível projeção trata da identificação da urgência e criticidade, o mais rapidamente possível, com base nos níveis anteriores, com a formação de uma massa crítica de conhecimento que apoie a tomada de decisão.

Nesse ambiente, conforme o autor, em exercícios de segurança cibernética existe um padrão para a definição das equipes, sendo as mesmas divididas, primariamente, nas seguintes cores: branca, vermelha e azul. A equipe branca controlaria o exercício, o time vermelho se comportaria como o atacante e o time azul ficaria responsável pela defesa. Alguns exercícios, contam também com a equipe verde, responsável pelas questões técnicas e administrativas.

No que diz respeito ao *Blue Team*, foco da pesquisa de Lötjönen (2017), as informações que as equipes precisariam são apresentadas em sistemas de CSC. Lötjönen (2017) identificou que um sistema de CSC deveria possuir as seguintes classes de requisitos: incidentes cibernéticos, usabilidade, automação, visualização, tratamento de dados, formação da equipe azul, dentre outros.

Observando a pesquisa anterior, os requisitos apresentados por Lötjönen (2017) apoiaram a estrutura criada por Tianfield (2016), com exceção dos requisitos para as equipes de defesa cibernética, isto é, *Blue Team*, que se relacionadas a esta pesquisa, participariam da formação do NuCDAer.

Por último, Guimarães (2019), da mesma forma que Tianfield (2016) e Lötjönen (2017), também utilizou o modelo de Endsley para definir CSC, porém trouxe ênfase para ações ofensivas de ataque cibernético. Segundo Guimarães (2019), “[...] o desenvolvimento de uma CSC tornou-se fundamental para o processo de tomada de decisão sobre as ações ofensivas e defensivas de guerra cibernética.”

A pesquisa de Guimarães (2019) propôs estabelecer “métricas e indicadores que representassem as características quantitativas da condição de proteção de um espaço cibernético, categorizadas em proteção de perímetro, cobertura e disponibilidade/confiabilidade” e que fossem relevantes para a modelagem do processo de CSC.

O processo de CSC, pesquisado por Guimarães (2019), se baseia no modelo de Endsley - percepção, compreensão e projeção. Guimarães (2019) não apresentou uma estrutura de CSC, como o CSSA, porém, por meio de um modelo “mental”, estabeleceu condições de medição para os próprios níveis de CSC.

Esse modelo “mental” considerou o trabalho de Paul e Whitley (2013), que foi baseado em questões a serem respondidas, durante o curso de um evento de segurança de rede para direcionamento de uma CSC. O modelo foi composto por uma taxonomia de questões centradas no usuário, sendo divididas em duas categorias: detecção de eventos e orientação do evento.

Guimarães (2019) considerou que o espaço cibernético a ser protegido deve possuir três áreas basilares: rede externa, composta pela Internet; rede desmilitarizada, na qual estão disponibilizados os serviços de rede externa e interna com seus respectivos sensores de proteção de perímetro (*antispam, firewall e Intrusion Prevention System - IPS*) e área do antivírus.

Para isso, foram estabelecidas três categorias de métricas para a defesa: métricas de proteção de perímetro, métricas de cobertura e métricas de disponibilidade e confiabilidade. O Quadro 1 apresenta exemplos de métricas apresentadas por Guimarães (2019).

As métricas de proteção de perímetro visam compreender o risco de incidentes por ameaças externas ao espaço cibernético de interesse, medindo a efetividade dos principais sistemas de proteção da borda da rede interna (*firewall*, sistema de prevenção de intrusão e sistema *antispam*) e proteção de *host* (*software* antivírus); as métricas de cobertura buscam entender a extensão e a eficácia dos sistemas de gerenciamento de configuração, correção e vulnerabilidade, caracterizando o alcance da política de segurança adotada pela instituição; e as métricas de disponibilidade e a confiabilidade, [...], destinam-se a entender a resistência dos sistemas, considerados críticos, às falhas de hardware, software e energia, cujo objetivo é a disponibilidade dos serviços durante o maior tempo possível. (GUIMARÃES, 2019).

Quadro 1 – Exemplos de métricas relacionadas à disponibilidade e à confiabilidade

<b>Disponibilidade e Confiabilidade</b>	
<b>Métrica</b>	<b>Propósito</b>
Tempo total de disponibilidade dos servidores críticos durante o período de medição.	Estabelecer um <i>baseline</i> de disponibilidade dos servidores críticos.
Tempo de indisponibilidade planejada dos servidores críticos durante o período <i>p</i> de medição.	Estabelecer um <i>baseline</i> de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
<b>Indicador de Desempenho</b>	<b>Propósito</b>
Índice de disponibilidade dos servidores críticos durante o período de medição	Identificar o nível de disponibilidade dos servidores críticos.
Índice de indisponibilidade planejada dos servidores críticos durante o período <i>p</i> de medição.	Identificar o nível de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.

Fonte: Adaptado de Guimarães (2019)

De acordo com Guimarães (2019), a medição dos níveis de CSC foi baseada na percepção do próprio analista de segurança cibernética. Entretanto, conforme especificou Lötjönen (2017), existe uma equipe, denominada *Blue Team*, responsável pela estrutura de defesa. Ainda assim, ambas as pesquisas, apesar de valorizarem a importância de CSC, não trataram da influência da estrutura organizacional nos níveis de CSC.

Finalizando o arcabouço teórico, o trabalho de Satuf (2016) sugeriu complementar as pesquisas anteriores envolvendo consciência situacional, principalmente quanto ao trabalho de Guimarães (2019). Apesar de não ser específico em relação à CSC, o autor apresentou técnicas usadas para medir consciência situacional, que incluem abordagens de avaliação objetivas e subjetivas.

Dentre as principais métricas para consciência situacional, apresentadas por Satuf (2016), a métrica Consciência Situacional – três níveis ou CS3 se mostrou mais adequada ao escopo desta pesquisa. Segundo Satuf (2016), foram propostas, para avaliação da interface, perguntas sobre os três níveis de consciência situacional. Nessa técnica, as perguntas foram também subjetivas e autodeclaratória, abordando os mesmos três níveis de consciência situacional apresentados no modelo de Endsley: percepção, compreensão e projeção.

Ainda segundo o autor, as questões inseridas na técnica CS3 pretenderam estimar o “quanto o operador concordaria que uma dada interface ajudaria na percepção de alarmes e na percepção de variáveis relevantes, o quanto ajudaria na compreensão da situação e na capacidade de prever a evolução do processo.”

Percepção 1) A interface utilizada ajuda a perceber cada nova ativação de alarme. 2) A interface ajuda a perceber os valores das variáveis relevantes em relação aos alarmes ativos. Compreensão 3) A interface ajuda a entender o significado de cada alarme (as causas do alarme e a qual anomalia o alarme se refere). Projeção 4) A interface utilizada ajuda a prever a evolução do processo (normalização da situação ou seu agravamento). (SATUF, 2016).

Dessa forma, após contextualizar o problema de pesquisa e apresentar o estágio atual de conhecimento acerca da questão a ser resolvida, bem como as contribuições proporcionadas por investigações já realizadas, passou-se a tratar da metodologia adotada na condução desta pesquisa (GIL, 2022).

### 3 METODOLOGIA

Nesta seção, foram descritos os procedimentos metodológicos adotados que viabilizaram a consecução do objetivo geral deste artigo científico.

