



UNIVERSIDADE DA FORÇA AÉREA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS

RAIMUNDO FELIPE DA **SILVA COSTA**, 1º Ten QOCon SED

O Papel Estratégico da Segurança e Defesa no Poder Aeroespacial Brasileiro: Uma
Análise do Centro de Lançamento de Alcântara sob a Ótica da Segurança Corporativa
Estratégica.

Rio de Janeiro
2025

UNIVERSIDADE DA FORÇA AÉREA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS

RAIMUNDO FELIPE DA SILVA COSTA, 1º Ten QOCon SED

O Papel Estratégico da Segurança e Defesa no Poder Aeroespacial Brasileiro: Uma Análise do Centro de Lançamento de Alcântara sob a Ótica da Segurança Corporativa Estratégica.

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea, como requisito parcial para obtenção do título de Mestre em Ciências Aeroespaciais.

Linha de Pesquisa: Poder Aeroespacial Brasileiro, Segurança e Defesa.

Orientador: Luciano Vaz Ferreira.

Rio de Janeiro
2025

Ficha catalográfica elaborada pela Biblioteca da UNIFA

Costa, Raimundo Felipe da Silva

C837

O papel estratégico da segurança e defesa no poder
aeroespacial brasileiro: Uma análise do Centro de lançamento de
Alcântara sob a ótica da segurança corporativa estratégica. /
Raimundo Felipe da Silva Costa. – Rio de Janeiro: Universidade
da Força Aérea, 2025.

126 f.: il., enc.

Orientador: Prof. Luciano Vaz Ferreira

Dissertação (mestrado) – Universidade da Força Aérea, Rio
de Janeiro, 2025.

Referências: f. 118-123

1. segurança e defesa . 2. poder aeroespacial. 3. Força
Aérea Brasileira. 4. segurança corporativa. I. Título. II. Ferreira,
Luciano Vaz. III. Universidade da Força Aérea.

CDU: 351.861

RAIMUNDO FELIPE DA SILVA COSTA, 1º Ten QOCon SED

O Papel Estratégico da Segurança e Defesa no Poder Aeroespacial Brasileiro: Uma Análise do Centro de Lançamento de Alcântara sob a Ótica da Segurança Corporativa Estratégica.

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea, como requisito parcial para obtenção do título de Mestre em Ciências Aeroespaciais.

Aprovado por:

Documento assinado digitalmente
 **LUCIANO VAZ FERREIRA**
Data: 23/09/2025 14:38:52-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. LUCIANO VAZ FERREIRA – UNIFA
Presidente da Banca de Defesa

Documento assinado digitalmente
 **NEWTON HIRATA**
Data: 23/09/2025 15:06:51-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. NEWTON HIRATA – UNIFA
Examinador Interno

Documento assinado digitalmente
 **VILMAR ANTONIO GONCALVES TONDOLO**
Data: 23/09/2025 14:47:09-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. VILMAR ANTONIO GONÇALVES TONDOLO – UFPel
Examinador Externo

Rio de Janeiro

2025

AGRADECIMENTOS

Esta alegre fase da minha vida se inicia com um profundo agradecimento àqueles que me apoiaram nos momentos mais difíceis: minha família, em especial, meus pais - Antonio e Verônica, irmãos - Gustavo, João e Vitória, meu amado filho – Antonio Felipe, e minha companheira – Helyda. Foram inúmeras as vezes em que pensei em desistir, mas graças ao apoio e à confiança de vocês, hoje estamos aqui.

Minha gratidão se estende ao meu Orientador, que me acompanhou nesta jornada e contribuiu decisivamente para a realização deste grande sonho. Não foi uma tarefa simples, o teor da dissertação desafiou a todos nós, mas sua atenção e excelente orientação foram cruciais para que a missão fosse concluída com sucesso.

Agradeço, também, aos meus companheiros de trabalho e amigos que, de alguma forma, direta ou indiretamente, contribuíram para este estudo.

Um reconhecimento especial ao Centro de Lançamento de Alcântara (CLA), na figura de seu Diretor, Coronel Aviador Clóvis, por permitir o acesso aos documentos que foram vitais para esta pesquisa.

Ao Grupo de Segurança e Defesa de Alcântara (GSD-AK), representado por todos os seus comandantes desde o ano de 2020: ao Ten Cel Inf Rafael, pelo estudo das legislações atinentes; ao Maj Inf Abdias, pelo apoio e total confiança na participação e relevância deste estudo; e ao meu atual comandante, Maj Inf Diamante, pela ajuda na sua estruturação. Aos senhores, meu muito obrigado por apoiarem e darem a devida importância a esta pesquisa.

Com a certeza do dever cumprido, finalizo meus agradecimentos com a mensagem: “Me responsabilizo por todos os meus feitos!”.

RESUMO

O Centro de Lançamento de Alcântara (CLA) constitui um ativo de valor inestimável para o Programa Espacial Brasileiro e para a soberania nacional, cuja relevância é amplificada pelo Acordo de Salvaguardas Tecnológicas (AST). Contudo, a crescente complexidade das operações e os rigorosos requisitos internacionais elevam os desafios para sua Segurança e Defesa (SEGDEF). O presente estudo objetivou analisar a arquitetura de SEGDEF do CLA, a fim de propor um modelo de otimização estratégica. A metodologia adotada foi o estudo de caso único, de natureza qualitativa, com base em pesquisa bibliográfica e documental aprofundada, utilizando como principal referencial teórico o modelo de Segurança Corporativa Estratégica (SCorPE). Os resultados do diagnóstico indicam a existência de vulnerabilidades estratégicas, especialmente nos domínios da gestão do conhecimento, dos recursos humanos e dos processos, que não são plenamente endereçadas pelo modelo de segurança vigente, de caráter predominantemente reativo. Considera-se, portanto, que a adoção de um Plano Diretor de Segurança Estratégica (PDSE), fundamentado na gestão integrada de riscos e na prevenção de perdas, é crucial para garantir a proteção, a resiliência e a sustentabilidade das operações no CLA, fortalecendo a defesa e a projeção internacional do Brasil.

Palavras-chave: Segurança e Defesa; Segurança Corporativa Estratégica; Centro de Lançamento de Alcântara; Poder Aeroespacial; Força Aérea Brasileira.

ABSTRACT

The Alcântara Launch Center (CLA) is a strategic asset for the Brazilian Space Program and national sovereignty, its relevance amplified by the Technology Safeguards Agreement (TSA). However, the increasing complexity of operations and stringent international requirements heighten the challenges for its Security and Defense (SEGDEF). This study aimed to analyze the SEGDEF architecture of the CLA to propose a strategic optimization model. The methodology adopted was a single case study of a qualitative nature, based on in-depth bibliographic and documentary research, using the Strategic Corporate Security (SCorpE) model as the main theoretical framework. The diagnostic results indicate the existence of strategic vulnerabilities, especially in the domains of knowledge management, human resources, and processes, which are not fully addressed by the current, predominantly reactive security model. It is considered, therefore, that the adoption of a Strategic Security Master Plan (PDSE), based on integrated risk management and loss prevention, is crucial to ensure the protection, resilience, and sustainability of operations at the CLA, thereby strengthening Brazil's defense and international projection.

Keywords: Security and Defense; Strategic Corporate Security; Alcântara Launch Center; Aerospace Power; Brazilian Air Force.

LISTA DE ILUSTRAÇÕES

Figura 1 - Infraestrutura do CLA no município de Alcântara-MA.....	31
Figura 2 - Infraestrutura do Complexo do CLA.....	33
Figura 3 - Amplitude de azimutes de lançamentos.....	35
Figura 4 - Vista lateral da torre móvel de integração após o acidente de 2003.....	38
Figura 5 - Elementos do Poder Espacial.....	46
Figura 6 - Os quatro grandes segmentos da Segurança Corporativa.....	74
Figura 7 - Teoria dos Círculos Concêntricos.....	75

LISTA DE TABELAS

Tabela 1 – Fases da Investigação Metodológica.....	24
Tabela 2 – Principais Instalações do CLA em Alcântara-MA.....	32
Tabela 3 – Importância do AST para o Brasil.....	41
Tabela 4 – Espectro de Perdas Potenciais no CLA.....	44
Tabela 5 – Características do Poder Aeroespacial.....	49
Tabela 6 – Quadro Comparativo Era Industrial x Era do Conhecimento.....	68
Tabela 7 – Segmentos da Segurança Orgânica (SO) no Contexto do CLA.....	70
Tabela 8 – Segmentação da Segurança Corporativa.....	74
Tabela 9 – Classificação das Áreas.....	75
Tabela 10 – Escala de Criticidade.....	85
Tabela 11 – Discrição vs. Ostensividade no Transporte.....	88
Tabela 12 – Princípios das Organizações de Alta Confiabilidade (HRO)	96

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

AEB – Agência Espacial Brasileira

AGU - Advocacia-Geral da União

AIDA – Área Interna da Organização Militar

AST – Acordo de Salvaguardas Tecnológicas

BCA – Boletim do Comando da Aeronáutica

C2 - Comando e Controle

C4I – Comando, Controle, Comunicações, Computação e Inteligência

CEA – Centro Espacial de Alcântara

CEBRA - Complexo Espacial Brasileiro

CENIPA – Centro de Investigação e Prevenção de Acidentes Aeronáuticos

CFTV - Circuito Fechado de Televisão

CJF - Conselho da Justiça Federal

CLA - Centro de Lançamento de Alcântara

CLBI - Centro de Lançamento da Barreira do Inferno

CNMP - Conselho Nacional do Ministério Público

COMAER - Comando da Aeronáutica

COMPREP - Comando de Preparo

CPOL - Curso de Preparação para Operações de Lançamento

DCA - Diretriz do Comando da Aeronáutica

DTI - Diretoria de Tecnologia da Informação

EMAER - Estado-Maior da Aeronáutica

END - Estratégia Nacional de Defesa

ERT - Estação Redundante de Telemetria

ESG - Escola Superior de Guerra

ETIR - Equipe de Tratamento e Respostas de Incidentes em Redes Computacionais

FAB - Força Aérea Brasileira

GSD-AK - Grupo de Segurança e Defesa de Alcântara

HRO - Organizações de Alta Confiabilidade (High-Reliability Organizations)

IC - Infraestruturas Críticas

INFAER - Infantaria da Aeronáutica

INE.EAD - Instituto Nacional de Ensino a Distância

KPIs - Indicadores-Chave de Desempenho (*Key Performance Indicators*)

LEO - Órbita Baixa Terrestre (*Low Earth Orbit*)

MECB - Missão Espacial Completa Brasileira

MD - Ministério da Defesa

MP - Ministério Público

NSCA - Norma de Sistema do Comando da Aeronáutica

PCA - Plano do Comando da Aeronáutica

PCG - Plano de Contingência Geral

PDI-CEA - Programa de Desenvolvimento Integrado para o Centro Espacial de Alcântara

PDSE - Plano Diretor de Segurança Estratégica

PEB - Programa Espacial Brasileiro

PEMAER - Plano Estratégico Militar da Aeronáutica

PESE - Programa Estratégico de Sistemas Espaciais

PGR - Plano de Gerenciamento de Riscos

POPs - Procedimentos Operacionais Padrão

PSI - Plano de Segurança das Instalações

PSIC - Plano de Segurança da Informação e Comunicações

PSO - Plano de Segurança Orgânica

PSOD - Plano de Segurança Orgânica e Defesa

RH - Recursos Humanos

RTC - Rastreamento, Telemetria e Comando

SCAI - Software de Controle de Acesso e Informações

SCorpE - Segurança Corporativa Estratégica

SEGDEF - Segurança e Defesa

SGAI - Segurança da Gestão das Áreas e Instalações

SGC - Segurança da Gestão do Conhecimento

SGDC - Satélite Geoestacionário de Defesa e Comunicações Estratégicas

SGP - Segurança da Gestão das Pessoas

SGProc - Segurança da Gestão dos Processos

SInsu - Segurança dos Insumos

SINTAER - Sistema de Inteligência da Aeronáutica

SISBIN - Sistema Brasileiro de Inteligência

SISDE - Sistema de Segurança e Defesa

SISI - Suporte Integrado de Segurança das Instalações

SO - Segurança Orgânica

SOp - Segurança das Operações

SPIj - Segurança do Planejamento

SSA - Consciência Situacional Espacial (*Space Situational Awareness*)

TCA - Tabela do Comando da Aeronáutica

TMI - Torre Móvel de Integração

TRC - Transporte Rodoviário de Cargas

UFMA - Universidade Federal do Maranhão

UNIFA - Universidade da Força Aérea

USEGDEF - Unidade de Segurança e Defesa

VLS - Veículo Lançador de Satélites

SUMÁRIO

1 INTRODUÇÃO	18
2 A IMPORTÂNCIA ESTRATÉGICA DO CENTRO DE LANÇAMENTO DE ALCÂNTARA (CLA) PARA O PODER AEROESPACIAL BRASILEIRO	26
2.1 O CENTRO ESPACIAL DE ALCÂNTARA (CEA) E CENTRO DE LANÇAMENTO DE ALCÂNTARA (CLA) COMO ATIVOS ESTRATÉGICOS.....	28
2.1.1 O CLA como Infraestrutura Estratégica	30
2.1.2 Vantagens Geográficas e Comparativas do CLA	34
2.1.3 O CLA como Pilar do Programa Espacial Brasileiro (PEB) e da Projeção Internacional.....	36
2.1.4 O Acidente de 2003 e suas Lições para a Segurança	37
2.1.5 O Ambiente Sociopolítico.....	39
2.2 O ACORDO DE SALVAGUARDAS TECNOLÓGICAS (AST) E A SEGURANÇA E DEFESA (SEGDEF) NO CLA	40
2.2.1 Implicações Legais, de Soberania e Propriedade Intelectual no Contexto do AST	41
2.3 VULNERABILIDADES E DESAFIOS À SEGDEF DO CLA SOB A ÓTICA DAS “PERDAS” COM AST.....	43
3 A SEGURANÇA E DEFESA COMO ELEMENTO DO PODER AEROESPACIAL.....	46
3.1 A SEGURANÇA E DEFESA DA INFRAESTRUTURA TERRESTRE ESTRATÉGICA.....	54
3.2 ANÁLISE DO ARCABOUÇO NORMATIVO DA SEGURANÇA E DEFESA NO COMAER.....	57
3.2.1 Diretrizes para a Segurança e Defesa no COMAER (DCA 205-4) e o Sistema de Segurança e Defesa (NSCA 205-3) Aplicados ao CLA.....	60
3.2.2 O Suporte Integrado de Segurança das Instalações (DCA 205-9) como Modelo de Modernização para a SEGDEF do CLA	63
4 FUNDAMENTOS DA SEGURANÇA CORPORATIVA ESTRATÉGICA (SCORPE).....	65
4.1 A EVOLUÇÃO DA SEGURANÇA: DA ERA INDUSTRIAL À ERA DO CONHECIMENTO	67
4.2 RAMOS DA SEGURANÇA CORPORATIVA	69