Quanto aos métodos empregados, foi utilizada a pesquisa bibliográfica envolvendo a Teoria das Estruturas Organizacionais de Mintzberg, o modelo de Endsley e trabalhos relacionados; a pesquisa documental envolvendo o NuCDCAer e legislações da FAB, assim como normas relacionadas à defesa cibernética nas Forças Armadas - FA; e a pesquisa de campo com o efetivo do NuCDCAer para a realização das medições de CSC necessárias.

Para a avaliação da influência da proposta de Estrutura Organizacional de Defesa Cibernética, à luz da Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, além desta teoria, foi utilizado o modelo de Endsley e assim, limitado ao processo de implantação do NuCDCAER e no âmbito do PPCG, os níveis de CSC do próprio Núcleo foram estimados e avaliados. Este objetivo geral foi dividido em três objetivos específicos.

O primeiro objetivo específico - identificar, à luz da Teoria das Estruturas Organizacionais de Mintzberg, uma proposta de Estrutura Organizacional de Defesa Cibernética, que seja mais aderente ao NuCDCAER, no contexto do PPCG, foi alcançado por meio de pesquisa bibliográfica envolvendo esta teoria e de pesquisa documental, conforme apoiado por Moreira *et al.* (2019), envolvendo as diretrizes do Comando da FAB, estruturas organizacionais do COMAER, do NuCDCAer, do PPCG e da doutrina e manual militar de defesa cibernética do Exército Brasileiro - EB.

O processo de construção do objetivo específico nº 1 foi limitado à identificação da “Missão da Organização”, das partes básicas e dos mecanismos de coordenação relacionados ao NuCDCAer, no contexto do PPCG, pois o Núcleo ainda não possui uma estrutura organizacional envolvendo este Projeto.

Ainda como fator limitante desta pesquisa, as atividades de defesa cibernética se concentraram na atividade-fim e não na atividade-meio, i.e., no contexto das OM apoiadas pela BACG, conforme premissas estabelecidas na Diretriz do Comandante 2021-2022, de acordo

com Brasil (2021), cujo detalhamento restringiu-se à identificação apenas de cada parte básica sem o devido aprofundamento interior a cada uma delas.

O segundo objetivo específico desta pesquisa - conceber métricas para os níveis de CSC relacionados à proposta de Estrutura Organizacional de Defesa Cibernética – envolveu a adaptação e a aplicação da técnica CS3, apresentada por Satuf (2016), juntamente com as considerações apontadas por Tianfield (2016), Lötjönen (2017) e Guimarães (2019).

Nesse caso, a adaptação da técnica CS3 levou em consideração o trabalho de Lötjönen (2017), que tratou de CSC, no contexto do modelo de Endsley, em relação a uma Estrutura Organizacional de Defesa Cibernética.

A técnica CS3, proposta por Satuf (2016), foi adaptada para envolver a proposta de Estrutura Organizacional de Defesa Cibernética concebida anteriormente. Assim, os níveis de consciência situacional, propostos no modelo de Endsley: percepção, compreensão e projeção, consideraram como “interface” a “Estrutura Organizacional de Defesa Cibernética”.

Quanto à percepção - a) A Estrutura Organizacional de Defesa Cibernética utilizada ajuda a perceber cada nova ativação de alarme. b) A Estrutura Organizacional de Defesa Cibernética ajuda a perceber os valores das variáveis relevantes em relação aos alarmes ativos; quanto à compreensão - c) A Estrutura Organizacional de Defesa Cibernética ajuda a entender o significado de cada alarme (as causas do alarme e a qual anomalia o alarme se refere); e em relação à projeção - d) A Estrutura Organizacional de Defesa Cibernética utilizada ajuda a prever a evolução à situação de normalização, i.e., ataque cibernético mitigado.

Já quanto ao objetivo específico nº 3, estimar os níveis de CSC em relação a proposta de Estrutura Organizacional de Defesa Cibernética, à luz da Teoria das Estruturas Organizacionais de Mintzberg, durante o processo de implantação do NuCDCAER, no contexto do PPCG, foi realizada uma pesquisa de campo no NuCDCAer.

Nesse desiderato, conforme apoiado por Martin e Guimarães (2018) e Moreira *et al.* (2019), foram realizadas entrevistas com a alta gestão do NuCDCAer, ou seja, Chefe e Chefe da Divisão de Operações, de acordo com as métricas concebidas anteriormente.

No contexto das entrevistas, vide Apêndice A, de acordo com as perguntas abordadas e adaptadas da técnica CS3, conforme Satuf (2016, pp. 143-144), cada um respondeu conforme sua percepção quanto à proposta de Estrutura Organizacional de Defesa Cibernética identificada acrescida das considerações de Tianfield (2016) e Guimarães (2019) quanto à CSC.

Após cada pergunta, recebeu-se uma resposta na escala de 1 a 5, onde “1” representou “discordo fortemente” e “5” representou “concordo fortemente”, conforme a concepção das métricas para os níveis de CSC de uma Estrutura Organizacional de Defesa Cibernética.

Ao final, estas estimativas ofereceram condições para a avaliação da influência da proposta de Estrutura Organizacional de Defesa Cibernética nos níveis de CSC, no período e contexto apresentados anteriormente.

Circunstâncias essas cujos valores foram avaliados conforme as seguintes comparações em relação à escala supracitada: “1 – discordo fortemente” significando “CSC baixa”; “2 – tendo a discorda ou discordo parcialmente” significando “CSC ligeiramente baixa”; “3 – neutro” significando “CSC neutra”; “4 – tendo a concorda ou concordo parcialmente” em “CSC ligeiramente alta” e “5 – concordo fortemente” equivalente a “CSC alta”.

Sendo assim, o resultado da aplicação desta metodologia foi apresentado e analisado na próxima seção.

#### **4 APRESENTAÇÃO DE DADOS E ANÁLISE DE RESULTADOS**

Esta seção aborda a construção de cada objetivo específico com consequente construção do objetivo geral. Inicialmente, a Estrutura Organizacional de Defesa Cibernética proposta foi identificada à luz da Teoria das Estruturas Organizacionais de Mintzberg; em seguida, foram concebidas métricas para os respectivos níveis de CSC; e, ao final, após estimados os níveis de CSC em relação a proposta de Estrutura Organizacional de Defesa Cibernética, foi realizada uma avaliação em relação ao objetivo geral.

Inicialmente, quanto à identificação de uma proposta de Estrutura Organizacional de Defesa Cibernética para o NuCDCAer, no contexto do PPCG, delimitada pela missão, pelas partes básicas e pelos mecanismos de coordenação, conforme citados na seção anterior, as definições apresentadas por Mintzberg (2006) foram utilizadas em conjunto com as principais legislações internas à FAB, as quais dizem respeito ao tema.

A partir da definição da missão da organização, Mintzberg (2006) apresentou cinco partes básicas e cinco mecanismos de coordenação, respectivamente representados nos seguintes grupos: (a) núcleo operacional, cúpula estratégica, linha intermediária, tecnoestrutura e assessoria de apoio; e (b) ajuste mútuo, supervisão direta, padronização das saídas, padronização das habilidades e padronização dos processos.

A missão da organização teve por base a própria missão-síntese da FAB: “Manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da Pátria”. Assim, no contexto da Ação de Defesa Cibernética, prevista em Brasil (2020a), considerou-se a missão

da Base Aérea de Campo Grande<sup>1</sup>, como referência interna ao PPCG, “[...] planejar, coordenar, executar e controlar as atividades administrativas de apoio necessárias ao funcionamento das Organizações Militares em sua área de atuação.” para balizar a estrutura organizacional do NuCDCAer, i.e., planejar, coordenar, executar e controlar as atividades administrativas que defendam as OM subordinadas à BACG de ataques cibernéticos, que venham a comprometer suas missões.

Quanto às partes básicas da organização, iniciando pelo núcleo operacional, Brasil (2021), juntamente com Brasil (2017) e Brasil (2021c) ofereceram subsídios documentais que apoiaram a criação de um “Esquadrão<sup>2</sup> de Defesa Cibernética – EDC”.

Os princípios da eficiência e da eficácia, juntamente com a necessidade de melhorar a sinergia entre as atividades operacionais (OM apoiadas pela BACG) e administrativas, ambas orientadas pela Diretriz de Comando 2021-2022 e o aproveitamento da própria estrutura de Tecnologia da Informação - TI adotada pela BACG, conforme o REGINT da BACG, de acordo com Brasil (2021c), formaram a base para a criação do EDC.

O EDC seria composto pelas principais capacidades de defesa cibernética, conforme Brasil (2017), i.e., gestão de riscos, consciência situacional, defesa ativa, pronta-resposta, forense digital, teste de artefatos cibernéticos, conformidade<sup>3</sup> de Sistemas de TI e gestão de incidentes de redes.

Toda essa estrutura, próxima ao dia a dia das OM subordinadas à BACG, conforme Anexo A, traria agilidade com conducente eficácia às tarefas de defesa cibernética, conforme defendido por Tianfield (2016) quanto à CSC.

Segundo Mintzberg (2006), esses foram os elementos que executaram o trabalho básico diretamente relacionado à prestação de serviços para a produção dos *outputs* essenciais, i.e., aqueles serviços diretamente relacionados à defesa cibernética.

Já quanto à cúpula estratégica, conforme Mintzberg (2006), responsável por assegurar que a organização cumprisse sua missão, de modo eficiente e eficaz, e que atendesse suas necessidades internas e externas, temos o próprio NuCDCAer.

---

<sup>1</sup> A missão da BACG considerada para estes fins acadêmicos foi a relacionada ao último Regimento Interno da OM, que atualmente está revogado.

<sup>2</sup> Adotado por adequação à cultura organizacional da Força Aérea Brasileira.

<sup>3</sup> A conformidade, por abranger a aplicação de políticas de segurança cibernética, substituiu as tarefas de Controle de Acesso, Proteção das comunicações, Emprego de Criptografia, Implementação de controles de segurança, Segurança Física e Gestão da Continuidade da Missão e Recuperação de Desastres.

O NuCDCAer, conforme Brasil (2020b), dentre suas responsabilidades estratégicas, teriam o planejamento e a gestão da ação de defesa cibernética do Comando da Aeronáutica – COMAER e o planejamento, a programação e a coordenação das ações de proteção cibernética.

Ainda no grupo das partes básicas, tem-se a linha intermediária. Mintzberg (2006) tratou desta parte como um ponto mediano localizado entre a cúpula estratégia e o núcleo operacional. A organização necessitaria dessa cadeia completa de gerentes de linha intermediária, na extensão de seu porte e conforme sua confiança na supervisão direta para coordenação.

Nessa hierarquia, o gerente de linha intermediária desempenha várias tarefas no fluxo de supervisão direta acima e abaixo dele. Coleta informações de “feedback” sobre o desempenho de sua unidade e transfere algumas delas aos gerentes acima, [...]. Também intervém no fluxo de decisões. Fluem para cima os problemas da unidade, as propostas de mudança e as decisões que requerem autorização. (MINTZBERG, 2006, pp.26).

Por esse contexto, o Comando de Preparo – COMPREP, ainda de acordo com o Anexo A, possibilitou esta gerência intermediária entre a BACG e o NuCDCAer, especificamente na figura de um Grupo<sup>4</sup> de Defesa Cibernética - GDC. Conforme Brasil (2018), o COMPREP tem por finalidade preparar os meios de Força Aérea sob sua responsabilidade e, neste sentido, conforme o artigo 34, dentre outros: realizar a governança dos processos relacionados ao preparo dos meios de Força Aérea sob sua responsabilidade.

Assim, de acordo com as características institucionais do COMPREP, previstas em Brasil (2018), à luz da teoria de Mintzberg, o GDC intermediaria a relação de supervisão direta do NuCDCAer no EDC para a defesa cibernética das OM subordinadas à BACG, de acordo com os interesses operacionais do COMPREP.

A tecnoestrutura foi definida por Mintzberg (2006, pp. 26 e 27) como a parte básica na qual seriam encontrados analistas de controle, membros que estão a serviço da organização para afetar o trabalho de outros membros efetivando certas maneiras de padronização. Não fazendo parte do fluxo operacional, podem estar inseridos no desenho, planejamento, mudança ou treinamento das pessoas que executam o trabalho, visando tornar este trabalho mais eficaz.

Conforme Mintzberg (2006), pode-se distinguir três tipos de analistas de controle quanto às formas de padronização: (a) analistas de sistemas e métodos, que padronizariam os processos de trabalho; (b) analistas de planejamento e controle, que padronizariam as saídas; e (c) analistas de pessoas, que padronizariam as habilidades dos trabalhadores envolvidos nos processos operacionais.

---

<sup>4</sup> Da mesma forma que a nomenclatura “Esquadrão”, este termo foi adotado tendo em vista o ambiente de Força Aérea e sua posição hierarquia em relação ao Esquadrão, ou seja, um Grupo pode ser constituído por um ou mais Esquadrões.

Assim, da mesma forma que a linha intermediária, conforme Brasil (2018), percebeu-se a interseção nas responsabilidades do COMPREP, especificamente do GDC, com a necessidade de analistas de controle vocacionados para a padronização das saídas efetivadas pelo núcleo operacional, i.e., EDC sediado na BACG, uma vez que diz respeito diretamente à disponibilidade de seus meios aeroespaciais, por exemplo. Já quanto à padronização dos processos e das habilidades, estes dizem mais respeito ao próprio NuCDCAer.

São responsabilidades estratégicas do NuCDCAer: (a) planejamento, gerenciamento da capacitação e gestão da Ação de Defesa Cibernética do COMAER; [...]; (d) definição dos normativos sistêmicos relacionados à cibernética; [...]; (g) estabelecimento das linhas de pesquisa da área de cibernética e criptografia. (BRASIL, 2020b).

Finalmente, a última parte básica, proposta pela Teoria de Mintzberg (2006), diz respeito à assessoria de apoio, que conforme o autor, tratou daquelas unidades especializadas que existiriam para prover o apoio à organização, porém estariam fora do seu fluxo de trabalho operacional. Neste sentido, a pesquisa documental trouxe principalmente o próprio Regimento Interno da BACG, de acordo com Brasil (2021c). Considerando o EDC situado no interior da BACG, ter-se-ia a Divisão de Tecnologia da Informação e Comunicações - DTIC, que possui as seguintes responsabilidades: “coordenar e executar as atividades técnicas relacionadas à segurança das redes internas de TI e Comunicações, em coordenação com a assessoria de inteligência, a fim de minimizar os efeitos de ataques cibernéticos.” (BRASIL, 2021c).

Dessa maneira, a DTIC proveria ao EDC os meios necessários para que o Esquadrão cumpra sua missão de defender as OM sediadas na BACG de ataques cibernéticos. Dentre estes meios necessários, *software* - SW e *hardware* - HW, por exemplo, para detecção de *malware* e para a realização da tarefa de gestão de risco e incidentes cibernéticos.