4.2.1 Segurança das Pessoas na Organização Militar	71
4.2.2 Segurança dos Ativos: Além do Patrimônio Físico	72
4.3 SEGURANÇA CORPORATIVA E OS SEGMENTOS DA ATIVIDADE DE SEGURANÇA.....	73
4.3.1 Segurança da Gestão das Áreas e Instalações (SGAI)	74
4.3.2 Segurança da Gestão das Pessoas (SGP)	81
4.3.3 Segurança da Gestão dos Processos (SGPROC).....	83
4.3.3.1 Segurança das Operações (SOP)	84
4.3.3.2 Segurança do Planejamento (SPLJ)	86
4.3.3.3 Segurança dos Insumos (SINSU)	87
4.3.4 Segurança da Gestão do Conhecimento (SGC)	89
4.4 A SEGURANÇA CORPORATIVA ESTRATÉGICA (SCORPE): PILARES E APLICAÇÃO NA FAB.....	90
4.4.1 Cultura Organizacional, Filosofia e Política de Segurança na FAB.....	92
4.4.2 Endomarketing e Educação para Segurança na FAB.....	93
4.5 DIÁLOGO COM A TEORIA DA ESTRATÉGIA CORPORATIVA	95
4.5.1 A Teoria das Organizações de Alta Confiabilidade (HRO).....	96
5 ANÁLISE E OTIMIZAÇÃO DA SEGURANÇA E DEFESA DO CLA À LUZ DA SEGURANÇA CORPORATIVA ESTRATÉGICA	97
5.1 PLANEJAMENTO ESTRATÉGICO DA SEGURANÇA NO AMBIENTE AEROSPAÇIAL	98
5.1.1 Proposta de Inclusão do Módulo de SEGDEF no Curso de Preparação para Operações de Lançamento (CPOL)	100
5.1.2 Planejamento de Contingências e Gerenciamento de Crises no CLA	101
5.1.3 Modularidade e Faseamento na Implementação da Segurança Estratégica no CLA.....	103
5.2 GESTÃO DE RISCOS NA SEGURANÇA E DEFESA DO CLA.....	104
5.2.1 Identificação, Análise e Avaliação de Riscos e Ameaças (Diagnóstico) no Contexto do CLA	105

5.2.2 Tratamento e monitoramento contínuo de riscos no CLA	107
5.3 A ATIVIDADE DE INTELIGÊNCIA NO APOIO À SEGURANÇA E DEFESA DO CLA.....	108
5.4 O SUPORTE INTEGRADO DE SEGURANÇA DAS INSTALAÇÕES (SISI) COMO MODELO NORMATIVO PARA A MODERNIZAÇÃO DA SEGDEF NO CLA.....	109
5.5 PROPOSTA DE UM PLANO DIRETOR DE SEGURANÇA ESTRATÉGICA (PDSE) PARA O CLA: CONSOLIDANDO A OTIMIZAÇÃO DA SEGDEF.....	111
6 CONCLUSÃO.....	115
REFERENCIAS	118
ANEXO I –APRESENTAÇÃO DE PROPOSTA PARA O MANUAL DE SEGURANÇA E DEFESA PARA OPERAÇÕES DE LANÇAMENTO NO CENTRO DE LANÇAMENTO DE ALCÂNTAR	124
ANEXO II – APROVAÇÃO DO MANUAL DE SEGURANÇA E DEFESA PELO CENTRO DE LANÇAMENTO DE ALCÂNTARA	125
ANEXO III – PORTARIA DE APROVAÇÃO DO MANUAL DE SEGURANÇA E DEFESA PELO CENTRO DE LANÇAMENTO DE ALCÂNTARA	126

1 INTRODUÇÃO

O domínio aeroespacial é uma área que carrega crescentes importâncias estratégicas para os países, dado que é constantemente interligado aos mais recentes avanços científicos e tecnológicos que fazem o progresso da humanidade. De igual modo, o avanço da tecnologia, em adição ao crescente uso de plataformas espaciais, revela que a defesa e a projeção do poder soberano de uma nação dominar a atmosfera e o espaço se tornaram centrais para uma diversidade de atividades. Assim, Poder Aeroespacial ganha destaque, simbolizando a habilidade de um país de empregar de maneira integrada os domínios aéreos e espaciais para atingir seus objetivos nacionais.

As crescentes complexidades do cenário aeroespacial global, juntamente com o aumento da competição entre as nações e a prevenção de ameaças multifacetadas, destacam a relevância estratégica de ações como o Centro de Lançamento de Alcântara (CLA) para o Poder Aeroespacial Brasileiro. O CLA, com sua singularidade geográfica e competitiva, desempenha um papel essencial tanto no Programa Espacial Brasileiro (PEB) quanto na projeção internacional do Brasil, particularmente após a ratificação de acordos como o Acordo de Salvaguardas Tecnológicas (AST). Nesse cenário, a Segurança e Defesa (SEGDEF) vai além da simples proteção física e reativa, firmando-se como um componente facilitador e amplificador das habilidades nacionais no setor espacial, tendo sua importância ainda mais destacada quando se considera seu alinhamento direto com os objetivos estratégicos da Força Aérea Brasileira (FAB).

A principal missão da Aeronáutica, de acordo com a Concepção Estratégica da Força Aérea 100 (DCA 11-45), é “manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da Pátria” (Brasil, 2018, p. 22). Nesse contexto, a SEGDEF efetiva do CLA, ao salvaguardar um recurso fundamental para a exploração espacial, assume um papel relevante na capacidade da FAB de supervisionar e controlar o espaço aéreo, evidenciar sua atuação e facilitar a integração nacional por meio de tecnologias espaciais, fortalecendo, assim, a soberania e a defesa da nação.

Adicionalmente, a mesma DCA 11-45 apresenta a visão da FAB de ser “uma força aérea de grande capacidade dissuasória, operacionalmente moderna e atuando de forma integrada para a defesa dos interesses nacionais” (Brasil, 2018, p. 22), sendo diretamente apoiada pela segurança de suas infraestruturas críticas.

Um CLA seguro e confiável é fundamental para o domínio da modernização da Força, proteção de tecnologias avançadas, um dos desafios destacados pelo DCA 11-45, e

demonstração de uma capacidade dissuasória crível no aeroespacial, particularmente no âmbito de acordos internacionais como AST. De acordo com o DCA 11-45, a capacidade de dissuasão é fundamental para encorajar possíveis ataques e se baseia na disponibilidade e prontidão de recursos militares específicos. Assim, a habilidade de exercer o Poder Aeroespacial é essencial não apenas para a defesa, mas também para o avanço científico-tecnológico e para a participação do Brasil no cenário global.

A materialização e a sustentação do Poder Aeroespacial dependem de uma complexa rede de capacidades, que vai muito além dos vetores aéreos e espaciais. Um dos pilares fundamentais é a SEGDEF de toda a infraestrutura, do pessoal, do conhecimento e das operações que o tornam possível. A Diretriz do Comando da Aeronáutica (DCA) 205-4/2020, que versa sobre a SEGDEF no Comando da Aeronáutica (COMAER), serve como documento basilar para orientar a execução eficiente da SEGDEF das instalações, equipamentos e pessoal. Os termos “segurança” e “defesa” são, portanto, cruciais para as medidas de proteção das instalações de interesse do COMAER (Brasil, 2020, p. 7).

À luz desses conceitos, entende-se, num sentido mais amplo, que segurança é uma necessidade, uma aspiração e um direito inalienável do ser humano, enquanto defesa é um ato ou conjunto de atos realizados para obter ou resguardar as condições reconhecidas como segurança. Assim, Segurança e Defesa englobam o conjunto de Ações de Força Aérea que contribuem para a preservação do poder de combate da FAB. Consiste na consecução de ações defensivas, ofensivas e de proteção, a fim de garantir o grau de segurança desejado. (Brasil, 2020, p. 7).

Cabe ressaltar que as atividades de SEGDEF no âmbito do CLA são de responsabilidade do Grupo de Segurança e Defesa de Alcântara (GSD-AK), conforme preconiza a DCA 205-4/2020, parafraseando: “uma Unidade de Segurança e Defesa (USEGDEF) do COMAER, Contingente de Infantaria da Aeronáutica, cuja atuação abarca as Ações de Segurança das Instalações, Polícia da Aeronáutica e Autodefesa de Superfície.” (Brasil, 2020, p. 9).

Alinhada com essa perspectiva, a Norma de Sistema do Comando da Aeronáutica (NSCA) 205-3/2024, que aborda o Sistema de Segurança e Defesa (SISDE) do COMAER, determina que esse sistema “tem o objetivo de preservar o poder combatente da Força Aérea Brasileira (FAB), por meio de atividades de superfície, defensivas e específicas, garantindo o grau de segurança desejado para as Operações Aéreas” (Brasil, 2024, p. 3). A finalidade do SISDE é “padronizar, por meio de normas e recomendações emitidas pelo Órgão Central, os procedimentos relativos ao planejamento e à condução das medidas de SEGDEF” (Brasil, 2024, p. 6).

Como a SEGDEF abrange vários segmentos institucionais, seu desenvolvimento deve ser feito de forma sistêmica (Brasil, 2020, p. 7), o que torna essencial um planejamento estratégico e abrangente para proteger as infraestruturas críticas. Desse modo, a SEGDEF vai além de um simples apoio, estabelecendo-se como um pilar que assegura a proteção de pessoal, instalações e equipamentos estratégicos, propiciando a própria existência e efetividade do Poder Aeroespacial.

O CLA, criado através do Decreto nº 88.136, datado de 1º de março de 1983, é uma organização militar brasileira (OM) vinculada ao COMAER e, dentre seus maiores propósitos, vale ressaltar a prática e o auxílio a ações de lançamento e rastreamento de veículos aeroespaciais, bem como a condução de testes e experiências importantes para a área (UFMA, 2020).

A relevância estratégica do CLA, e por extensão do seu SEGDEF, é ampliada ao considerar os desafios duradouros que historicamente formaram o Programa Espacial Brasileiro (PEB). Oliveira (2015) destaca em sua pesquisa sobre os desafios do Brasil na criação de satélites nacionais que a “baixa prioridade que o Programa Espacial Brasileiro tem recebido [...] no que tange ao investimento em ciência e tecnologia” e o subfinanciamento teórico representam obstáculos consideráveis.

Oliveira (2015, p. 33) resalta como fatores que historicamente impediram o progresso independente do Brasil no setor espacial: “a forte barreira tecnológica imposta pelos países desenvolvidos”, “esvaziamento das equipes de engenharia do INPE e do DCTA” e “limitados resultados industriais da MECB”.

Considerando a escassez comum de verbas e o esforço contínuo para diminuir a nossa subordinação tecnológica, defender um recurso estratégico como o CLA não se resume a manter a segurança das operações. É fundamental salvaguardar os investimentos relevantes já realizados e assegurar que o Centro impulse a independência e o avanço da ciência e tecnologia aeroespacial no Brasil.

Uma SEGDEF robusta no CLA é imprescindível para preservar as competências conquistadas com muito trabalho e criar um ambiente confiável, atraindo o capital e as parcerias indispensáveis para o fortalecimento da nossa PEB.

Cumprе salientar ainda que a importância do CLA foi expandida com sua participação no mercado global de lançamentos por meio do AST com os EUA (promulgado pelo Decreto n.º 10.220, de 5 de fevereiro de 2020), o que ocorreu em um aumento específico nos desafios à sua SEGDEF.

Logo, conclui-se que o CLA é, em essência, uma manifestação tangível e um vetor de desenvolvimento do Poder Aeroespacial Brasileiro e que o recrudescimento da criminalidade em todo o país, as ações de violência e das invasões e roubos de armas em quartéis, bem como ameaças internacionais representadas pelo terrorismo, tornaram imperioso o aprofundamento de reflexões sobre o assunto, visando a uma atualização dos conceitos relacionados com a SEGDEF das Organizações Militares (OM) do COMAER, conforme preconiza a NSCA 205-3/2024 (Brasil, 2024, p. 3).

Ao mesmo tempo que possibilita o avanço comercial e tecnológico do CLA, o AST estabelece critérios de segurança rigorosos para proteger tecnologias sensíveis. Essas demandas podem expor ou piorar vulnerabilidades já existentes, exigindo uma reavaliação e um reforço constante das medidas de SEGDEF. A complexidade das operações no espaço e a necessidade de proteger informações e tecnologias essenciais colocam o CLA em uma variedade de riscos e a ausência de uma estratégia unificada e direcionada de SEGDEF pode comprometer a integridade das instalações, as operações e a imagem internacional do Brasil.

A operação de um sistema sociotécnico de alto risco, como um centro de lançamento, um ambiente sujeito a acidentes constantes, de acordo com Perrow (1999), demanda uma cultura de segurança que esteja presente em toda a organização. A análise desse ambiente por meio da Teoria das Organizações de Alta Confiabilidade (HRO), proposta por Weick e Sutcliffe (2007), é essencial para entender a importância de uma atenção coletiva integral e um foco contínuo na prevenção de falhas, além do mero cumprimento formal de procedimentos.

Somando-se ao exposto, a visão geopolítica da Astropolitik destaca ainda mais a importância do CLA. De acordo com a tese de Dolman (2001), quem controla a órbita baixa da Terra, controla o espaço próximo à Terra. Quem domina o espaço próximo à Terra, domina o mundo. O CLA, por suas vantagens geográficas ímpares, oferece ao Brasil um dos acessos mais eficientes do mundo a esta região orbital estratégica e a SEGDEF do Centro, portanto, não se resume a proteger uma instalação militar; trata-se de salvaguardar o principal ativo geopolítico do Brasil na arena mais crítica do futuro.

Embora seja de grande importância, a arquitetura de SEGDEF do CLA, historicamente baseada em um modelo reativo e voltado para a proteção do patrimônio - um legado da Era Industrial, segundo Mandarini (2005), enfrenta dificuldades para se adaptar completamente à complexidade da Era do Conhecimento. A segurança de ativos intangíveis, como o saber, a proteção internacional e a continuidade das operações, requer uma estratégia sistêmica e proativa, baseada na gestão de riscos e na prevenção de perdas. A salvaguarda de ativos

intangíveis - como o conhecimento estratégico, a proteção internacional e a própria continuidade operacional - demanda uma abordagem de segurança que seja, ao mesmo tempo, sistêmica e proativa. Uma estratégia meramente reativa, baseada apenas na prevenção de perdas, é insuficiente. A ausência de um plano totalmente integrado e orientado não é uma falha trivial; ela compromete diretamente a integridade das operações, mina a confiança de parceiros internacionais e, em última instância, incapacita o CLA de cumprir seu papel fundamental no Poder Aeroespacial.

Considerando a importância de garantir a funcionalidade e a proteção de um ativo crucial como o CLA, bem como o papel essencial da SEGDEF na sustentação do Poder Aeroespacial, surge a seguir o problema de pesquisa: De que forma a Segurança e Defesa (SEGDEF) do Centro de Lançamento de Alcântara (CLA), quando otimizada pelos preceitos da Segurança Corporativa Estratégica (SCorpE), pode consolidar o Poder Aeroespacial Brasileiro e fortalecer a soberania nacional?

O objetivo principal deste estudo é avaliar a SEGDEF no CLA para sugerir um modelo de otimização estratégica que aumente a proteção, resiliência e capacidade operacional. Isso deve estar em conformidade com o Poder Aeroespacial Brasileiro, com as diretrizes do COMAER e com os princípios da Segurança Corporativa Estratégica (SCorpE), adaptados ao contexto militar e às particularidades do COMAER.

Para atingir o objetivo principal, este estudo propõe descrever o CLA, sua relevância estratégica no âmbito do Poder Aeroespacial Brasileiro e os desafios atuais à sua SEGDEF, incluindo as consequências do AST; fundamentar a SEGDEF como uma dimensão crucial do Poder Aeroespacial Brasileiro, detalhando seu impacto e a estrutura normativa do COMAER; apresentar os princípios da SCorpE como um referencial teórico para a otimização da SEGDEF; diretrizes e recomendações para a melhoria da estrutura, dos processos e dos recursos elaborados de SEGDEF no CLA, com base na aplicação do SCorpE e em uma abordagem estratégica para a gestão de riscos.

A principal hipótese que orienta este estudo é que uma implementação não otimizada dos princípios de SEGDEF no CLA, combinada com uma possível desconexão de seu papel como componente essencial do Poder Aeroespacial, prejudica a gestão eficiente de riscos e, por consequência, a plena capacidade operacional e a confiança de parceiros estratégicos. Essa circunstância pode levar a consequências diretas e relevantes na proteção de pessoal, instalações, equipamentos estratégicos e, acima de tudo, na continuidade e eficácia das operações do CLA. A confirmação dessas situações indica a necessidade de uma estratégia unificada e integrada para a SEGDEF no CLA.