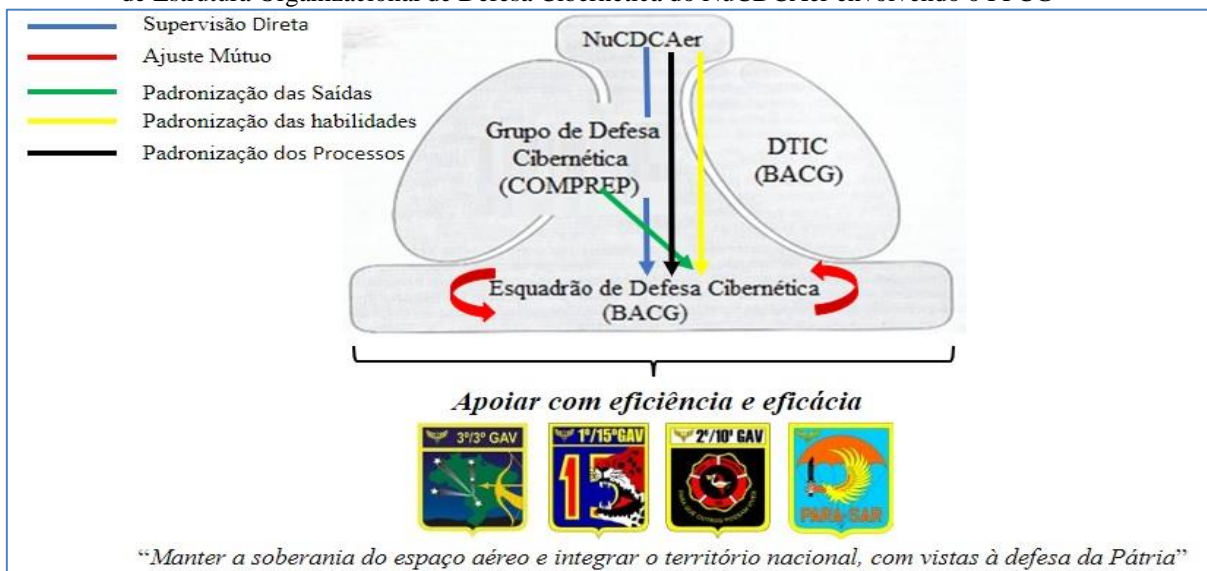
A Figura 5 apresenta a proposta de Estrutura Organizacional de Defesa Cibernética do NuCDCAer no contexto do PPCG com as cinco partes básicas e os mecanismos de coordenação. O NuCDCAer representando a cúpula estratégica, o Grupo de Defesa Cibernética (COMPREP) representando a linha intermediária juntamente com a tecnoestrutura e a DTIC (BACG) estaria relacionada à assessoria de apoio. Esse conjunto existindo para apoiar, conforme Brasil (2021), a atividade-fim com eficiência e eficácia.

Quanto aos mecanismos de coordenação, dadas as devidas considerações sobre as partes básicas, evidenciou-se a supervisão direta entre o NuCDCAer e o EDC com a respectiva intermediação do COMPREP, na figura do GDC. O ajuste mútuo surgindo pela coordenação realizada entre as células internas ao EDC. Já em relação aos tipos de padronização, habilidades e processos mostraram-se mais aderentes ao NuCDCAer e a padronização das saídas ofereceu mais coerência sendo realizada pelo GDF.

Ainda que não possibilitando identificar as respectivas dimensões de cada parte básica, assim como o grau de influência de cada mecanismo de coordenação, condições que viabilizariam o estabelecimento das relações entre os parâmetros de *design* e fatores situacionais, a proposta de Estrutura Organizacional de Defesa Cibernética identificada sugeriu a predominância da burocracia mecanizada, uma vez que o ajuste mútuo previsto no núcleo operacional, i.e., EDC, entre suas células seria adequada e suficiente para a principal saída – defesa cibernética das OM sediadas na BACG.

Por esse arcabouço, a Figura 5 sintetiza a conclusão do objetivo nº 1, onde a proposta de Estrutura Organizacional de Defesa Cibernética do NuCDCAer, envolvendo o PPCG, foi identificada. Sua base, no contexto da missão, guardou relação com a Diretriz do Comandante da FAB 2021-2022, conforme Brasil (2021), a missão da BACG, de acordo com Brasil (2021c) e a própria missão da FAB.

Figura 5 – Cinco partes básicas e os cinco mecanismos de coordenação da organização que compõem a proposta de Estrutura Organizacional de Defesa Cibernética do NuCDCAer envolvendo o PPCG



Fonte: O autor

Já quanto à concepção de métricas mais adequadas para os níveis de CSC de uma Estrutura Organizacional de Defesa Cibernética, a adaptação da técnica CS3 para a medição de CSC, apresentada por Satuf (2016), considerou a pesquisa de Lötjönen (2017), sendo os níveis de CS presentes no modelo Endsley - percepção, compreensão e projeção - especificados para medirem CSC.

Assim, o nível de percepção mensurou “como uma Estrutura Organizacional de Defesa Cibernética percebe o *status*, os atributos e a dinâmica de elementos relevantes para alcançar a consciência situacional”; a compreensão tratou das possibilidades de correlações e entendimentos possíveis a serem realizados com os dados e informações gerados no primeiro

nível; e o nível projeção tratou da identificação da urgência e criticidade com base nos níveis anteriores, com a formação de uma massa crítica de conhecimento que apoie a tomada de decisão.

Já Tianfield (2016) e Guimarães (2019) contribuíram com a concepção dessas métricas, por meio das estruturas internas que esta organização deve possuir para que a mesma tenha um ambiente mensurável quanto aos níveis de CSC.

O *framework* proposto por Tianfield (2016) apoiaria a criação de eventos e visualizações, que seriam estabelecidos pelas métricas e pelos indicadores apontados por Guimarães (2019). Especificamente, o *framework* de Tianfield (2016) envolveria o ambiente protegido pelo EDC na infraestrutura da BACG, o GDC no COMPREP e o próprio NuCDCAer. Esses dois últimos absorveriam as métricas e os indicadores apresentados por Guimarães (2019).

Dessa forma, por meio da percepção da alta gestão do NuCDCAer quanto à proposta de Estrutura Organizacional de Defesa Cibernética concebida nos contextos de Tianfield (2016) e Guimarães (2019), as seguintes perguntas foram respondidas para se estimar e avaliar os níveis de CSC quanto à percepção, compreensão e projeção:

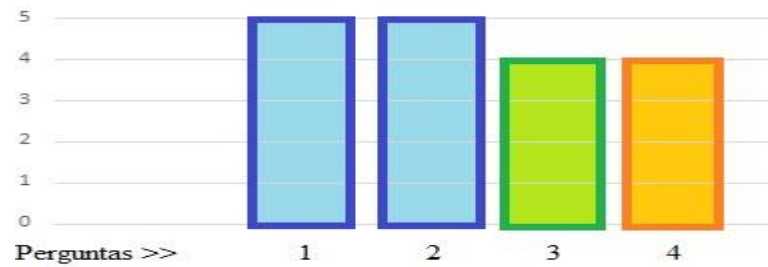
A Percepção - a) A Estrutura Organizacional de Defesa Cibernética utilizada ajuda a perceber cada nova ativação de alarme dedicado a incidentes cibernéticos. b) A Estrutura Organizacional de Defesa Cibernética ajuda a perceber os valores das variáveis relevantes em relação aos alarmes ativos dedicados a incidentes cibernéticos.