A delimitação da pesquisa foca na avaliação da SEGDEF no CLA, considerando a doutrina do COMAER e utilizando o referencial teórico da SCorpE. Apesar de o Poder Aeroespacial e a SEGDEF serem assuntos abrangentes, este estudo concentra-se especificamente no CLA como caso de estudo, sem explorar outros Centros de Lançamento ou todas as Ações da Força Aérea que integram a SEGDEF, mas apenas aqueles relevantes para a proteção de uma infraestrutura crítica aeroespacial.

A relevância prática e teórica desta pesquisa é diversificada. Em termos práticos, as sugestões de otimização aqui têm como objetivo fornecer apoio concreto ao COMAER, com possíveis efeitos na eficácia da proteção do CLA, na adesão a acordos internacionais e na criação de uma mentalidade de defesa sólida e proativa. As recomendações abrangem a criação e execução eficaz de um Plano Diretor de Segurança Estratégica (PDSE) para o CLA, a priorização da adoção do modelo Suporte Integrado de Segurança das Instalações (SISI), a reformulação do Curso de Preparação para Operações de Lançamento (CPOL) com um módulo obrigatório de SEGDEF, além do fortalecimento constante da gestão de riscos e inteligência de segurança.

Do ponto de vista acadêmico, as principais contribuições estão na utilização do SCorpE no contexto específico de uma infraestrutura aeroespacial crítica, no fortalecimento da SEGDEF como um elemento estratégico na gestão de riscos e prevenção de perdas, na avaliação das consequências do AST para a segurança do CLA e na sugestão de um modelo de otimização materializado no PDSE. Como resultado técnico-tecnológico desta dissertação, em alinhamento com as diretrizes da UNIFA, as fundamentações para este PDSE são apresentadas como uma proposta de Manual de Segurança e Defesa para o Centro de Lançamento de Alcântara.

Este estudo é uma pesquisa qualitativa de natureza descritivo-analítica, empregando uma estratégia de estudo de caso único (Yin, 2001; Martins, 2006). A abordagem qualitativa é adequada para descrever a complexidade de problemas e compreender processos dinâmicos, como a gestão da segurança em uma organização de alta tecnologia (Cellard, 2014).

O CLA foi selecionado como caso único por ser um caso crítico e revelador para a análise da SEGDEF aeroespacial no Brasil (Yin, 2001). Sua relevância estratégica única, sua condição de infraestrutura crítica nacional e a complexidade dos desafios de segurança que enfrentam, intensificados por acordos internacionais, fazem dele um objeto de estudo cuja avaliação detalhada possibilita a geração de insights relevantes e a proposição de um modelo otimizado com ampla aplicabilidade prática.

A pesquisa foi realizada por meio de um estudo bibliográfico e documental aprofundado. A análise da literatura especializada em SCorpE, Estudos de Defesa, Gestão Estratégica e geopolítica do setor espacial foi parte da pesquisa bibliográfica. A pesquisa documental focou-se em normativas, diretrizes e planos estratégicos do COMAER, bem como em documentos relacionados ao CLA e ao AST (Cellard, 2014).

A pesquisa documental focou-se em normativas, diretrizes e planos estratégicos do COMAER, incluindo a DCA 205-4/2020 (Diretriz de Segurança e Defesa), a NSCA 205-3/2024 (Sistema de Segurança e Defesa do COMAER), a PCA 11-47 (Plano Estratégico Militar da Aeronáutica – PEMAER) e a DCA 205-9 (Suporte Integrado de Segurança das Instalações – SISI). Também foram incluídos documentos que regulamentam a formação e a capacitação de pessoal, como o TCA 37-15 (Cursos do DCTA para o ano de 2025).

Para garantir a precisão científica e a possibilidade de replicação, o estudo segue um procedimento organizado em três etapas principais:

Tabela 1 - Fases da Investigação Metodológica.

Fase	Objetivos e Atividades Principais	Capítulos Correspondentes
Fase 1 – Revisão Teórico-Documental e Contextualização	Coleta e análise sistemática de material bibliográfico e documental para estabelecer o referencial teórico (SCorpE), compreender o arcabouço normativo da FAB e descrever o contexto estratégico do CLA.	Capítulos 2, 3 e 4
Fase 2 – Construção do Diagnóstico de Segurança	Execução de um diagnóstico abrangente das vulnerabilidades e ameaças específicas do CLA à luz da SCorpE e das normativas. Incluiu a identificação de ativos críticos, análise e avaliação de riscos.	Seções iniciais do Capítulo 5
Fase 3 – Elaboração da Proposta de Otimização	Desenvolvimento de diretrizes e recomendações para a otimização da SEGDEF no CLA, culminando na proposição de um Plano Diretor de Segurança Estratégica (PDSE).	Seções finais do Capítulo 5 e Conclusão (Capítulo 6)

Fonte: O Autor.

Para abordar esses pontos, este estudo está organizado em seis capítulos, de acordo com as diretrizes para trabalhos acadêmicos da Universidade da Força Aérea (UNIFA, 2024).

O primeiro capítulo, que é esta introdução, fornece o contexto do tema da SEGDEF no CLA e sua conexão com o Poder Aeroespacial Brasileiro. Além disso, define o problema de pesquisa, estabelece os objetivos gerais e específicos, apresenta a justificativa da escolha

do tema, delimita o estudo, descreve a metodologia utilizada e expõe as questões centrais que orientam a pesquisa.

O Capítulo 2 analisa o objeto principal do estudo, apresentando o CLA, seu contexto operacional e sua relevância estratégica para o Brasil. Além disso, examina os desafios atuais à sua SEGDEF, com foco nas consequências e demandas decorrentes do AST firmado com os Estados Unidos.

O Capítulo 3 concentra-se na definição da SEGDEF como uma dimensão essencial do Poder Aeroespacial Brasileiro. Este capítulo examina o efeito da SEGDEF na habilidade aeroespacial do país e analisa a configuração doutrinária e normativa do COMAER, que a sustenta e direciona.

O Capítulo 4 se concentra na exposição dos princípios da SCorPE, fundamentada nas pesquisas de Marcos Mandarini (2005) e outros autores. Este capítulo define o referencial teórico que será empregado para analisar e sugerir melhorias na gestão da SEGDEF no contexto específico do CLA.

O Capítulo 5, por sua vez, aplica o referencial teórico de forma prática, examinando a SEGDEF do CLA com base nos princípios da SCorPE. Com base nessa avaliação, são sugeridas orientações para aprimorar a estrutura, os processos e os recursos do SEGDEF no Centro, incluindo estratégias para o planejamento estratégico de segurança, gerenciamento de riscos e reforço das atividades de inteligência de segurança.

Por fim, o Capítulo 6 traz as conclusões da pesquisa, resumindo os principais resultados e respondendo à questão da pesquisa e aos objetivos propostos. Serão abordadas as contribuições do estudo, suas limitações e recomendações para a FAB evoluindo o aperfeiçoamento da SEGDEF no CLA, além de propostas para pesquisas futuras no campo.

Portanto, este estudo está alinhado com a linha de pesquisa Poder Aeroespacial Brasileiro, Segurança e Defesa do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA), sendo essencial desenvolver pesquisas e estratégias que melhorem a SEGDEF na FAB, com atenção especial ao CLA, visando fortalecer a infraestrutura espacial do Brasil e a importância da defesa nacional.

2 A IMPORTÂNCIA ESTRATÉGICA DO CENTRO DE LANÇAMENTO DE ALCÂNTARA (CLA) PARA O PODER AEROESPACIAL BRASILEIRO

A partir do final do século XX, houve uma mudança significativa no setor aeroespacial, caracterizada pela introdução de novos armamentos e métodos de uso, como o uso de drones e maior utilização de plataformas espaciais resultando na redefinição das capacidades militares e na projeção de poder das nações. Nesse cenário, a atmosfera deixou de ser uma barreira restritiva, e o espaço exterior consolidou-se como um campo de atuação militar. O entendimento contemporâneo, portanto, é que “a guerra no ar e no espaço não mais se restringe aos enfrentamentos entre aeronaves”, exigindo uma concepção doutrinária que abranja as potencialidades advindas de ambos os domínios (Brasil, 2024, p. 23).

O conceito de Poder Aéreo, precursor da noção mais ampla de Poder Aeroespacial, foi definido por teóricos como William Mitchell como a habilidade de fazer algo no ar ou pelo ar (Rosa, 2014). A nova Doutrina Básica da Força Aérea Brasileira formaliza a evolução desse pensamento, afirmando que “a inclusão da dimensão do espaço exterior e do ciberespaço, conjugados à dimensão aérea, transformam-na em Teoria do Poder Aeroespacial” (Brasil, 2024, p. 23). Dessa forma, o termo tornou-se mais empregado para unir as características distintas dos setores que operam dentro e fora da atmosfera.

O Poder Aeroespacial é definido como “a expressão do Poder Nacional resultante da integração dos recursos de que a Nação dispõe para a utilização do espaço aéreo e do espaço exterior” (Brasil, 2024, p. 25). Fica nítida, portanto, a divisão conceitual: o setor aéreo abrange os elementos que operam na atmosfera terrestre, ao passo que o setor espacial engloba os componentes que atuam além dela, expandindo os impactos das ações aéreas e terrestres.

O ponto de partida é entender de onde vem e onde se encaixa o Poder Aeroespacial. Primeiro, é preciso vê-lo como uma evolução, um passo adiante do que era o Poder Aéreo. Segundo, ele é parte de um todo muito maior, o Poder Nacional. Para facilitar a análise, tradicionalmente o Poder Nacional é dividido em cinco grandes dimensões: a Política, a Econômica, a Psicossocial, a Científico-Tecnológica e a Militar. E é dentro desta última, a dimensão militar, que a coisa toda se ramifica novamente. Segundo Mesquita (2018), ela se desdobra para atuar nos diferentes ambientes, dando origem ao Poder Aeroespacial, ao Poder Terrestre e ao Poder Naval.

O Poder Aeroespacial, conforme descrito na Doutrina Básica da Força Aérea Brasileira (Brasil, 2024), tem a habilidade de impactar diretamente os centros de gravidade do oponente. Por meio de Tarefas como a Interdição, a doutrina prevê o emprego de meios

aéreos para “destruir ou neutralizar as fontes do poder inimigo” e realizar “ataques estratégicos em centros de gravidade do inimigo”, o que constitui uma estratégia fundamental na condução de conflitos (Brasil, 2024, p. 36). Para minimizar erros, essas operações exigem um planejamento baseado em um sistema de informações eficiente (Inteligência) (Mesquita, 2018).

Segundo Almeida (2006), o poder aeroespacial é considerado o principal vetor de projeção de força das grandes potências contemporâneas, como os Estados Unidos, devido à sua favorável relação de custo-benefício em termos de baixo risco e mínimas perdas humanas. Esta forma de poder é particularmente relevante para uma nação que enfrenta cenários variados e imprevisíveis, pois integra de maneira clara os pilares do poder nacional - militar, econômico, tecnológico e científico – e está intrinsecamente conectada a centros de pesquisa e desenvolvimento e a instituições militares.

A emergência do poder aeroespacial está historicamente relacionada à corrida espacial no período da Guerra Fria, quando houve competição entre os Estados Unidos e a União Soviética pela exploração do espaço. A possibilidade de conflitos no espaço, com o uso de satélites, missões balísticas, plataformas armadas e naves espaciais, foi inaugurada com o lançamento do satélite Sputnik pelos soviéticos em outubro de 1957. Essa nova arena de confronto levou a uma intensa busca por armamentos aeroespaciais avançados, com o objetivo de alcançar a supremacia militar, tendo como resultado o surgimento desse poder teve um impacto significativo na estratégia militar, na diplomacia, na economia, na ciência e na política internacional (Almeida, 2006).

Quando se trata da evolução do poder aeroespacial no Brasil ao longo do século XX tem se diversos marcos significativos, logo no início do século, iniciou-se a fabricação artesanal de aeronaves simples para uso civil e militar e um momento emblemático ocorreu em 1910, com o voo do São Paulo, o primeiro avião inteiramente projetado e construído no Brasil, simbolizando o início da aviação nacional (Almeida, 2006).

Nas décadas de 1930 e 1940, houve tentativas importantes de estabelecer uma indústria aeronáutica, como a Companhia Nacional de Navegação Aérea. Contudo, foi a partir dos anos 1970, com o Projeto Brasil-Potência, que o país começou a se consolidar como uma potência industrial nesse setor, esse projeto visava modernizar as Forças Armadas e refletiu uma mudança na posição do Brasil como exportador de produtos industrializados (Almeida, 2006).

Ademais, o Brasil começou suas atividades espaciais em 1957, e a partir de 1964, especialmente durante o período militar, houve um esforço estruturado para aprimorar as

competências aeroespaciais, resultando em um poder aeroespacial mais robusto e influenciando a geopolítica e a estratégia nacional (Almeida, 2006).

Almeida (2006, p. 7) explica de forma contundente:

O poder aeroespacial representa o vetor mais privilegiado de projeção de força das grandes potências da atualidade, como, por exemplo, Estados Unidos, pelo fato de ser a opção de mais baixo risco em termos de custo-benefício e de perdas humanas mínimas, a que melhor corresponde aos mais multiformes e imprevisíveis cenários que se apresentam a uma nação. O poder aeroespacial combina e define, de forma inequívoca, a base de poder nacional, militar, econômico, tecnológico e científico, em íntima ligação aos centros de investigação e desenvolvimento e às instituições militares. Historicamente, esse poder surge com o advento da corrida espacial, momento em que EUA e União Soviética passam a competir pela conquista do espaço sideral dentro do contexto da guerra fria. Quando os russos puseram em órbita o satélite Sputnik, em outubro de 1957, abriu-se a possibilidade de se travar a guerra no espaço exterior com satélites, mísseis balísticos, plataformas armadas e espaçonaves. Essa nova possibilidade de confronto fora da Terra lançou norte-americanos e russos numa intensa busca por armas aeroespaciais cada vez mais sofisticadas, com o intuito de obter supremacia militar e, com isso, garantir a vitória no conflito global. Como consequência, esse novo poder teve um alto impacto na Estratégia Militar, na Diplomacia, na Economia, na Ciência e na Política Internacional. (Almeida, 2006, p. 7).

Segundo Lima (2024), o Poder Aeroespacial possibilita uma eficácia na defesa e na criação de áreas de influência territorial. Sua estrutura, relacionada ao voo, examina o território por meio da cartografia aérea e da contextualização regional, unindo diversas situações em um cenário geopolítico informacional variado, com elementos transformadores que impactam a política de defesa e as relações internacionais do país.

Almeida (2006) aponta seis elementos fundamentais para que um país tenha uma capacidade aeroespacial reconhecida: Aviação Civil; Infraestrutura Aeroespacial (abrangendo aeroportos, sistemas de controle de tráfego aéreo e bases de lançamento); Força Aérea; Complexo Científico-Tecnológico; Indústria Aeroespacial; e um Programa Espacial. O Brasil abriga todos esses componentes em diversos estágios de desenvolvimento, sendo que alguns já são vistos como bastante progressivos (Almeida, 2006).