A compreensão - c) A Estrutura Organizacional de Defesa Cibernética ajuda a entender o significado de cada alarme (as causas do alarme e a qual anomalia o alarme se refere); e quanto à projeção - d) A Estrutura Organizacional de Defesa Cibernética utilizada ajuda a prever a evolução da normalização do ataque cibernético.

Cada resposta recebeu a seguinte graduação: 1 = discordo fortemente, 2 = tendo a discordar ou discordo parcialmente, 3 = neutro, 4 = tendo a concordar ou concordo parcialmente e 5 = concordo fortemente.

Dessa maneira, ao final da aplicação das métricas supracitadas propostas, pode-se estimar e avaliar os níveis de CSC. Sendo assim, após a realização das respectivas entrevistas ao Chefe do NuCDCAer e ao Chefe da Divisão de Operações do NuCDCAer, representantes da alta gestão do NuCDCAer, quanto aos níveis de CSC em relação a proposta de Estrutura Organizacional de Defesa Cibernética, estimou-se e avaliou-se os seguintes resultados, conforme a Figura 6.

Figura 6 – Percepção dos entrevistados quanto aos níveis de CSC



Fonte: O autor

Cada respondente, de acordo com as perguntas abordadas e adaptadas da técnica CS3, conforme Satuf (2016, pp. 143-144), respondeu de acordo com a percepção apresentada quanto à proposta de Estrutura Organizacional de Defesa Cibernética identificada, acrescida das considerações de Tianfield (2016) e Guimarães (2019) quanto à CSC. Finalmente, cada pergunta recebeu uma escala de 1 a 5, onde “1” representou “discordo fortemente” e “5” representou “concordo fortemente”.

Da entrevista com o Chefe do NuCDCAer, quanto às perguntas “1” e “2”, que trataram do nível percepção de CSC, obteve-se as seguintes respostas: “concordo fortemente” com os seguintes comentários, respectivamente: “Apesar de as percepções dos tráfegos anômalos necessitarem de aparelhamento tecnológico disponível hoje (2022) apenas no CTIR, e o GDC ter uma possível função comparada a uma ETIR, entende-se que a proximidade das OM da BACG, por meio do EDC, contribuiria de forma promissora.” e “Entende-se que as funções poderiam ser assumidas por uma sequência processual de uma ETIR, todavia deve-se considerar, também, a proximidade das OM da BACG.”

Ainda quanto ao nível “percepção” de CSC, perguntas “1” e “2”, da entrevista com o Chefe da Divisão de Operações do NuCDCAer, obteve-se “concordo fortemente” para ambas as perguntas. Os entrevistados emitiram os seguintes comentários, respectivamente: “Sim, ajuda, principalmente, se o NuCDCAER tiver visibilidade sobre o monitoramento realizado pelo Esquadrão.” e “Sim, ajuda, principalmente, se o NuCDCAER tiver visibilidade sobre o monitoramento realizado pelo Esquadrão.”

Agora, quanto ao nível de CSC “compreensão”, ambos os entrevistados responderam o equivalente a “4”, ou seja, “tendo a concordar ou concordo parcialmente”. O Chefe do NuCDCAer comentou que tal atividade é desenvolvida hoje (2022) pelos analistas de incidentes que apelam à estrutura tecnológica, justamente com gestores de riscos, os quais fornecem as estruturas analíticas mais aprofundadas. Destarte, a compreensão poderá depender da padronização das saídas propostas pelo GDC.

Já o Chefe da Divisão de Operações comentou o seguinte: “O entendimento do significado de cada alarme depende do nível de adestramento da equipe do Esquadrão e da capacidade de modelar eventos de interesse nas ferramentas disponíveis.”

Quanto ao nível projeção da CSC, o Chefe do NuCDCAer respondeu que “concorda parcialmente” comentando que o GDC pode responder quanto à normalização, mas há necessidade de análise e avaliação de riscos cibernéticos que esta estrutura pode não ser capaz de responder de forma eficaz. Por outro lado, esta possui uma sinergia com a fase anterior, e a ligação entre EDC, GDC, DTIC da BACG mais o NuCDCAer poderiam favorecer o retorno da normalidade após o ataque cibernético.

Outrossim, o Chefe da Divisão de Operações do NuCDCAer também respondeu que “concorda parcialmente” comentando que “A evolução à situação de normalidade dependerá da capacitação da equipe do Esquadrão e da maturidade dos processos de tratamento de incidentes e continuidade de negócios.”

Dessa forma, após a devida estimativa quanto aos níveis de CSC em relação à proposta de Estrutura Organizacional de Defesa Cibernética identificada e seus comentários realizados por cada entrevistado, avaliou-se os resultados obtidos, conforme a metodologia proposta nesta pesquisa, chegando ao objetivo geral: “avaliar a influência de uma proposta de Estrutura Organizacional de Defesa Cibernética, baseada na Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, durante o processo de implantação do NuCDCAer, no contexto do PPCG.”

Assim, pelo apresentado, a influência da proposta de Estrutura Organizacional de Defesa Cibernética identificada foi avaliada da seguinte forma em relação aos níveis de CSC:

(a) percepção – CSC alta – como cada entrevistado respondeu que “concorda fortemente” com as seguintes afirmações: “a Estrutura Organizacional de Defesa Cibernética utilizada ajuda a perceber cada nova ativação de alarme dedicado a incidentes cibernéticos” e “a Estrutura Organizacional de Defesa Cibernética ajuda a perceber os valores das variáveis relevantes em relação aos alarmes ativos dedicados a incidentes cibernéticos”;

(b) compreensão – CSC ligeiramente alta, pois as respostas relacionadas à pergunta: “a Estrutura Organizacional de Defesa Cibernética ajuda a entender o significado de cada alarme (as causas do alarme e a qual anomalia o alarme se refere)” foram “concordo parcialmente”; e

(c) projeção – CSC ligeiramente alta, uma vez que a resposta à pergunta: “a Estrutura Organizacional de Defesa Cibernética utilizada ajuda a prever a evolução da normalização do ataque cibernético.” foi “concordo parcialmente” para ambos os entrevistados.

## 5 CONCLUSÃO

O NuCDCAer, no contexto do Plano Piloto Campo Grande, ainda não possui uma estrutura organizacional aderente. Tal fato aliado à importância oferecida à Consciência Situacional Cibernética, juntamente com as possibilidades oferecidas pela Teoria das Estruturas Organizacionais de Mintzberg, fundamentou o objetivo geral desta pesquisa: “avaliar a influência de uma proposta de Estrutura Organizacional de Defesa Cibernética, baseada na Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, durante o processo de implantação do NuCDCAer, no contexto do PPCG.”

Conducente a esse objetivo geral, três objetivos específicos foram apresentados: identificar, à luz da Teoria das Estruturas Organizacionais de Mintzberg, uma proposta de Estrutura Organizacional de Defesa Cibernética, que seja mais aderente ao NuCDCAER, no contexto do PPCG; conceber métricas que sejam mais adequadas para os níveis de CSC de uma Estrutura Organizacional de Defesa Cibernética; e estimar os níveis de CSC em relação a proposta de Estrutura Organizacional de Defesa Cibernética, concebida à luz da Teoria das Estruturas Organizacionais de Mintzberg, durante o processo de implantação do NuCDCAER, no contexto do PPCG.

Para tal, inicialmente, buscou-se a identificação do estado do problema a ser pesquisado sob o aspecto teórico e de outros trabalhos e pesquisas realizados. Nesse sentido, apresentou-se uma breve fundamentação teórica envolvendo a Teoria das Estruturas Organizacionais de Mintzberg e CSC mais trabalhos relacionados a ambos, que apoiassem principalmente a identificação de uma proposta de Estrutura Organizacional de Defesa Cibernética e a concepção de métricas para mensurar os níveis de CSC relacionados a esta estrutura.

Dessa maneira, apesar da ausência de trabalhos que tratassem exatamente do objetivo geral apresentado, as pesquisas de Aguiar e Martins (2006), Martin e Guimarães (2018) e Moreira *et al.* (2019) auxiliaram os objetivos específicos, aplicando a Teoria das Estruturas Organizacionais de Mintzberg.

Da mesma forma, quanto à CSC, o modelo de Endsley – percepção, compreensão e projeção - serviu de base teórica, assim como os trabalhos de Tianfield (2016), Lötjönen (2017), Guimarães (2019) e Satuf (2016), principalmente quanto à consecução do segundo objetivo específico, que foi a concepção das métricas os níveis de CSC relacionados a estrutura organizacional identificada.

Já com vistas ao atingimento dos objetivos específicos, a metodologia envolveu primeiramente uma pesquisa exploratória e documental para identificar, à luz da Teoria das

Estruturas Organizacionais de Mintzberg, uma proposta de Estrutura Organizacional de Defesa Cibernética, que seja mais aderente ao NuCDCAER, no contexto do PPCG.

Por segundo, envolveu a técnica CS3, apresentada por Satuf (2016), juntamente com as considerações apontadas por Tianfield (2016), Lötjönen (2017) e Guimarães (2019). A adaptação da técnica CS3 considerou o trabalho de Lötjönen (2017) que tratou de CSC, no contexto do modelo de Endsley, em relação à proposta de Estrutura Organizacional de Defesa Cibernética concebida nesta pesquisa.

Em terceiro, para estimar os níveis de CSC foi realizada uma pesquisa de campo no NuCDCAer e, por último, oferecendo condições para a avaliação prevista no objetivo geral, os valores de “CSC baixa” a “CSC alta” foi adequada para a estimativa dos níveis de CSC realizada no objetivo específico nº 3.

A seção de apresentação e análise de dados trouxe a realização de cada objetivo específico. A proposta de Estrutura Organizacional de Defesa Cibernética, conforme a Teoria das Estruturas Organizacionais de Mintzberg, mais aderente ao contexto desta pesquisa, foi a burocracia mecanizada, sendo a mesma apoiada pela identificação das seguintes partes básicas: NuCDCAer representando a cúpula estratégica, o Grupo de Defesa Cibernética do COMPREP a linha intermediária juntamente com a tecnoestrutura e a DTIC da BACG a assessoria de apoio.

Essas existindo para missão de apoiar, conforme Brasil (2021), a atividade-fim da BACG com eficiência e eficácia. Além das partes básicas e da “missão”, os mecanismos de coordenação também foram identificados e ilustrados, conforme Figura 5.

Quanto ao objetivo específico nº 2, a concepção das métricas para os níveis de CSC, contou com a estruturação de um questionário, vide Apêndice A, englobando as quatro perguntas apresentadas por Satuf (2016) envolvendo a percepção, a compreensão e a projeção, previstas no modelo de Endsley, sendo essas perguntas consideradas base para a compreensão do questionário.

Juntamente com essas perguntas, objetivo específico nº 2 também contou com a proposta de Estrutura Organizacional de Defesa Cibernética identificada anteriormente sendo apoiada pelo *framework* criado por Tianfield (2016), vide Figura 4, e as métricas internas de CSC desenvolvidas por Guimarães (2019).

Por terceiro, a estimativa dos níveis de CSC foi atingida aplicando o questionário contendo as métricas concebidas anteriormente para os níveis de CSC relacionados à proposta de estrutura organizacional identificada.

Os questionários foram aplicados ao Chefe do NuCDCAer e ao Chefe da Divisão de Operações do NuCDCAer, representantes da alta gestão do NuCDCAer, estimando que, para

ambos os entrevistados, quanto ao nível de CSC – percepção – “concordo fortemente”; já quanto aos níveis de CSC – compreensão e projeção – “tendo a concordar ou concordo parcialmente”.

Finalmente, completando os fundamentos necessários para o atingimento do objetivo geral desta pesquisa, da avaliação da influência de uma proposta de Estrutura Organizacional de Defesa Cibernética, baseada na Teoria das Estruturas Organizacionais de Mintzberg, nos níveis de CSC, durante o processo de implantação do NuCDCAer, no contexto do PPCG, chegou-se ao seguinte resultado: o nível de CSC percepção foi “CSC alta” e para os níveis de CSC compreensão e projeção foi “CSC ligeiramente alta”.

Da mesma forma, percebe-se como principais contribuições para a FAB, dada a importância da defesa cibernética para a missão da instituição, principalmente, quanto aos níveis de CSC, a proposta de uma Estrutura Organizacional de Defesa Cibernética em contribuição ao processo de implantação do CDCAer, podendo ser um modelo a ser aplicado aos outros Grandes Comandos, além do próprio COMPREP.

A Teoria das Estruturas Organizacionais de Mintzberg foi aplicada, entretanto limitada à identificação das partes básicas e dos mecanismos de coordenação envolvendo a missão da instituição, condição que propõe, como trabalho futuro, a identificação dos parâmetros de *design* e dos fatores situacionais, aplicando a proposta de Estrutura Organizacional de Defesa Cibernética identificada neste trabalho. Da mesma maneira, a validação da burocracia mecanizada como Estrutura Organizacional mais aderente ao NuCDCAer.

Outrossim, também se percebe como propostas de trabalhos futuros, com vistas à estimativa mais precisa dos níveis de CSC, a inclusão de todo o efetivo do NuCDCAer para a coleta de dados e a inclusão de mais perguntas aderentes também aos níveis de percepção, compreensão e projeção presentes nas métricas concebidas.