2.1 O CENTRO ESPACIAL DE ALCÂNTARA (CEA) E CENTRO DE LANÇAMENTO DE ALCÂNTARA (CLA) COMO ATIVOS ESTRATÉGICOS

No Brasil, a autonomia e soberania no setor aeroespacial são refletidas na construção e operação de centros especializados, como o Centro de Lançamento de Alcântara (CLA), que desempenham um papel fundamental no fortalecimento do poder aeroespacial nacional. A integração entre o CLA e o mais amplo conceito de Centro Espacial de Alcântara (CEA)

fortalece o Poder Aeroespacial Brasileiro, permitindo ao país desenvolver uma presença mais robusta em atividades espaciais. Esse Centro não apenas apoia o desenvolvimento e a operação de satélites e lançamentos espaciais, mas também posicionam o Brasil como um parceiro estratégico e um player no mercado global de acesso ao espaço, contribuindo para a autonomia nacional e reduzindo a dependência de lançadores estrangeiros.

Conforme estabelece o Programa de Desenvolvimento Integrado para o Centro Espacial de Alcântara (PDI-CEA), a diferença entre o CEA e o CLA, resta, que no tocante que o CLA é uma organização militar (OM) que se vincula ao COMAER, e concebe-se o CEA como um complexo de infraestruturas, bens e serviços necessários para as atividades de lançamento de veículos espaciais suborbitais e orbitais, não militares, a partir do território brasileiro. O CEA tem como objetivos realizar:

Lançamentos comerciais nacionais e internacionais de veículos espaciais; lançamentos por aeronaves - air-launch a partir do Aeroporto de Alcântara; atividades de rastreamento e de recuperação de artefatos lançados de outros centros; atividades de desenvolvimento tecnológico; atividades industriais que se relacionem ao Setor Espacial Brasileiro; capacitação de capital humano; e turismo e conscientização da sociedade sobre o valor das atividades espaciais. (Brasil, p.15, 2022).

O CEA figura como uma das infraestruturas espaciais mais cruciais no cenário brasileiro, sendo que englobam uma série de elementos, como equipamentos terrestres, recursos logísticos, instalações, dispositivos espaciais, sistemas computacionais e ferramentas, todos empregados na condução das atividades espaciais nacionais e no ciclo de vida dos sistemas espaciais, isso abrange desde a construção até o lançamento de artefatos espaciais que viabilizam diversas aplicações no domínio espacial.

A consolidação efetiva do CEA coloca o Brasil como um protagonista notável no mercado global de lançamentos espaciais, enaltecendo que o Centro assume um papel crucial para estabelecer o Programa Espacial Brasileiro (PEB) como um programa de caráter estatal, transformando-se em uma infraestrutura espacial essencial e um recurso estratégico para a nação.

Embora as principais instalações do CEA estejam concentradas em Alcântara, no Maranhão, ele abrange uma série de infraestruturas espaciais distribuídas por todo o território nacional, além disso, o CEA impulsiona uma variedade de atividades ao seu redor, propiciando a instalação de centros de pesquisa, universidades e indústrias.

Por outro lado, o CLA é uma instituição militar brasileira associada ao Comando da Aeronáutica do Ministério da Defesa. Sua instituição se deu por meio do Decreto n.º 88.136, de 1º de março de 1983, com os principais objetivos de executar e apoiar atividades de

lançamento e acompanhamento de veículos aeroespaciais, além de realizar testes e experimentos de interesse do Ministério da Aeronáutica à época, no contexto da Política Nacional de Desenvolvimento Aeroespacial (UFMA, 2020).

O CLA surgiu como uma resposta estratégica às limitações operacionais e de expansão do Centro de Lançamento da Barreira do Inferno (CLBI), localizado em Natal – RN, onde o crescimento urbano ao redor do CLBI limitava gradualmente suas operações, tornando-o possivelmente insuficiente para as aspirações espaciais do país, portanto, a criação do CLA esteve diretamente relacionada à concepção da Missão Espacial Completa Brasileira (MECB) em 1980, sendo um de seus elementos essenciais.

Desde o planejamento inicial, havia uma perspectiva de uso do CLA para realizar atividades comerciais com outras partes. Em 1998, um acordo entre o Ministério da Aeronáutica, a Agência Espacial Brasileira (AEB) e a INFRAERO tinha como objetivo permitir a exploração comercial do Centro, no entanto, essa iniciativa não teve sucesso, e o convênio foi encerrado em 2001 (Andrade et al., 2018).

Embora tenha sido enfrentado esse revés, o Brasil continuou investindo na infraestrutura do CLA, mudando-o em um centro espacial que colocasse o país inicial no grupo restrito de Estados com capacidade de autônoma de lançamento. A obtenção dessa habilidade tem uma relevância estratégica significativa, tendo em vista que apenas alguns países, como Estados Unidos, Rússia, China, França, Japão e Índia, possuem o controle total do ciclo de produção espacial (Almeida, 2006).

Desde sua criação, calcula-se que o Brasil tenha investido cerca de R\$ 1,3 bilhão no desenvolvimento do CLA, somando os esportes da AEB e do COMAER. Durante sua trajetória, o CLA já executou o lançamento de mais de 500 artefatos espaciais em mais de cem campanhas de lançamento, segundo o Programa de Desenvolvimento Integrado para o Centro Espacial de Alcântara (PDI-CEA). Contudo, apesar dos investimentos consideráveis, o país ainda trabalha para fortalecer sua habilidade de lançar veículos orbitais de maneira autônoma (UFMA, 2020).

2.1.1 O CLA como Infraestrutura Estratégica

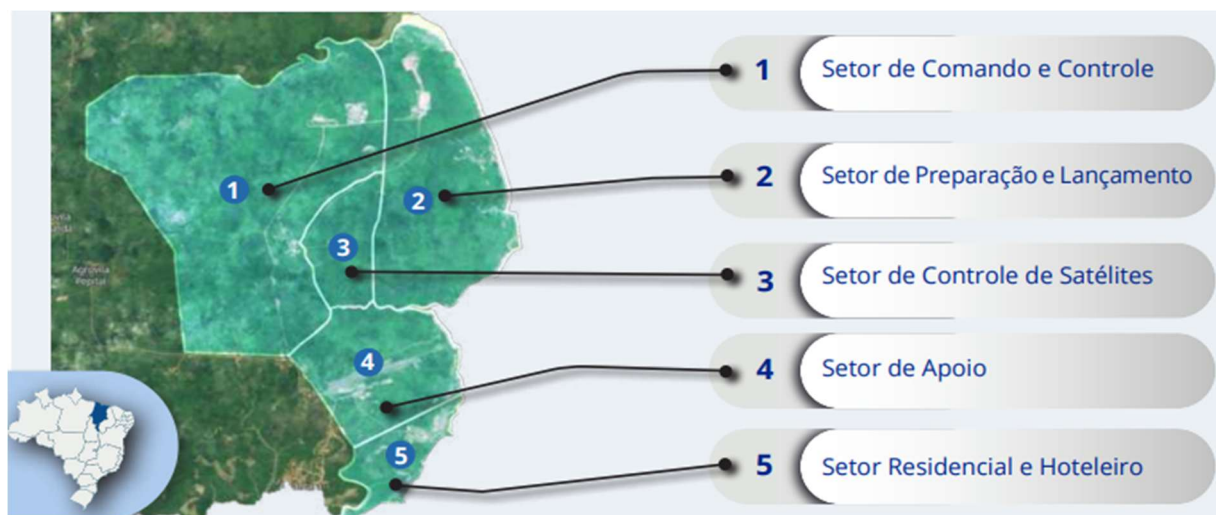
No âmbito da doutrina de defesa do Brasil, o CLA é reconhecido oficialmente como uma Infraestrutura Crítica (IC). Segundo o Decreto nº 9.573, de 22 de novembro de 2018 que aprovou a Política Nacional de Segurança de Infraestruturas Críticas, essas ações são descritas, *in verbis*:

Instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoca sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade (Brasil, 2018).

A defesa e segurança nacional dependente da proteção de IC's, dada a sua importância estratégica (Brasil, 2012) e a relevância do CLA resulta de diversos aspectos que transcendem a sua função militar. Em primeiro lugar, ele é um pilar da soberania nacional, proporcionando ao Brasil a autonomia para acesso ao espaço, uma habilidade possuída por um número restrito de países (Durão; Ceballos, 2011). Em segundo lugar, é um vetor fundamental para o avanço científico e tecnológico do país. Em terceiro lugar, representa um ativo econômico com a capacidade de posicionar o Brasil de maneira competitiva no mercado global de lançamentos, que gera centenas de bilhões de dólares por ano (Moura, 2021).

Em analogia ao conceito de “perdas”¹ definido por Mandarinini (2005), o comprometimento e/ou perda do CLA não resultaria somente em um prejuízo militar, mas em um retrocesso estratégico, tecnológico e econômico para o país. Em análise a infraestrutura do CLA, cumpre destacar que a mesma é complexa e distribuída em setores funcionais, cada um com um papel vital e requisitos de segurança específicos, sendo projetadas para suportar toda a cadeia de atividades de lançamento, desde a preparação até o rastreo, onde cada setor desempenha uma função vital e interdependente.

Figura 1 - Infraestrutura do CLA no município de Alcântara-MA.



Fonte: Brasil, 2022, p. 13.

¹ A Perda pode ser entendida como uma perda de ativos de qualquer natureza como consequência de dano real ou potencial, cujos efeitos, uma vez medidos e quantificados, expressem prejuízo pecuniário de qualquer monta (Mandarinini, 2005, p. 34).

O Setor de Preparação e Lançamento (SPL) funciona como o coração pulsante dessas operações. Sua peça central é a Torre Móvel de Integração (TMI) — reconstruída com modernos sistemas de segurança após o marco do acidente de 2003 — e outras áreas dedicadas a veículos de médio porte (Aguiar, 2018; Brasil, 2017). É ali que a montagem final e a contagem regressiva ganham vida, dentro de um perímetro protegido por instalações de apoio como o Prédio de Segurança e o Depósito de Propulsores.

Se o SPL é o coração, o Setor de Comando e Controle é o cérebro, o centro nevralgico de onde toda a missão é orquestrada. Ali, dados de telemetria, meteorologia e radares convergem para garantir uma tomada de decisão precisa e o controle total do voo (Brasil, 2013; AEB, 2021). Nenhum lançamento acontece sem a sua coordenação.

Paralelamente, o Prédio de Preparação de Carga Útil opera como um verdadeiro santuário tecnológico. Nesta instalação de segurança máxima e acesso restrito, o componente mais valioso da missão — o satélite — é preparado, testado e cuidadosamente integrado ao seu lançador (AEB, 2021).

Finalmente, o Aeroporto funciona como o grande portal logístico e estratégico do CLA. Sua pista de 2,6 quilômetros não apenas recebe as aeronaves de grande porte que transportam componentes e equipes, mas também posiciona Alcântara para o futuro, com capacidade projetada para operações de lançamento aéreo (*air-launch*), uma fronteira tecnológica em expansão (AEB, 2021). Juntos, esses setores formam uma engrenagem complexa, onde a falha em um componente compromete o sucesso de toda a missão, em resumo:

Tabela 2 - Principais Instalações do CLA em Alcântara-MA.

Setor / Instalação	Função Primária	Importância Estratégica
Setor de Preparação e Lançamento (SPL)	Montagem final, integração e lançamento de veículos espaciais.	Execução da missão; Segurança operacional crítica no “ponto zero”.
Setor de Comando e Controle	Gerenciamento centralizado, monitoramento e controle da missão em tempo real.	Tomada de decisão; Cérebro operacional que garante a segurança do voo.
Prédio de Preparação de Carga Útil	Preparação, teste e integração de satélites e outras cargas.	Proteção do ativo de maior valor (a carga útil); Garantia de sigilo.
Aeroporto	Recepção de grandes cargas e pessoal; Plataforma para futuras operações.	Logística vital para a viabilidade do centro; Vetor para expansão de capacidades.

Fonte: Adaptado da AEB (2021).

Conforme a Cartilha institucional do Centro de Lançamento de Alcântara (Brasil, 2016), além do complexo principal em Alcântara, o CLA conta, em São Luís, a capital, o CLA mantém um escritório que oferece apoio logístico e residencial para o efetivo, dispondo de um

Residencial Próprio Nacional, um Hotel de Trânsito para Oficiais e Suboficiais/Sargentos, clubes recreativos para ambos os níveis hierárquicos, e postos médico e odontológico, visando o bem-estar e suporte dos militares e servidores.

A terceira localidade é a Estação Redundante de Telemetria (ERT), situada no município de Raposa, Maranhão. Esse local atua como uma base de suporte essencial para o Centro de Lançamento de Alcântara, particularmente no que diz respeito ao monitoramento e à comunicação durante os lançamentos. A infraestrutura da ERT abrange uma estação de micro-ondas, uma subestação elétrica, moderada e o radar Atlas, um radar de alta precisão que suporta os radares de proximidade nas operações de lançamento (Brasil, 2016).

Além disso, a Ilha de Santana, situada no município de Humberto de Campos-MA, faz parte do complexo de instalações do CLA. O CLA usa este local apenas para operações de lançamento, executado como uma base remota fundamental para apoiar as missões de recuperação de cargas úteis (Brasil, 2022, p. 13).

Figura 2 - Infraestrutura do Complexo do CLA.



Fonte: Brasil (2022, p. 14).

O ritmo operacional do CLA tem aumentado, evidenciando sua importância crescente e a necessidade urgente de um modelo de segurança sólido. Um marco importante nesse processo ocorreu em 19 de março de 2023, quando foi realizado com sucesso o lançamento do foguete sul-coreano HANBIT-TLV, da empresa Innospace, durante a Operação Astrolábio (Padilha, 2023).

Esse evento foi marcante por ser o primeiro lançamento de uma empresa privada estrangeira originada de Alcântara. Naquele momento, o foguete foi transportado como carga

útil do Sistema de Navegação Inercial (SISNAV), uma tecnologia criada no Brasil (Padilha, 2023).

O êxito dessa operação confirmou que o Centro de Lançamento de Alcântara está plenamente apto para realizar lançamentos de foguetes, tanto nacionais quanto estrangeiros, com precisão e segurança em praticamente qualquer época do ano. No que diz respeito aos lançamentos orbitais planejados, a Innospace tem um lançamento previsto para 2025, de acordo com um anúncio de setembro de 2024. Contudo, as fontes não detalham que esses serão os primeiros lançamentos orbitais em parceria com a Innospace, nem especificam que levarão os cubesats Golds-UFSC (satélite do PEB) e Conasat-1 nesse ano (Brasil, 2025).

Essa internacionalização e o aumento do ritmo operacional do CLA elevam seu valor como um alvo estratégico e, conseqüentemente, a complexidade da sua proteção. Dessa forma, a segurança corporativa se manifesta como um pilar estratégico que influencia fatores financeiros e reputacionais. Para proteger os ativos e criar valor, é essencial conduzir uma gestão de riscos constante, com profissionais treinados e informados sobre as inovações do setor. As operações arriscadas e a complexidade das instalações de um centro de lançamento exigem um elevado padrão de segurança e uma atenção minuciosa aos detalhes.

2.1.2 Vantagens Geográficas e Comparativas do CLA

O Centro de Lançamento de Alcântara (CLA) apresenta um leque de benefícios que o estabelecem como um ponto chave para o envio de artefatos espaciais. Um dos principais é sua localização no litoral maranhense, que oferece mais segurança para lançamentos direcionados ao quadrante norte-leste, abrindo caminho para órbitas polares, inclinadas e, notavelmente, equatoriais. Nas fases iniciais da decolagem, o veículo que parte do CLA cruza o Atlântico, o que diminui a necessidade de grandes ajustes para desviar de zonas povoadas e, por extensão, atenua os perigos envolvidos.