## REFERÊNCIAS

- AGUIAR, A. B.; MARTINS, G. A. A teoria das estruturas organizacionais de Mintzberg e a gestão estratégica de custos: um estudo nas ONGs paulistas. **Revista Contabilidade & Finanças**, v. 17, p. 51-64, 2006.
- BRASIL. Ministério da Defesa. Exército Brasileiro. Portaria nº 42 - COTER, de 8 jun. 2017. Aprova o Manual de Campanha EB70-MC-10.232 - Guerra Cibernética. **Boletim do Exército**, Brasília, n. 25, de 23 jun. 2017
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria COMPREP nº 188/SPOG-23, de 14 nov. 2018. Aprova a reedição do Regimento Interno do Comando de Preparo. **Boletim do Comando da Aeronáutica**, Brasília, n. 203, 22 nov. 2018, 2018.
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria nº 1.225/GC3, de 10 nov. 2020. Aprova a edição da Doutrina Básica da Força Aérea Brasileira - Volume 2. **Boletim do Comando da Aeronáutica**, Brasília, n. 205, 12 nov. 2020, 2020a.
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria nº 1.008/GC3, de 2 out. 2020. Aprova a Diretriz de implantação do Núcleo do Centro de Defesa Cibernética da Aeronáutica. **Boletim do Comando da Aeronáutica**, Brasília, n. 182, 7 out. 2020, 2020b.
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Centro de Comunicação Social da Aeronáutica. **Diretriz do Comandante da Aeronáutica 2021-2022**. Brasília: Agência Força Aérea, 2021. Disponível em: <https://www.fab.mil.br/noticias/mostra/37410/DIRETRIZ%20-%20Publicada%20Diretriz%20do%20Comandante%20da%20Aeron%C3%A1utica%202021-2022>. Acesso em: 23 jun. 2022.
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria GABAER nº 108/GC3, de 07 jul. 2021. Aprova a Diretriz que dispõe sobre a implantação do Projeto Piloto Campo Grande. **Boletim do Comando da Aeronáutica**, Brasília, n. 125, 8 jul. 2021, 2021a.
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria EMAER nº 91/ISC, de 9 dez. 2021. Aprova a Diretriz que dispõe sobre a estrutura organizacional do Comando da Aeronáutica. **Boletim do Comando da Aeronáutica**, Brasília, n. 229, 15 dez. 2021, 2021b.
- BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria SEFA nº 32/AJUR, de 12 fev. 2021. Aprova o Regimento Interno da Base Aérea de Campo Grande. **Boletim do Comando da Aeronáutica**, Brasília, n. 032, 18 fev. 2021, 2021c.
- ENDSLEY, M. R. **Toward a theory of situation awareness in dynamic systems: human factors**, 37(1), p. 32-64, 1995.
- JUNIOR, S. A. F. **A aquisição de alvos da artilharia de campanha e a formação da consciência situacional**. 2019.
- GUIMARÃES, F. Q. Quantificando a Guerra Cibernética: métricas de proteção e indicadores para a obtenção de uma consciência situacional cibernética. *In: SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA*, 19., 2019, Rio de Janeiro, RJ. **Anais [...]**. Rio de Janeiro: Centro de Análises de Sistemas Navais, 2019.

LÖTJÖNEN, J. **Requirement specification for cyber security situational awareness: defender's approach in cyber security exercises.** 2017.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, 2003.

MARTIN, J. G.; GUIMARÃES, G. S. A teoria das estruturas organizacionais de Mintzberg: análise de uma estrutura organizacional da startup–target situada no município de Belém/PA e sua contribuição para a tomada de decisão. **Revista de Administração de Empresas Eletrônica-RAEE**, n. 9, p. 24-43, 2018.

MINTZBERG, H. **Criando organizações eficazes.** 2. ed. São Paulo: Atlas, 2006.

MOREIRA, T. P. *et al.* A estrutura organizacional da Universidade Federal do Ceará (UFC): um estudo de caso à luz da teoria das cinco configurações de Mintzberg. **Revista Gestão Universitária na América Latina-GUAL**, v. 12, n. 1, p. 73-96, 2019.

PAUL, C. L.; WHITLEY, K. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. *In: International conference on human aspects of information security, privacy, and trust.* Springer, Berlin, Heidelberg, p. 145-154, 2013.

SATUF, E. N. **Utilização de Técnicas de Medição de Consciência Situacional para Avaliar Interface Ecológica de Alarmes.** 2016. Tese de Doutorado (Ciências em Engenharia Elétrica) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2016.

STANTON, N. A.; CHAMBERS, P. R. G.; PIGGOTT, J. Situational Awareness and Safety, **Safety Science**, v. 39, n. 3, p. 189-204, 2001.

TIANFIELD, H. Cyber security situational awareness. *In: 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical, and social computing (CPSCom) and IEEE smart data (SmartData).* IEEE, p. 782-787, 2016.

## GLOSSÁRIO

**Esquadrão de Defesa Cibernética:** Camada tática da Estrutura Organizacional de Defesa Cibernética identificada nesta pesquisa que possui uma Estrutura formada pelo conjunto de recursos humanos capacitados e dedicados juntamente com seus equipamentos (HW) disponíveis para a realização de defesa cibernética em apoio às missões das OM subordinadas à BACG. Contêm todas as células de defesa cibernética previstas no Manual de Campanha – Guerra Cibernética do EB. Subordinado aos elos de TI da FAB e administrativamente à BACG.

**Grupo de Defesa Cibernética:** Camada operacional da Estrutura Organizacional de Defesa Cibernética identificada nesta pesquisa que possui uma Estrutura formada pelo conjunto de recursos humanos capacitados e dedicados para padronizar as saídas previstas nas tarefas de defesa cibernéticas realizadas no Esquadrão de Defesa Cibernética. Sua principal atividade deve estar ligada à identificação de indicadores de defesa cibernética relacionados à missão do COMPREP com estreita relação com as atividades diretamente relacionadas ao cumprimento das missões das Unidades Aéreas e do Esquadrão Aeroterrestre de Salvamento subordinados à BACG.

## APÊNDICE A – Questionário para Coleta de Dados

### Concepção de uma Estrutura Organizacional de Defesa Cibernética à luz da Teoria das Estruturas Organizacionais de Mintzberg para o NuCDCAer no Contexto do Projeto Piloto Campo Grande

Este questionário é parte integrante de artigo científico relativo ao Curso de Comando e Estado Maior Avançado (CEM-A) - 2022 e está dividido nas seguintes etapas: compreensão do assunto e coleta de dados, para, ao final, proporcionar subsídios para a mensuração dos níveis de Consciência Situacional Cibernética. A seção de compreensão traz a Estrutura Organizacional de Defesa Cibernética que foi concebida, a apresentação do trabalho de Tianfield (2016) e as métricas e indicadores apresentados por Guimarães (2019).

\*Obrigatório

1. Posto/Graduação/nome de guerra \*

\_\_\_\_\_

2. Função/cargo exercido no NuCDCAer? \*

\_\_\_\_\_

As seguintes considerações deverão ser levadas em conta para que cada participante compreenda a concepção da Estrutura Organizacional de Defesa Cibernética para o NuCDCAer, no contexto do Projeto Piloto Campo Grande, juntamente com suas características internas:

O NuCDCAer corresponde ao setor responsável pela Ação de Defesa Cibernética da FAB, prevista na DCA 1-1.

A Estrutura Organizacional de Defesa Cibernética deve ser capaz de oferecer defesa cibernética à Estrutura Organizacional prevista no Projeto Piloto Campo Grande.

Considere a necessidade de defender com eficácia o 1º/15º Grupo de Aviação (GAv), o 2º/10º GAv, o EAS e o 3º/3º GAv, Organizações Militares pertencentes à Base Aérea de Campo Grande (BACG), de ataques cibernéticos que possam comprometer severamente o cumprimento de suas respectivas missões e por conseguinte a própria missão da FAB.

#### Estrutura Organizacional de Defesa Cibernética



Os mecanismos básicos da Estrutura Organizacional de Defesa Cibernética são os seguintes: NuCDCAer representa a cúpula estratégica; o Grupo de Defesa Cibernética (COMPREP) representa a ligação e a padronização das saídas entre o NuCDCAer e o elemento tático de defesa cibernética, i.e. o Esquadrão de Defesa Cibernética; o próprio elemento tático de defesa cibernética dentro da estrutura do Organograma do Projeto Piloto Campo Grande e a estrutura de TI da FAB como a Assessoria de Apoio.

De maneira geral, a defesa cibernética aproximada seria realizada pelo Núcleo Operacional, i.e., Esquadrão de Defesa Cibernética, que, por estar mais próximo ao dia a dia das OM sediadas e possuir em sua estrutura interna todas as células previstas para a contenção de ataque (análise de malware, forense, gestão de riscos, análise de incidentes, dentre outras capacidades) poderia oferecer com mais propriedade a eficácia e eficiência exigidos na Diretriz do Comandante 2021 - 2022.