Dentre outras vantagens significativas, destacam-se (Choairy, 2000; UFMA, 2020; Brasil, 2022):

a) Proximidade da Linha do Equador: Situado a apenas 2°18" ao sul da linha do Equador, o CLA se beneficia da maior velocidade de rotação da Terra nessa região. Isso se traduz em uma significativa economia de propelente (até 30% em comparação com centros em latitudes mais elevadas) para alcançar órbitas equatoriais e de baixa inclinação, permitindo o lançamento de cargas úteis maiores ou o uso de veículos menos potentes. Mesmo para órbitas

mais inclinadas, essa localização confere vantagens sobre centros situados em latitudes mais elevadas.

b) Amplitude de Azimutes de Lançamento: O CLA oferece uma vasta gama de azimutes de lançamento, chegando a até 107° , o que proporciona flexibilidade na escolha de órbitas para diversas missões espaciais.

c) Segurança de Lançamento sobre o Oceano: A trajetória inicial sobre o oceano minimiza riscos para áreas povoadas.

d) Baixa Densidade de Tráfego Aéreo: A região possui um tráfego aéreo reduzido, facilitando a coordenação e a segurança das janelas de lançamento.

e) Condições Climáticas Favoráveis: O clima estável ao longo do ano permite uma maior previsibilidade e disponibilidade para operações de lançamento, incluindo responsive launches (lançamentos sob demanda).

f) Estabilidade Geológica: A área é geologicamente estável, com baixo risco sísmico, garantindo a integridade das instalações e a segurança das operações.

g) Baixa Densidade Demográfica: A reduzida população no entorno do CLA simplifica questões de segurança e minimiza os custos associados a eventuais processos de desapropriação ou evacuação.

h) Proximidade à Capital São Luís: A relativa proximidade da capital do estado, São Luís-MA, oferece suporte logístico importante para as operações do CLA.

Essas características consolidam o CLA como um ativo geoestratégico de grande valor para o Brasil e para a comunidade espacial internacional.

Figura 3 - Amplitude de azimutes de lançamentos.



Fonte: Brasil (2022, p. 9).

Para elevar a análise a um patamar superior, é necessário inserir o CLA em um quadro geopolítico que explique por que o acesso autônomo ao espaço é um imperativo estratégico. A teoria da Astropolitik, de Everett Dolman, oferece este enquadramento ao aplicar os princípios da geopolítica clássica (como o Heartland de Halford Mackinder e o poder marítimo de Alfred Mahan) ao domínio espacial. A tese central de Dolman é expressa em sua poderosa analogia: “Quem controla a órbita baixa da Terra, controla o espaço próximo à Terra. Quem controla o espaço próximo à Terra, controla o planeta” (Dolman, 2001, p. 14, tradução nossa).

A tese central de Dolman é expressa em sua poderosa analogia: “Quem controla a órbita baixa da Terra, controla o espaço próximo à Terra. Quem controla o espaço próximo à Terra, controla o planeta” (Dolman, 2001). Nesta visão, a órbita baixa terrestre (LEO) funciona como o Heartland estratégico do século XXI. O acesso garantido a esta região é fundamental para a projeção de poder militar, econômico e informacional.

A partir daí, as vantagens geográficas do CLA deixam de ser apenas um benefício econômico para se tornarem um ativo geopolítico de primeira ordem. O CLA oferece ao Brasil um dos acessos mais eficientes do mundo a este Heartland orbital. A segurança do CLA, portanto, não é apenas uma questão de proteger uma base da FAB; é uma questão de salvaguardar o principal ativo do Brasil na disputa geopolítica pelo domínio mais crítico do futuro.

2.1.3 O CLA como Pilar do Programa Espacial Brasileiro (PEB) e da Projeção Internacional

O CLA, com sua infraestrutura e capacidade operacional é essencial para que o Brasil possa desenvolver e lançar seus próprios satélites e veículos lançadores, garantindo autonomia no acesso ao espaço e reduzindo a dependência de serviços de lançamento de outros países, é representando um pilar estratégico para a autonomia e o desenvolvimento do PEB. Essa autonomia é vital não apenas para a soberania nacional, mas também para o desenvolvimento científico, tecnológico e econômico do país, permitindo a criação de aplicações espaciais em áreas estratégicas como comunicações, sensoriamento remoto, meteorologia e defesa.

Contudo, a jornada do PEB em direção a essa autonomia tem sido caracterizada por obstáculos consideráveis, que enfatizam ainda mais a importância estratégica do CLA e a necessidade urgente de sua proteção. A busca por autonomia e crescimento por meio do CLA torna-se ainda mais significativa ao se levar em conta o passado de dificuldades enfrentadas

pelo PEB. Oliveira (2015) indica que problemas como falta de financiamento, dependência tecnológica e fragilidades da base industrial têm sido obstáculos constantes.

Nesse cenário, a existência de um ativo como o CLA, que detém vantagens geográficas singulares e capacidade para diminuir a dependência externa em lançamentos, transforma-se em um pilar ainda mais essencial. Um CLA que seja eficiente e, sobretudo, seguro, constitui não só uma infraestrutura de lançamento, mas também um instrumento essencial para reduzir essas dependências, salvaguardar os investimentos nacionais e fortalecer a habilidade do Brasil de operar de maneira soberana no espaço.

A solidificação do CLA como um centro de lançamento seguro, eficaz e competitivo no mercado internacional pode resultar em retornos econômicos consideráveis ao Brasil, atrair investimentos em tecnologia avançada, impulsionar a produção nacional no setor aeroespacial e gerar postos de trabalho qualificados. Ademais, essas instalações não apenas atendem às necessidades militares da FAB, mas também promovem a pesquisa e o desenvolvimento em áreas que fortalecem a posição do Brasil no cenário espacial internacional.

A sólida SEGDEF do CLA não só resguarda os significativos investimentos feitos em sua infraestrutura, como também garante a habilidade nacional de continuar com projetos estratégicos, como a criação de satélites, além de estabelecer um ambiente seguro que atraia os investimentos e colaborações internacionais essenciais para vencer os obstáculos históricos do PEB.

Com todas essas vantagens, o CEA e o CLA têm papéis essenciais para garantir a segurança e defesa do espaço aéreo brasileiro, enquanto promovem a economia e o progresso tecnológico do país. A participação ativa no mercado global de lançamentos e nas parcerias espaciais aumenta a visibilidade internacional do Brasil, sua influência geopolítica e sua imagem como nação com tecnologia de ponta. Assim, o êxito do CLA está intimamente relacionado à habilidade do país em assegurar a segurança de suas operações e resguardar os ativos tecnológicos e intelectuais envolvidos. Este é um assunto que será explorado mais detalhadamente no próximo capítulo, particularmente no âmbito do Acordo de Salvaguardas Tecnológicas.

2.1.4 O Acidente de 2003 e Suas Lições para a Segurança

O PEB enfrentou seu pior revés em 22 de agosto de 2003, quando o Veículo Lançador de Satélites (VLS-1 V03) explodiu na plataforma de lançamento do CLA, causando a trágica morte de 21 (vinte e um) técnicos e engenheiros. O acidente, que aconteceu três dias antes do

lançamento programado, foi causado por uma ativação intempestiva de um dos motores do primeiro estágio, de acordo com o Relatório da Investigação do Acidente (Brasil, 2004).

A análise das informações coletadas durante a investigação conduziu às seguintes conclusões de caráter geral: (1) o acidente teve início com o funcionamento intempestivo, porém nominal, do propulsor A do primeiro estágio; (2) foram encontrados fortes indícios de que o funcionamento intempestivo do propulsor A tenha sido causado pelo acionamento, também intempestivo, de um dos detonadores do conjunto de ignição do referido propulsor. (Brasil, p. 99, 2004)

O relatório final da investigação, apesar de descartar sabotagem, indicou que falhas latentes e deterioração das condições de trabalho foram fatores que contribuíram. A prolongada convivência do projeto com a falta de recursos humanos e materiais pode ter levado a uma dificuldade cada vez maior em identificar a deterioração da segurança (Brasil, 2004). O trágico incidente funcionou como um lembrete doloroso da complexidade e dos perigos envolvidos na atividade aeroespacial, levando a uma revisão completa dos protocolos de segurança no CLA.

Figura 4 - Vista lateral da torre móvel de integração, lado dos propulsores C e D.



Fonte: BRASIL (2004, p. 36).

A análise dos fatores operacionais que contornaram o acidente de 2003 no CLA revela um conjunto de vulnerabilidades sistêmicas que transcendem falhas pontuais, vejamos:

FATOR OPERACIONAL

Há indicações de que a infra-estrutura de apoio, provida pelo CLA a campanhas de lançamento, com relação a recursos humanos e físicos possui pontos de fragilidade que devem ser minimizados; A segurança operacional do CLA, composta pela segurança de terra, de voo e de plataforma apresenta alguns pontos de fragilidade.; Foi constatada a necessidade de haver um melhor intercâmbio de informações entre as organizações participantes, inclusive com desconhecimento, por parte dos operadores do CTA, CLBI e INPE, de regras ou normas estabelecidas pelo CLA; Foi

observada a falta de um gerenciamento de risco, realizado de maneira formal e criteriosa, principalmente na condução das atividades de integração e preparação para o lançamento. (Brasil, 2004, p. 101)

Logo, verifica-se a relevância da segurança corporativa é destacada pela capacidade de evitar perdas financeiras significativas e pela promoção de um ambiente de trabalho seguro onde a falha humana é um ponto vulnerável, e as empresas necessitam investir em programas de capacitação, conscientização e simulações de ataques para preparar as equipes e a gestão de riscos envolve a identificação, avaliação e implementação de estratégias de mitigação.

2.1.5 O Ambiente Sociopolítico

A instalação do CLA no início dos anos 1980 ocorreu em um cenário social complexo e delicado, que gerou conflitos e afetou negativamente as comunidades tradicionais de Alcântara devido à remoção de várias famílias da área. Alcântara, município brasileiro, abriga a maior população quilombola do país, com 84,6% de seus habitantes se autodeclarando como tal. A instalação da base na década de 1980 resultou na realocação de centenas de famílias de suas terras ancestrais, o que gerou um conflito territorial que durou quatro décadas.

Um acordo de conciliação significativo entre o Governo Federal e as comunidades quilombolas de Alcântara foi estabelecido em setembro de 2024, com a mediação da Advocacia-Geral da União (AGU). O acordo estabelece a titulação de uma área de 78.105 hectares para as comunidades, que, em troca, concordam com a continuidade do CLA em sua área atual de 9.256 hectares e se comprometem a não levantar novas questões jurídicas.

Este pacto transforma fundamentalmente a dinâmica de segurança do entorno. O paradigma de conflito latente é substituído por um de coexistência e gestão de interfaces, o que altera o perfil de risco, vejamos:

- I. **Redução de Ameaças:** A possibilidade de uma disputa legal de grande escala ou de ações destinadas a desestabilizar o Centro diminui significativamente, proporcionando ao CLA maior segurança jurídica e estabilidade operacional.
- II. **Novas Vulnerabilidades:** A proximidade e a interação contínua com as comunidades, que agora têm direitos territoriais reconhecidos formalmente, criam novas fragilidades. A maior complexidade no gerenciamento de acesso e, sobretudo, o perigo de que agentes mal-intencionados (como inteligência estrangeira e crime organizado) busquem utilizar as comunidades como uma fachada ou ponto de acesso para atividades de espionagem ou sabotagem.

Nesse cenário, a gestão da segurança do CLA deve levar em conta não só as ameaças externas, mas também a dinâmica social da região, a fim de estabelecer uma relação harmoniosa e cordial com as comunidades locais. Essa estratégia está em consonância com o conceito de análise de vizinhança na segurança corporativa, que enfatiza a importância do monitoramento contínuo e do fortalecimento de relações positivas com o ambiente externo para reduzir riscos e assegurar a proteção da organização.

2.2 O ACORDO DE SALVAGUARDAS TECNOLÓGICAS (AST) E A SEGURANÇA E DEFESA (SEGDEF) NO CLA

A inserção do CLA no mercado global de lançamentos comerciais, um objetivo estratégico para o Brasil, recebeu um impulso significativo com a confirmação do AST com os EUA. Embora esse acordo seja essencial para a viabilidade comercial do CLA, ele traz uma série de exigências e desafios importantes para a Segurança e Defesa do Centro. Este capítulo examinará o AST, suas consequências legais e operacionais, bem como as vulnerabilidades que ele revela ou cria, ligando esses problemas aos fundamentos da Segurança Corporativa Estratégica.

O mercado global de lançamento de satélites é amplamente dominado pela tecnologia americana. Acredita-se que a maioria dos equipamentos espaciais comerciais em todo o mundo contém peças fabricadas nos Estados Unidos. Nesse cenário, a negociação de um Acordo de Salvaguardas Tecnológicas (Andrade et al., 2018) tornou-se fundamental para que o Brasil pudesse utilizar o CLA de forma eficaz para lançamentos comerciais de artefatos com tecnologia americana.

Após longas negociações, o AST foi promulgado no Brasil pelo Decreto nº 10.220, de 5 de fevereiro de 2020. O acordo estabelece um pacto bilateral que visa proteger as tecnologias e patentes norte-americanas contra o uso ou cópia não autorizados durante as atividades de lançamento realizadas a partir do território brasileiro, especificamente do CLA. Ele define os procedimentos e requisitos técnicos que o Brasil deve cumprir para garantir que a tecnologia sensível dos EUA, presente em foguetes, espaçonaves, satélites e componentes, seja devidamente protegida contra acesso, manuseio ou replicação indevidos.

A importância do AST para o Brasil é imensa, podendo-se destacar:

Tabela 3 - Importância do AST para o Brasil

Benefício Estratégico	Descrição/Impacto
Viabilidade Comercial	Abre as portas do CLA para o lucrativo mercado de lançamentos comerciais, atraindo empresas e investimentos internacionais.
Desenvolvimento Tecnológico e Socioeconômico	Impulsiona a cadeia produtiva aeroespacial nacional e fomenta o desenvolvimento econômico e social na região de Alcântara.
Cooperação Internacional	Fortalece os laços de cooperação com os EUA no setor espacial.

Fonte: Adaptado de Bandeira (2020).

O acordo garante aos Estados Unidos a salvaguarda de sua tecnologia vital, um elemento fundamental de sua política externa e de segurança nacional. É fundamental destacar que o AST não inclui a transferência de tecnologia para o Brasil, nem autoriza o lançamento de artefatos bélicos a partir do CLA. Ademais, o Centro continua sob completa jurisdição e controle operacional do Brasil (Andrade et al., 2018).

No entanto, a condição para esses benefícios é a adoção de um sistema de segurança estrito. A exigência de aderir aos estritos protocolos do AST para a proteção de tecnologia estrangeira apresenta desafios diretos à implementação das diretrizes de SEGDEF do COMAER, como a DCA 205-4 e a NSCA 205-3. Situação no qual, harmonizar os procedimentos operacionais da FAB, os imperativos de soberania e as exigências de segurança dos parceiros internacionais requer uma interpretação e adaptação cuidadosa dessas diretrizes, o que aumenta a complexidade do planejamento e da execução da SEGDEF no CLA.

Esse regime de segurança demanda uma estratégia que incorpore os fundamentos da Segurança Corporativa Estratégica (SCorpE) para assegurar tanto a conformidade com o AST quanto a proteção eficiente dos ativos e a continuidade das operações. Este trabalho demonstrará a habilidade da instituição em proteger seus ativos intangíveis, como credibilidade e confiança dos colaboradores internacionais.

2.2.1 Implicações Legais, de Soberania e Propriedade Intelectual no Contexto do AST

Com a ratificação do Acordo de Salvaguardas Tecnológicas (AST) entre Brasil e Estados Unidos, houve o surgimento de novas perspectivas para o Centro de Lançamento de Alcântara (CLA), suscitando importantes discussões no âmbito legal, da soberania nacional e da proteção da propriedade intelectual quanto a natureza do acordo, que, via de regra, visa proteger tecnologias sensíveis de origem norte-americana, impondo uma série de direitos e

obrigações para ambas as partes, com reflexos diretos na operação e gestão da segurança no CLA.

Um dos aspectos fundamentais do AST diz respeito à determinação de áreas controladas dentro do CLA, em que equipamentos e tecnologias dos EUA serão manipulados e incorporados. Nessas regiões, o acesso será limitado e supervisionado, com procedimentos específicos para os indivíduos brasileiros e norte-americanos envolvidos. Apesar de o Brasil manter a jurisdição e controle soberano sobre todo o seu território, incluindo o CLA, a operação dessas áreas controladas requer uma colaboração estreita e o cumprimento rigoroso dos protocolos de segurança estabelecidos, a fim de evitar qualquer tipo de vazamento ou uso indevido de tecnologia protegida exigindo um sistema robusto de Segurança e Defesa (SEGDEF), especialmente nas áreas de Segurança de Pessoal e Segurança de Instalações (Silva et al., 2020).

No que tange à propriedade intelectual, o AST, especialmente em seu Artigo III, é explícito quanto à proteção das tecnologias norte-americanas. Isso significa que o Brasil se compromete a impedir a cópia, a engenharia reversa ou a transferência não autorizada de qualquer componente, software ou dado técnico dos EUA. Este compromisso tem implicações diretas para os procedimentos de segurança da documentação e do material, bem como para a segurança da informação no CLA. Conforme prevê Mandarinini (2005), a proteção de dados confidenciais e do conhecimento, um dos fundamentos da Segurança Corporativa Estratégica (SCorpE), se torna ainda mais crucial sob a égide do AST, onde qualquer erro nesse sentido pode resultar não apenas em prejuízos financeiros ou de reputação, mas também em graves consequências diplomáticas (Silva et al., 2020).

Durante o processo de aprovação do AST, um tema que gerou bastante debate foi a questão da soberania do país, situação no qual grupos da oposição e membros da comunidade civil manifestaram preocupação com a possibilidade do CLA se tornar muito dependente dos Estados Unidos, com risco de uma “americanização”, ou, de que os objetivos do Brasil fossem deixados de lado em favor dos interesses americanos. Contudo, a versão final aprovada do acordo busca equilibrar a importância de proteger a tecnologia com a manutenção da soberania nacional (Da Silva Oliveira, 2020).

É importante ressaltar que o Brasil mantém o controle sobre as operações de lançamento e o acesso às instalações, de acordo com os Artigos II e IV do acordo, ressaltando que o texto enfatiza que não há previsão para a instalação de bases militares estrangeiras, restringindo-se exclusivamente às atividades de lançamento, nem para a transferência de tecnologia dos EUA para o Brasil, conforme detalhado no Artigo III. No entanto, a

implementação efetiva da segurança, de acordo com os termos do acordo, representa um desafio para a habilidade do Estado brasileiro em administrar um ativo estratégico em colaboração com uma potência global, sem abrir mão de seus interesses soberanos (Andrade et al., 2018). Isso requer uma estrutura de segurança e inteligência bem organizada no CLA.

A confidencialidade das informações é outro ponto jurídico importante, o AST, em seu Artigo VI, prevê que informações militares classificadas trocadas entre as partes, ou relativas às tecnologias protegidas, sejam tratadas com o devido sigilo, em conformidade com o acordo bilateral de proteção de informações militares já existente entre Brasil e EUA. Isso traz dificuldades para a transparência e para o controle público das atividades no CLA, porém é uma exigência usual em acordos desse tipo, que envolvem tecnologia de uso dual (civil e militar) e interesses de segurança nacional (Da Silva Oliveira, 2020).

É nesse ponto que a análise estratégica encontra a governança prática. As implicações do AST exigem da FAB e das demais instituições uma gestão da segurança que vá além da proficiência técnica. É preciso uma consciência estratégica aguda dos deveres e direitos assumidos, no qual o sucesso desta empreitada - e a consolidação do CLA no cenário global - dependerá diretamente da habilidade brasileira de ser um guardião impecável de propriedade intelectual alheia, enquanto se projeta, sem ambiguidades, como o único soberano de seu destino aeroespacial.

2.3 VULNERABILIDADES E DESAFIOS À SEGDEF DO CLA SOB A ÓTICA DAS “PERDAS” COM AST

O Acordo de Salvaguardas Tecnológicas (AST), ao mesmo tempo em que representa uma oportunidade para o Centro de Lançamento de Alcântara (CLA), também expõe as vulnerabilidades existentes em sua SEGDEF e pode, inclusive, gerar novas complexidades. A necessidade de proteger tecnologia estrangeira de alto valor agregado eleva o nível de exigência sobre os sistemas de segurança do Centro. Qualquer falha pode resultar não apenas em prejuízos operacionais ou financeiros, mas também em “perdas” significativas especialmente quando vistas pela ótica da Segurança Corporativa Estratégica (SCorPE).

Proteger tecnologias estrangeiras de alto valor agregado impõe padrões mais rigorosos aos sistemas de segurança do Centro. Qualquer deslize não se limita a impactos operacionais ou financeiros; ele pode acarretar “perdas” profundas, especialmente quando vistas pela ótica da Segurança Corporativa Estratégica (SCorPE).

Mandarini (2005, p. 7) aborda a prevenção de perdas como uma das finalidades da atividade de segurança na Era do Conhecimento, embora não detalhe uma extensa tipologia de “perdas” nesses trechos específicos, o autor enfatiza que a segurança moderna visa a “administrar os riscos e as ameaças sobre as Pessoas e os Ativos (tangíveis e intangíveis)” e que o “dano efetivo ou potencial” (a perda) é o que se busca evitar ou minimizar.

Assim, a segurança, nessa perspectiva, concorre para a manutenção da regularidade, da normalidade e da continuidade da produção, e sua ausência ou ineficácia leva diretamente a perdas que afetam esses aspectos. Os Riscos Empresariais (inerentes à atividade) e os Riscos Não-Emprersariais (como crime, acidentes naturais, terrorismo, etc.) são as fontes dessas potenciais perdas e a SCorpE, ao gerenciar esses riscos, atua diretamente na prevenção das perdas deles decorrentes.

A natureza e a magnitude dessas potenciais “perdas” no contexto específico do CLA serão exploradas em maior detalhe no Capítulo 4, ao se analisar a aplicação dos diversos segmentos da SCorpE. Por ora, cumpre destacar os principais eixos de vulnerabilidade e desafios à SEGDEF do CLA, especialmente potencializados pelo Acordo de Salvaguardas Tecnológicas.

No contexto específico do CLA, um ativo estratégico para o Poder Aeroespacial Brasileiro e sujeito a acordos internacionais como o AST, o conceito de “perdas” de Mandarini se desdobra em múltiplas dimensões críticas:

Tabela 4 - Espectro de Perdas Potenciais no Centro de Lançamento de Alcântara (CLA)

Dimensão da Perda	Descrição e Exemplos Críticos no Contexto do CLA
Estratégicas e de Soberania	Comprometimento da capacidade de lançamento autônomo, enfraquecendo o Poder Aeroespacial; Redução do efeito dissuasório da FAB (DCA 11-45); Danos à credibilidade do Brasil como parceiro espacial internacional; Perda de autonomia tecnológica (contrário aos objetivos do PCA 11-47); Exposição a vulnerabilidades que afetem a segurança nacional.
Operacionais e Programáticas	Interrupção ou cancelamento de missões de lançamento; Atrasos nos cronogramas do Programa Estratégico de Sistemas Espaciais (PEB); Falha no cumprimento de metas estratégicas (PCA 11-47 e DCA 11-45).
De Conhecimento e Tecnológicas	Vazamento de informações técnicas sensíveis (projetos nacionais, tecnologias do AST); Perda de propriedade intelectual; Comprometimento de dados de comando, controle e telemetria.
De Recursos (Humanos, Materiais, Financeiros)	Danos ou destruição de ativos de alto valor (veículos lançadores, satélites, infraestrutura); Custos elevados de recuperação, reparos e investigações; Perda de vidas humanas ou ferimentos em pessoal técnico especializado.
Ambientais	Contaminação do ecossistema local decorrente de acidentes com propelentes ou outros materiais perigosos.
De Oportunidade	Incapacidade de atrair novas parcerias estratégicas ou contratos comerciais de lançamento devido a um histórico de falhas de segurança.

Fonte: O Autor.

Dessa forma, o AST não apenas exige medidas de segurança robustas, mas também serve como um catalisador para que o CLA adote uma perspectiva de SCorpE. A análise das vulnerabilidades sob a ótica da prevenção de perdas, conforme preconizado por Mandarinini (2005), é fundamental para direcionar os esforços e recursos da FAB na proteção eficaz deste ativo estratégico nacional, garantindo que as oportunidades trazidas pelo AST não sejam sobrepujadas por falhas de segurança e suas consequentes perdas.

Ao perscrutar as vulnerabilidades do CLA por meio dos diversos prismas da SCorpE, emerge um leque ainda mais vasto de “perdas” potenciais que a SEGDEF se esforça para conter – algo que exploraremos com mais detalhe nos capítulos vindouros.

3 A SEGURANÇA E DEFESA COMO ELEMENTO DO PODER AEROESPACIAL

O conceito de Poder Espacial aborda como a capacidade de um Estado de controlar e utilizar o espaço geográfico influencia sua autonomia e soberania. Nesse cenário, Aliberti, Cappella e Hrozensky (2019) dividem os elementos do poder aeroespacial (ou espacial, em sua análise) em duas categorias principais: Capacidade e Autonomia.

Figura 5 - Elementos do Poder Espacial



Fonte: Adaptado de Aliberti, Cappella e Hrozensky (2019).

A Capacidade representa tudo aquilo que um país consegue fazer, somando seus recursos, tanto os tangíveis quanto os intangíveis. Nas capacidades tangíveis, encontramos os elementos físicos: o Acesso ao Espaço, que é a habilidade de fisicamente alcançar e usar recursos em órbita; a Infraestrutura Terrestre, fundamental para sustentar as operações com redes de transporte e comunicação; e os Sistemas Espaciais Operacionais, como os satélites que já utilizamos para comunicação e monitoramento. Paralelamente, a Ciência e Exploração e a Consciência Situacional Espacial (SSA), que nos permitem monitorar ameaças e defender nossos ativos, também formam a base desse poder concreto.

Contudo, como salientam Aliberti et al. (2019), tais recursos físicos só atingem seu pleno potencial quando acompanhados de capacidades intangíveis. Nesse sentido, a formulação de políticas socioeconômicas capazes de transformar o potencial espacial em benefícios concretos para o desenvolvimento nacional é determinante. Essa visão reforça a ideia de que o

poder estatal não se limita à posse de meios, mas também à habilidade de integrá-los em estratégias coerentes e sustentáveis (Aliberti et al., 2019).

Além disso, a Ciência e Exploração se destaca, pois, a pesquisa e o desenvolvimento tecnológico são essenciais para aproveitar o espaço. O componente Consciência Situacional Espacial (SSA) e contra espaço se refere ao monitoramento de ameaças e a defesa de ativos espaciais. Já o Índice de Capacidades Intangíveis relaciona-se à Orientação das políticas socioeconômicas, que envolve a formulação de políticas que fomentem o desenvolvimento econômico e social em relação ao uso do espaço (Aliberti *et al.*, 2019).

A segunda categoria, Autonomia, é dividida em Índice de Autonomia Técnica e Índice de Autonomia Política. O Índice de Autonomia Técnica envolve a Fase de Produção, que trata da capacidade de um Estado de desenvolver sua própria tecnologia e manter independência na produção de bens essenciais; a Fase de Operação, que se refere à habilidade de operar de forma independente; e a Fase de Exploração, que analisa a capacidade de descobrir novos recursos ou territórios, tanto em termos econômicos quanto científicos (Aliberti *et al.*, 2019).

Por outro lado, o Índice de Autonomia Política abrange a Soberania Interna, que se relaciona ao controle sobre o território e à tomada de decisões sem interferências externas, e a Soberania Externa, que analisa a habilidade de um Estado de interagir com outros países no plano internacional, preservando sua autonomia.

Essa estrutura oferece uma análise abrangente de como a Capacidade e a Autonomia se interligam, refletindo a complexidade do poder que um Estado pode exercer em relação ao seu espaço geográfico e suas interações políticas e técnicas. Portanto, compreender esses elementos é fundamental para o planejamento e a formulação de estratégias nas relações internacionais e na defesa (Aliberti *et al.*, 2019).

Nesse panorama, o poder aeroespacial desponta como uma evolução natural do poder aéreo, assumindo papel central no cenário contemporâneo. Souza (2024) observa que o avanço acelerado da ciência e da tecnologia expandiu o campo de atuação dos Estados, de modo que os conflitos modernos já não se limitam às fronteiras terrestres. A capacidade de projetar força por meio de aeronaves e plataformas espaciais transformou profundamente as dinâmicas de guerra e as relações internacionais. A integração de recursos como comunicação via satélite e monitoramento contínuo da superfície terrestre oferece vantagem estratégica expressiva, permitindo acompanhar, em tempo real, as ações de aliados e adversários. Essa combinação de vigilância constante e capacidade de intervenção rápida posiciona o país em um patamar de superioridade que ultrapassa as formas tradicionais de combate militar.

Dentro dessa lógica, a utilização de satélites para monitoramento e vigilância, além de outros dispositivos aeroespaciais, tem se mostrado essencial para garantir a segurança e o domínio de um espaço aéreo e espacial. Essas ferramentas proporcionam uma capacidade de visualização e comunicação em tempos de paz, mas também oferecem vantagens táticas significativas em tempos de conflito. O monitoramento constante pode identificar atividades adversárias antes mesmo de uma ação militar ser iniciada, possibilitando intervenções precisas e com alta taxa de sucesso (Camargo; Souza, 2023).

Além disso, a utilização do poder aeroespacial não se limita à defesa militar, conforme apontado por Siqueira (2009), ele também tem um impacto significativo nas áreas de pesquisa científica, comunicação e economia. Por exemplo, a comunicação via satélite permite a conexão de regiões remotas do planeta, transformando a forma como países interagem e trocam informações. Além disso, o uso de satélites para monitoramento de recursos naturais, mudanças climáticas e desastres naturais também é um componente crucial das atividades de segurança nacional e da sustentabilidade ambiental. O domínio do espaço permite, assim, que um país obtenha vantagens tanto na defesa quanto no campo da inovação tecnológica.

Em um mundo cada vez mais globalizado, a rapidez em termos de intervenção militar e de ações de proteção pode fazer a diferença em muitos cenários. A combinação de velocidade, mobilidade e flexibilidade proporcionada pelas plataformas aeroespaciais permite que os países enfrentem ameaças complexas e dinâmicas, com a vantagem de poderem reagir com um mínimo de tempo de resposta. Isso é crucial em um cenário em que as ameaças podem surgir de diferentes frentes e em momentos imprevisíveis.

Do ponto de vista da economia, um poder aeroespacial bem desenvolvido tem implicações significativas. A indústria aeroespacial exige alta especialização e investimentos substanciais, mas também é um motor importante de inovação e crescimento econômico. O desenvolvimento de novas tecnologias aeroespaciais não só alimenta a capacidade de defesa de um país, mas também gera novos mercados e empregos. O Brasil, ao investir em seu programa espacial e nas tecnologias associadas, tem o potencial de diversificar sua economia e se posicionar como um líder regional na indústria aeroespacial (Dos Santos Lima, 2024).

É interessante observar que, no contexto geopolítico, o domínio do espaço e a capacidade de projetar poder através de plataformas aeroespaciais também têm impactos sobre a soberania e a autonomia de um país. Ao se tornar capaz de operar no espaço, um país não apenas garante sua segurança em território terrestre, mas também assegura a preservação de sua posição no cenário global. A crescente competição por recursos e influência no espaço é uma

realidade que faz com que o investimento em capacidades aeroespaciais se torne um componente essencial da política externa e da diplomacia de muitos países (Nogueira, 2014).