O NuCDCAer, considerada a Cúpula Estratégica, além de ser responsável pelo planejamento estratégico da Ação de Defesa Cibernética da FAB, apoiaria diretamente a padronização dos processos realizados pelo EDC, assim como, a padronização das habilidades requeridas pelas células internas ao EDC.

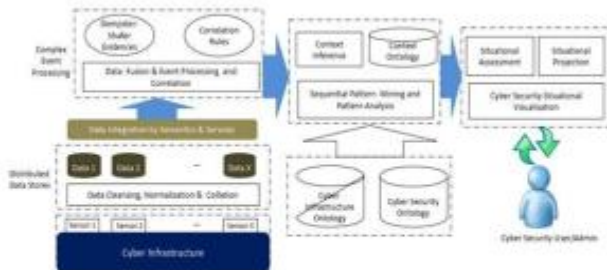
A Linha Intermediária e a Tecnoestrutura seriam representadas pelo COMPREP, na figura do Grupo de Defesa Cibernética, que basicamente teria a função de padronizar as saídas previstas pelo EDC, pois a este Grande Comando interessaria saber como seus meios estão preparados contra ataques cibernéticos de modo a não comprometer a missão da FAB. Ficando clara, neste primeiro momento, a não participação técnica desta unidade.

A Assessoria de Apoio, como elo de TI, representada pela DTIC da BACG, proporcionaria todo apoio necessário para a realização da missão pelo Esquadrão de Defesa Cibernética, i.e., SW, HW, licenças, estrutura de acomodação,...

Após as devidas considerações sobre a Estrutura de Defesa Cibernética concebida, apresenta-se os trabalhos de Tianfield (2016) e Guimarães (2019), pesquisas que deverão ser consideradas como internas à Estrutura concebida para que o ambiente para a devida medição de Consciência Situacional Cibernética possa ser realizada.

Para Tianfield (2016), a "ideia principal da consciência situacional no domínio cibernético é analisar os arredores da infraestrutura cibernética e criar determinados eventos e visualizações com o objetivo de tomar decisões rápidas e eficientes. Em palavras simples, CSSA pode ser descrito como a consciência situacional aplicada à segurança cibernética em uma infraestrutura cibernética."

No framework para Consciência Situacional Cibernética desenvolvido por Tianfield (2016): a cyber infraestrutura estaria ligada por "sensores" instalados no espaço cibernético de interesse no ambiente da DTIC da BACG; as demais estruturas, com exceção da avaliação, projeção e visualização da segurança cibernética, devem ser consideradas como parte do processo de obtenção de CSC. A última etapa - avaliação, projeção e visualização da segurança cibernética - é composta por elementos no EDC, GDC, principalmente pela preocupação com os indicadores de segurança cibernética, e do próprio NuCDCAer, que além dos indicadores, também pode monitorar as métricas internas de CSC, de acordo com Guimarães (2019).



A pesquisa de Guimarães (2019) propôs estabelecer "métricas e indicadores que representem as características quantitativas da condição de proteção de um Espaço Cibernético, categorizadas em proteção de perímetro, cobertura e disponibilidade/confiabilidade" e que sejam relevantes para a modelagem do processo de CSC, verificando os motivos que tornam o seu desenvolvimento tão crítico. Guimarães (2019) considerou que o Espaço Cibernético a ser protegido deve possuir ter "três áreas básicas: rede externa, composta pela Internet; rede desmilitarizada (DMZ), onde estão disponibilizados os serviços à Rede Externa e uma rede interna (Rede Local) com seus respectivos sensores de proteção de perímetro (antispam, firewall e Intrusion Prevention System - IPS) e proteção de host (antivírus)." e para isso foram estabelecidos três categorias de métricas para a defesa: métricas de proteção de perímetro, métricas de cobertura e métricas de disponibilidade e confiabilidade.

Tabela com exemplo de métricas relacionadas a disponibilidade e confiabilidade

Disponibilidade e confiabilidade		
Variável	Métrica	Propósito
$t_{up}$	Tempo total de disponibilidade dos servidores críticos durante o período de medição.	Estabelecer um baseline de disponibilidade dos servidores críticos.
$t_{up}^p$	Tempo de indisponibilidade planejada dos servidores críticos durante o período de medição.	Estabelecer um baseline de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
$t_{up}^i$	Tempo de indisponibilidade dos servidores críticos devido a um incidente de segurança durante o período de medição.	Estabelecer um baseline de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
$\Sigma n$	Quantidade total de incidentes de segurança.	Estabelecer um baseline quantitativo de incidentes de segurança.
$\Sigma n_{top}$	Quantidade total de incidentes de segurança por tipo de incidentes.	Identificar os incidentes mais recorrentes no ECiber.
Variável	Indicador de desempenho	Propósito
$t_{up}^p$	Índice de disponibilidade dos servidores críticos durante o período p de medição.	Identificar o nível de disponibilidade dos servidores críticos.
$t_{up}^i$	Índice de indisponibilidade planejada dos servidores críticos durante o período p de medição.	Identificar o nível de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
$t_{up}^i$	Índice de indisponibilidade dos servidores críticos devido a um incidente de segurança durante o período p de medição.	Identificar o nível de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.

Levantamento de Dados

Nesta seção, à luz da Teoria das Estruturas Organizacionais de Mintzberg, de acordo com as considerações apresentadas na seção anterior, serão realizados questionamentos quanto à percepção dos respondentes sobre as Forças que venham a influenciar a tomada de decisão durante um ataque cibernético às Unidades Aéreas (UAe) da Base Aérea de Campo Grande.

3. A Estrutura Organizacional de Defesa Cibernética utilizada ajuda a perceber cada nova ativação de alarme dedicado a incidentes cibernéticos. \*

Marque todas que se aplicam.

- 1 = discordo fortemente  
 2 = tendo a discordar ou discordo parcialmente  
 3 = neutro  
 4 = tendo a concordar ou concordo parcialmente  
 5 = concordo fortemente.

4. Comente a resposta anterior: \*

---

---

---

---

---

5. A Estrutura Organizacional de Defesa Cibernética ajuda a perceber os valores das variáveis relevantes em relação aos alarmes ativos dedicados a incidentes cibernéticos. \*

Marque todas que se aplicam.

- 1 = discordo fortemente  
 2 = tendo a discordar ou discordo parcialmente  
 3 = neutro  
 4 = tendo a concordar ou concordo parcialmente  
 5 = concordo fortemente.

6. Comente a resposta anterior: \*

---

---

---

---

---

7. A Estrutura Organizacional de Defesa Cibernética ajuda a entender o significado de cada alarme (as causas do alarme e a qual anomalia o alarme se refere) \*

Marque todas que se aplicam.

- 1 = discordo fortemente  
 2 = tendo a discordar ou discordo parcialmente  
 3 = neutro  
 4 = tendo a concordar ou concordo parcialmente  
 5 = concordo fortemente.

8. Comente a resposta anterior: \*

---

---

---

---

---

9. A Estrutura Organizacional de Defesa Cibernética utilizada ajuda a prever a evolução à situação de normalização, i.e., ataque cibernético mitigado. \*

Marque todas que se aplicam.

- 1 = discordo fortemente
- 2 = tendo a discordar ou discordo parcialmente
- 3 = neutro
- 4 = tendo a concordar ou concordo parcialmente
- 5 = concordo fortemente.

10. Comente a resposta anterior: \*

---

---

---

---

---

ANEXO A – Organograma da Estrutura Organizacional do COMPREP