Nesse sentido, como observado anteriormente, o Poder Aeroespacial apresenta características específicas que o diferenciam dos outros elementos do Poder Militar, podendo tanto potencializar quanto limitar sua utilização. A Doutrina Básica da Força Aérea Brasileira (2024) atualiza a análise dessas particularidades, unificando os antigos conceitos de pontos fortes e pontos fracos, anteriormente usados, em um rol único de características do Poder Aeroespacial.

Essa nova abordagem reflete uma visão estratégica onde cada característica pode, a depender do preparo, da tecnologia e do contexto, atuar tanto como um potencializador da força quanto como uma vulnerabilidade a ser mitigada. A Tabela 5, a seguir, consolida essas características, alinhando-as à doutrina vigente.

Tabela 5 - Características do Poder Aeroespacial

Característica	Descrição e Implicação para a SEGDEF do CLA
Alcance	Capacidade de atingir objetivos a grandes distâncias. A SEGDEF garante a integridade das bases e sistemas que permitem projetar esse alcance a partir de Alcântara.
Flexibilidade/Versatilidade	Habilidade de mudar rapidamente de missões e táticas. A SEGDEF deve ser igualmente flexível para se adaptar a diferentes cenários operacionais e perfis de missão no CLA.
Mobilidade	Capacidade de desdobrar meios de forma rápida. A proteção das infraestruturas logísticas e de apoio do CLA é vital para assegurar essa mobilidade.
Penetração	Habilidade de adentrar território hostil. Depende da proteção de informações sensíveis (inteligência, planejamento) e tecnologias furtivas, tarefas centrais da SEGDEF.
Perspectiva	Capacidade de fornecer uma visão tridimensional e privilegiada do ambiente operacional. A SEGDEF protege os centros de comando e controle onde essa perspectiva é analisada e utilizada.
Precisão	Emprego de armamento com alto grau de acerto. A segurança dos sistemas de guiagem, dados de alvos e da cadeia de suprimentos de munições inteligentes é crítica.
Pronta-Resposta	Capacidade de reagir imediatamente a uma ameaça. Exige uma SEGDEF que garanta a disponibilidade e segurança contínua dos meios e da infraestrutura do CLA.

Tecnologia	O Poder Aeroespacial é inerentemente tecnológico. A SEGDEF é fundamental para proteger esse diferencial contra espionagem, sabotagem e ataques cibernéticos.
Velocidade	Capacidade de percorrer grandes distâncias em curto tempo. A segurança dos processos de preparação e lançamento garante que essa velocidade possa ser empregada sem atrasos.
Altos Custos	O elevado valor dos ativos (aeronaves, satélites, infraestrutura) torna a SEGDEF um investimento crucial para a prevenção de perdas catastróficas.
Dependência de Tecnologia	A sensibilidade a inovações e a dependência de sistemas complexos tornam a proteção de tecnologias e a cibersegurança tarefas vitais para a SEGDEF.
Dependência de Infraestrutura	A necessidade de bases especializadas como o CLA torna essas instalações um centro de gravidade e um alvo prioritário, exigindo o mais alto nível de proteção da SEGDEF.
Fragilidade	Os componentes aeroespaciais são inerentemente frágeis. A SEGDEF mitiga essa vulnerabilidade em solo, protegendo os meios contra danos acidentais ou intencionais.
Necessidade de C²	O emprego eficaz do Poder Aeroespacial demanda robustos sistemas de Comando e Controle, que são alvos prioritários e devem ser protegidos pela SEGDEF.
Necessidade de Inteligência	Operações precisas dependem de conhecimento profundo do adversário. A SEGDEF, por meio da contrainteligência, protege esse conhecimento e os meios que o produzem.
Permanência	A capacidade de se manter em operação é limitada. A SEGDEF contribui ao proteger a logística de reabastecimento e manutenção que permite estender a permanência.
Restrição de Carga Útil	A limitação na capacidade de carga exige otimização. A SEGDEF garante que os ativos de alto valor, mesmo em menor número, sejam protegidos eficazmente.
Suscetibilidade Meteorológica	As condições climáticas impactam as operações. A SEGDEF deve incluir em seus planos de contingência a proteção da infraestrutura contra eventos climáticos extremos.

Fonte: Adaptado de Doutrina Básica Da Força Aérea Brasileira (Brasil, 2024).

A Segurança e Defesa (SEGDEF) é crucial para potencializar as características vantajosas. Uma SEGDEF eficaz garante a disponibilidade e a integridade das bases de operação (um aspecto da Pronta-resposta e Mobilidade), protege as informações que permitem a Penetração e a Precisão, e assegura que os meios estejam aptos para exercer seu Alcance e Flexibilidade.

Ao mesmo tempo, a SEGDEF desempenha um papel vital na mitigação das características que representam vulnerabilidades, visando proteger os Altos Custos investidos, minimizando perdas por acidentes ou ações hostis, a proteção da Infraestrutura é uma de suas funções primordiais, assim como a salvaguarda da Tecnologia. A SEGDEF também busca reduzir a Fragilidade dos sistemas em solo por meio de medidas de proteção física e controle.

A análise dessas características do Poder Aeroespacial revela uma complexa interdependência com a segurança e a eficácia da sua infraestrutura terrestre. Pontos fortes como alcance, pronta-resposta e velocidade são diretamente potencializados pela disponibilidade e segurança de bases de lançamento e sistemas de controle bem protegidos. Contudo, pontos fracos como custos elevados, dependência de tecnologia e, crucialmente, dependência de infraestrutura sublinham a vulnerabilidade inerente.

Uma infraestrutura terrestre inadequada ou insegura pode anular as vantagens operacionais e agravar as fragilidades existentes. A dependência de infraestrutura, por exemplo, torna centros de lançamento como o CLA alvos estratégicos, cuja proteção contra ameaças físicas, cibernéticas ou por comprometimento interno é vital. A SEGDEF eficaz é, portanto, essencial para mitigar essa dependência, garantindo a integridade e a operacionalidade dessas instalações críticas.

A fragilidade dos componentes aeroespaciais também se estende à sua infraestrutura de solo, que, se comprometida, pode resultar em perdas catastróficas e na interrupção de programas estratégicos. Portanto, uma abordagem estratégica para a segurança dessas instalações, informada pelos princípios da SEGDEF, não é apenas uma medida de proteção patrimonial, mas um imperativo para a sustentabilidade e eficácia do Poder Aeroespacial como um todo.

A DCA 205-4, por exemplo, enfatiza que as medidas de SEGDEF têm o objetivo de “garantir a segurança das instalações, do material, dos equipamentos, dos suprimentos e do pessoal em grau compatível com a missão de cada OM, contribuindo para a conservação da capacidade operacional do COMAER” (Brasil, 2020, p. 6).

Isso se aplica diretamente à necessidade de proteger a infraestrutura que sustenta o Poder Aeroespacial.

A consolidação do Poder Aeroespacial de uma nação não se sustenta apenas pela capacidade de operar no ar e no espaço, mas também, e de forma crítica, pela segurança e resiliência de sua infraestrutura terrestre de apoio. Para o Brasil, e especificamente para o Centro de Lançamento de Alcântara (CLA), a segurança e defesa dessa infraestrutura é um componente indissociável da própria capacidade de exercer o Poder Espacial, com implicações diretas para a defesa nacional e a proteção de ativos estratégicos.

A SEGDEF no contexto da infraestrutura terrestre são aspectos fundamentais para garantir a soberania nacional, a proteção de ativos estratégicos e o funcionamento eficaz das operações militares e civis.

A infraestrutura terrestre que suporta as operações aeroespaciais, como centros de lançamento, bases de monitoramento e controle, redes de comunicação e sistemas logísticos, constitui-se como um conjunto de ativos de alto valor estratégico. Sua proteção é essencial para evitar sabotagens, espionagem, ataques cibernéticos ou qualquer forma de interferência que possa comprometer a mobilidade, a capacidade operacional das forças e a integridade das missões espaciais.

A Estratégia Nacional de Defesa (END) do Brasil preconiza a necessidade de dissuadir a concentração de forças hostis nas fronteiras terrestres e nos limites das águas jurisdicionais brasileiras, além de impedir o uso do espaço aéreo nacional. Isso depende diretamente da integridade e da segurança das instalações terrestres que viabilizam tais capacidades.

Rocha (2019) ressalta que, para assegurar a proteção de um país, são necessárias ações complexas que vão além da mera atuação militar, sendo imprescindível uma estrutura civil que forneça insumos e mão de obra, pois a falta desses recursos pode comprometer a capacidade de resposta militar.

Nesse contexto, a infraestrutura terrestre do CLA é classificada como uma infraestrutura crítica (IC), cuja interrupção ou destruição teria um impacto debilitante na segurança nacional, na economia, na capacidade de defesa e no moral da população. Conforme Sá (2017), as redes de infraestrutura crítica consistem em “sistemas interligados e distribuídos que fazem uso de recursos humanos e tecnológicos para satisfazer as demandas da população e das atividades comerciais e industriais”.

Rocha (2019) alerta para sua exposição a vulnerabilidades devido à sua dependência em relação a outros setores ou a outras infraestruturas críticas dentro do mesmo setor, além das vulnerabilidades próprias de cada uma. A falta de uma classificação de criticidade e de um plano, política ou marco legal para abordar a questão da infraestrutura crítica no Brasil, como

apontado por Reis et al. (2016), representa um desafio que precisa ser enfrentado para garantir a segurança do CLA.

A segurança da infraestrutura terrestre no CLA, portanto, transcende a mera proteção patrimonial, integrando-se diretamente à capacidade de defesa do Poder Aeroespacial. Isso envolve:

- I. **Proteção Física e Operacional:** Garantir a integridade das instalações contra intrusões, sabotagens ou ataques diretos é fundamental para preservar a capacidade de lançamento e proteger o pessoal envolvido. A implementação de barreiras perimetrais para isolar áreas de interesse, o patrulhamento constante do perímetro e a existência de uma força de reação com capacidade de pronta resposta, equipada com viaturas rápidas e um sistema de comunicação eficiente, conforme recomendado no Programa de Trabalho Anual do CLA (PTACLA, 2017), são medidas essenciais. A vulnerabilidade acentuada pela inexistência de limites físicos que delimitem o perímetro do CLA, criando um ambiente propício para arrombamentos e furtos, exige priorização na área patrimonial, buscando recursos e meios para garantir a segurança.
- II. **Proteção de Ativos Estratégicos e do Conhecimento:** A infraestrutura terrestre do CLA não apenas suporta operações, mas também abriga tecnologias sensíveis e conhecimento científico vital para o programa espacial. A segurança eficaz deve garantir a proteção desses ativos intangíveis contra espionagem ou acesso não autorizado.
- III. **Resiliência e Continuidade Operacional:** A capacidade de manter as operações essenciais ou de recuperá-las rapidamente após um incidente de segurança é crucial. Isso requer planos de contingência robustos e uma infraestrutura que possa absorver e se adaptar a perturbações.

A integração das operações aéreas e terrestres, como destacado pelo COMAER, é vital, exigindo coordenação meticulosa entre diferentes forças e a implementação de um sistema de comando unificado, essencial para assegurar uma resposta ágil e eficaz em situações de crise. A infraestrutura terrestre deve ser equipada com sistemas avançados de monitoramento e vigilância que incorporem tecnologias espaciais e aéreas, além de meios de comunicação e controle que facilitem a troca de informações, proporcionando uma visão abrangente do espaço aéreo e do território.

Em suma, a segurança da infraestrutura terrestre do CLA é um multiplicador de força para o Poder Aeroespacial Brasileiro. Sua eficácia não apenas protege os ativos físicos e humanos, mas também garante a credibilidade do Brasil como um parceiro confiável no cenário espacial internacional, sustenta a soberania nacional e contribui para a capacidade dissuasória do país.

3.1 A SEGURANÇA E DEFESA DA INFRAESTRUTURA TERRESTRE ESTRATÉGICA

De acordo com Ministério da Defesa (2012) o impacto da Segurança e Defesa na Infraestrutura Terrestre como elemento do Poder Espacial e a inserção internacional do Brasil no respectivo mercado pode ser compreendido através de 4 pontos principais sendo: integração da infraestrutura terrestre com a defesa, importância do poder aeroespacial, inserção internacional do Brasil no mercado de defesa e segurança, e desenvolvimento tecnológico.

A Segurança e a Defesa no contexto da infraestrutura terrestre são aspectos fundamentais para garantir a soberania nacional, a proteção de ativos estratégicos e o funcionamento eficaz das operações militares e civis. A infraestrutura terrestre que suporta as operações aeroespaciais, como centros de lançamento, bases de monitoramento e controle, redes de comunicação e sistemas logísticos, constitui-se como um conjunto de ativos de alto valor estratégico. Sua proteção é essencial para evitar sabotagens, espionagem, ataques cibernéticos ou qualquer forma de interferência que possa comprometer a mobilidade, a capacidade operacional das forças e a integridade das missões espaciais.

Nesse sentido, a proteção legal dessas áreas adjacentes é crucial. Modesto e Neves (2025), ao analisarem a segurança de quartelamentos do Exército, resgatam o conceito de servidão militar, que impõe restrições em áreas vizinhas para preservar o interesse público e a segurança das operações, e afirmam a legitimidade do poder de polícia das Forças Armadas para fiscalizar e atuar nessas zonas. Essa visão é diretamente aplicável ao CLA, onde a proteção deve se estender para além de seus muros para mitigar ameaças e garantir a integridade das atividades de lançamento.

A integração da infraestrutura terrestre com a defesa é um pilar fundamental para a projeção de poder e a capacidade de resposta das Forças Armadas. Uma infraestrutura robusta, que suporte operações militares, logística e mobilidade, é essencial para a segurança e defesa nacionais. Isso inclui a manutenção de estradas, ferrovias, portos e aeroportos, que são cruciais para o deslocamento eficaz de tropas e equipamentos.

A segurança terrestre é um componente essencial da defesa nacional, focando na proteção do território e das infraestruturas críticas de um país. Ela envolve a proteção do espaço aéreo, das fronteiras e das águas jurisdicionais, garantindo que atividades ilícitas, como tráfico de drogas e contrabando, sejam prevenidas. Para isso, é fundamental que haja uma integração eficaz entre as Forças Armadas, onde as Forças Terrestres, Aéreas e Navais operem em conjunto, permitindo uma resposta coordenada a diversas ameaças.

E nesse contexto, a capacitação e o treinamento das tropas são fundamentais para a eficácia da segurança terrestre. As forças devem estar preparadas para enfrentar uma variedade de cenários, que vão desde operações de combate até missões de paz e ajuda humanitária. Além disso, o uso de tecnologias avançadas, como sistemas de monitoramento e vigilância, é vital para detectar ameaças em tempo real e garantir uma visão abrangente do território (Brasil, 2012).

A resiliência e a capacidade de resposta a crises também são aspectos importantes da segurança terrestre. Planos de contingência devem ser elaborados para lidar com desastres naturais ou ataques, e a mobilização rápida, juntamente com a coordenação entre diferentes agências, é fundamental para proteger a população e as infraestruturas.

Construir relações positivas com a população é vital para o sucesso das operações de segurança e para a prevenção de conflitos, garantindo que a segurança não seja apenas uma questão militar, mas também uma preocupação social e comunitária. Assim, a segurança terrestre se revela como um campo complexo que requer uma abordagem abrangente, integrando defesa militar, segurança pública e proteção das infraestruturas críticas.

Quanto ao poder espacial, este se destaca como um componente vital para a segurança nacional, uma vez que o desenvolvimento de capacidades espaciais, como satélites e sistemas de monitoramento, permite um controle mais eficiente do espaço aéreo e terrestre. Essa infraestrutura deve ser capaz de suportar operações de vigilância e resposta rápida a potenciais ameaças, sendo o controle do espaço aéreo e a articulação com países vizinhos considerados objetivos prioritários.

Contudo, Lima (2024) menciona vulnerabilidades no contexto do poder aeroespacial e da defesa nacional. Especificamente, para o autor há a necessidade de aprimorar o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA) para enfrentar situações sensíveis e críticas. Isso inclui a defesa passiva por meio de ocultação, camuflagem e instalações subterrâneas para abrigar equipamentos sensíveis, o que visa aumentar a prontidão e a força de dissuasão do Brasil.

Ainda segundo Ministério da Defesa (2012) o terceiro ponto importante na questão de segurança e defesa na infraestrutura terrestre consiste na inserção internacional do Brasil no mercado de defesa e segurança a qual é influenciada por esses aspectos, pois a capacidade de projetar poder e participar de operações de paz ou humanitárias fortalece a credibilidade do país como um ator global, onde a cooperação com outras nações em projetos de defesa e tecnologia espacial pode abrir portas para parcerias estratégicas e fomentar o desenvolvimento de indústrias de defesa no Brasil.

Já o quarto ponto é o desenvolvimento tecnológico que é essencial para a busca de autonomia na defesa nacional, englobando a fabricação de veículos lançadores de satélites e satélites de dupla utilização. Essa autonomia é importante não só para garantir a segurança nacional, mas também para a inserção do Brasil no mercado internacional. O país defende uma ordem internacional que priorize a cooperação e a proscrição de armas, o que pode facilitar a colaboração em projetos de defesa e segurança. Esses elementos demonstram a interligação entre segurança, defesa, infraestrutura terrestre e poder espacial, impactando diretamente a posição do Brasil no cenário internacional (Ministério da Defesa, 2012).

Entretanto, para o Ministério da Defesa (2012) os avanços na tecnologia da informação e o uso de sistemas como satélites e sensoriamento eletrônico, embora tenham trazido maior eficiência, também criaram novas vulnerabilidades. Essas vulnerabilidades podem ser exploradas por agentes maliciosos com o objetivo de comprometer o uso dos sistemas de segurança ou facilitar interferências à distância.

Para mitigar essas vulnerabilidades, é essencial que o Estado invista em setores de tecnologia avançada, garantindo que as infraestruturas críticas estejam protegidas contra possíveis ataques cibernéticos e outras ameaças. A segurança das infraestruturas deve ser uma prioridade, considerando não apenas a proteção física, mas também a integridade dos sistemas tecnológicos que suportam essas infraestruturas.

E igualmente há a necessidade de uma estrutura ágil e bem equipada para prevenir ações terroristas e conduzir operações de contraterrorismo é enfatizada, assim como a importância de aperfeiçoar dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas de tecnologia da informação e comunicação. Portanto, a abordagem para a segurança das infraestruturas terrestres deve ser abrangente, envolvendo tanto a proteção física quanto a segurança cibernética, para garantir a resiliência e a continuidade dos serviços essenciais.

3.2 ANÁLISE DO ARCABOUÇO NORMATIVO DA SEGURANÇA E DEFESA NO COMAER

O alinhamento estratégico da SEGDEF do CLA com os objetivos da FAB é sustentado por um robusto arcabouço normativo. A Segurança e Defesa (SEGDEF) no Comando da Aeronáutica é orientada pela Diretriz do Comando da Aeronáutica (DCA) 205-4 e operacionalizada através do Sistema de Segurança e Defesa do Comando da Aeronáutica (SISDE), detalhado na Norma de Sistema do Comando da Aeronáutica (NSCA) 205-3. A aplicação eficaz destes documentos no Centro de Lançamento de Alcântara (CLA) exige, contudo, uma análise aprofundada de suas particularidades e dos desafios impostos por sua natureza estratégica e compromissos internacionais. Partindo-se para uma breve análise das legislações pertinentes no âmbito do Comando da Aeronáutica (COMAER), visando sistematizar, delegar e cumprir com suas atribuições está constantemente atualizando suas diretrizes e normas para garantir o cumprimento de suas competências, conforme preconiza o Art. 3º do Anexo I do Decreto nº 6.834, de 30 de abril de 2009, em especial as que seguem:

Ao Comando da Aeronáutica compete:

IV - executar ações relativas à defesa do País, no campo aeroespacial;

V - contribuir para a formulação e condução de políticas nacionais que digam respeito à aviação, ao controle do espaço aéreo, às atividades espaciais, à infra-estrutura aeronáutica e à espacial e às atividades afins com a destinação constitucional da Aeronáutica, especialmente as relativas a recursos e ao desenvolvimento científico, tecnológico e industrial de interesse aeronáutico e espacial;

XI - incentivar e realizar atividades de pesquisa e desenvolvimento relacionadas com as atividades aeroespaciais. (Brasil, 2009).

Através dessas atribuições, fica evidente que o Comando da Aeronáutica desempenha um papel fundamental na defesa do Brasil e na promoção das atividades aeroespaciais. A inter-relação entre as ações de defesa, a formulação de políticas nacionais e o incentivo à pesquisa e ao desenvolvimento é vital para garantir que o Brasil continue a avançar no cenário aéreo e espacial, assegurando tanto a segurança quanto o progresso tecnológico e científico do país.

O alinhamento estratégico da SEGDEF do CLA com os objetivos da FAB é sustentado por um robusto arcabouço normativo sendo orientada, no Comando da Aeronáutica, pela Diretriz do Comando da Aeronáutica (DCA) 205-4 e operacionalizada através do Sistema de Segurança e Defesa do Comando da Aeronáutica (SISDE), detalhado na Norma de Sistema do Comando da Aeronáutica (NSCA) 205-3. A aplicação eficaz destes documentos no Centro de Lançamento de Alcântara (CLA) exige, contudo, uma análise aprofundada de suas particularidades e dos desafios impostos por sua natureza estratégica e compromissos internacionais.

A Concepção Estratégica Força Aérea 100 (DCA 11-45) estabelece as diretrizes de mais alto nível que “nortearão os rumos da Força Aérea Brasileira (FAB) na busca pela sua capacidade de perceber, avaliar, adaptar-se e preparar-se para o futuro”.

Para a SEGDEF do CLA, este documento é fundamental pois define a Missão da Aeronáutica – “manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da pátria” – e a Visão de Futuro – “uma força aérea de grande capacidade dissuasória, operacionalmente moderna e atuando de forma integrada para a defesa dos interesses nacionais”.

A segurança eficaz do CLA é um pré-requisito para que a FAB possa alcançar esses desígnios, protegendo os meios e a infraestrutura necessários para o controle do espaço aéreo, para a integração territorial por meio de recursos espaciais, e para a demonstração de uma capacidade dissuasória moderna.

Os Eixos Estratégicos da DCA 11-45, como Infraestrutura Aeroespacial, Tecnologia Aeroespacial e Meios de Força Aérea, também orientam implicitamente a necessidade de uma SEGDEF robusta no CLA para proteger os investimentos e capacidades neles contidos. A DCA 11-45, ao almejar uma FAB que “contribua para o fortalecimento do Poder Aeroespacial Brasileiro”, posiciona a segurança de um ativo como o CLA no cerne dessa contribuição.

Essa imperatividade da SEGDEF para o Poder Aeroespacial Brasileiro, e particularmente para o Centro de Lançamento de Alcântara (CLA), é corroborada pelo seu alinhamento direto com os Eixos Estratégicos da Força Aérea Brasileira (FAB) e com os Programas e Processos delineados em seus documentos de mais alto nível.

O eixo de Infraestrutura Aeroespacial visa garantir a disponibilidade e modernidade das instalações que suportam o Poder Aeroespacial. O CLA é, por definição, uma Infraestrutura Aeroespacial de valor ímpar para o país, dessa forma uma SEGDEF robusta e estratégica é, portanto, a condição para a resiliência, disponibilidade e confiabilidade desta infraestrutura, assegurando sua capacidade de suportar as ambições espaciais do país, incluindo o suporte vital às operações espaciais, especialmente com relação ao controle da operação do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) e demais sistemas espaciais de interesse da Defesa Nacional (Brasil, 2018).

Com relação ao eixo de Tecnologia Aeroespacial, a DCA 11-45 preconiza “Suprir as atividades operacionais da Força Aérea do futuro com as tecnologias requeridas” e “obter transferências de tecnologias nas suas principais aquisições, a fim de incentivar a construção do amanhã”. Ora, o CLA é um polo de desenvolvimento, aplicação e recepção de tecnologias aeroespaciais avançadas, logo sua SEGDEF tem o papel crucial de proteger os investimentos

em P&D, os ativos tecnológicos nacionais e de parceiros internacionais, e o conhecimento sensível. Uma segurança eficaz no CLA mitiga riscos de espionagem e sabotagem, que poderiam comprometer o avanço tecnológico da FAB e do Brasil e a capacidade de “diminuir a dependência externa” (Brasil, 2018).

Por fim, os Meios de Força Aérea, foca no “ajuste dos Meios de Força Aérea [...] aos novos tempos, com a utilização de tecnologias modernas, aliadas a novos conceitos de operação”, visando a prontidão operacional necessária. O CLA, como instalação, é um habilitador essencial para o preparo e lançamento de meios espaciais, logo sua SEGDEF deve assegurar a disponibilidade da plataforma de lançamento e das infraestruturas de apoio, vitais para que os meios espaciais sejam desenvolvidos, preparados e lançados com segurança, contribuindo para a “prontidão operacional necessária para enfrentar os desafios que o domínio dos céus exigirá nas próximas décadas” (Brasil, 2018).

O Plano Estratégico Militar da Aeronáutica (PEMAER) 2024-2033 (PCA 11-47/2024) operacionaliza essa visão estratégica, e a SEGDEF do CLA demonstra sua importância ao se conectar diretamente aos seus principais Programas e Macroprocessos. Os Programas Estratégicos definidos no PCA 11-47/2024 são essenciais para a evolução das capacidades da FAB, e a SEGDEF do CLA é um fator de sucesso para vários deles.

O Programa Poder Aeroespacial tem como objetivo “fortalecer a afirmação da soberania no espaço aéreo do Brasil [...] por meio do desenvolvimento autônomo de tecnologias, da contínua atualização e prontidão dos recursos aeroespaciais”. Logo, a SEGDEF do CLA é pilar deste programa ao proteger a infraestrutura que permite o desenvolvimento autônomo de acesso ao espaço e ao assegurar a prontidão dos recursos aeroespaciais através da garantia da capacidade e segurança das operações de lançamento (Brasil, 2024).

O Programa C2 Aeroespacial visa “incrementar o exercício da soberania no espaço aéreo brasileiro por meio da autonomia tecnológica nacional, da atualização e disponibilidade de meios de detecção e enlace de dados”. Dessa forma, a SEGDEF do CLA é vital para este programa, pois assegura a integridade dos lançamentos de satélites de comunicação e observação, componentes cruciais dos futuros sistemas de C2 Aeroespacial (Brasil, 2024).

Por fim, o Programa Estratégico de Sistemas Espaciais (PESE) estabelece a estratégia de implantação de longo prazo dos projetos de sistemas espaciais de defesa com uso compartilhado (militar e civil). O Projeto CEBRA (Complexo Espacial Brasileiro), que consiste na consolidação da capacidade brasileira de acesso ao espaço, tem no CLA seu principal componente. Assim, a SEGDEF do CLA é fundamental para a execução do PESE, protegendo

os investimentos e as capacidades estratégicas, como os veículos lançadores e as constelações de satélites Carponis e Lessonia (Brasil, 2024).

A SEGDEF do CLA também oferece suporte crucial aos macroprocessos da Cadeia de Valor do COMAER, identificados no PCA 11-47, com relação aos Macroprocessos Finalísticos, o Emprego (P240100) é a principal entrega de valor do COMAER à sociedade brasileira, resultando no emprego de meios aeroespaciais para “defender e controlar o espaço aéreo, e integrar o território nacional”, sendo diretamente habilitado por um CLA seguro (Brasil, 2024). Já o macroprocesso de Preparo, que “abrange a preparação do efetivo operacional [...] para que os meios aeroespaciais e de Força Aérea estejam em condições de serem empregados”, se beneficia da SEGDEF do CLA ao garantir a segurança para testes, qualificação de sistemas e desenvolvimento de doutrina espacial (Brasil, 2024).

Com relação aos Macroprocessos de Suporte, a Defesa Terrestre (P241200), que “abrange as atividades relacionadas à proteção dos meios aeroespaciais e de Força Aérea do COMAER dentro da tarefa de Proteção da Força”, tem na SEGDEF do CLA uma de suas materializações mais complexas e estratégicas, alinhando-se à diretriz de “Aprimorar o modelo de segurança das instalações do COMAER, com ênfase nas infraestruturas críticas” (Brasil, 2024). Já o Espaço (P241500), engloba “as atividades de responsabilidade do COMAER relacionadas à exploração do espaço”, dependendo diretamente da SEGDEF do CLA para garantir a segurança das operações de lançamento e o desenvolvimento de “processos e sistemas de gestão relacionados à atividade espacial” (Brasil, 2024).

3.2.1 Diretrizes para a Segurança e Defesa no COMAER (DCA 205-4) e o Sistema de Segurança e Defesa (NSCA 205-3) Aplicados ao CLA

A Diretriz do Comando da Aeronáutica (DCA) 205-4/2020 versa sobre a Segurança e Defesa no Comando da Aeronáutica, servindo como base de orientação para os órgãos subordinados ao COMAER possa executar, com eficiência, a Segurança das Instalações, equipamentos e pessoal sob sua responsabilidade. A “segurança” e “defesa” são basilares para medidas essenciais para a proteção das instalações de interesse do COMAER (Brasil, 2020, p. 7).

À luz desses conceitos, entende-se, num sentido mais amplo, que segurança é uma necessidade, uma aspiração e um direito inalienável do ser humano, enquanto defesa é um ato ou conjunto de atos realizados para obter ou resguardar as condições reconhecidas como segurança. Assim, Segurança e Defesa englobam o conjunto de Ações de Força Aérea que

contribuem para a preservação do poder de combate da FAB. Consiste na consecução de ações defensivas, ofensivas e de proteção, a fim de garantir o grau de segurança desejado (Brasil, 2020, p. 7).

Cabe ressaltar que as atividades de Segurança e Defesa no âmbito do CLA, são de responsabilidade do Grupo de Segurança e Defesa de Alcântara (GSD-AK), conforme preconiza a DCA 205-4/2020, parafraseando, “uma Unidade de Segurança e Defesa (USEGDEF) do COMAER, Contingente de Infantaria da Aeronáutica cuja atuação abarca as Ações de Segurança das Instalações, Polícia da Aeronáutica e Autodefesa de Superfície.” (Brasil, 2020).

Analisando-se a DCA 125-5/2020, verificamos que uma das possibilidades de Atuação e Ações de Força Aérea características da Infantaria da Aeronáutica são a Garantia da Soberania, Integridade Territorial e Defesa Patrimonial materializada através da Segurança das Instalações. Além disto, estabelece as Ações de Força Aérea e Áreas de Atuação da Infantaria da Aeronáutica, onde a Segurança das Instalações se enquadra na área de atuação da Infantaria da Aeronáutica (INFAER) Segurança e Defesa.

Ainda tomando-se por base a DCA 125-5/2020, O Sistema de Segurança e Defesa do COMAER (SISDE) gerencia as atividades de SEGDEF, em tempo de paz ou de guerra. O Órgão Central do SISDE é o Comando de Preparo (COMPREP).

A DCA 125-5/2020, em paralelo com a DCA 1-1/2024 – Doutrina Básica da Força Aérea Brasileira, estabelece que a Ação de Segurança das Instalações (Seg Inst) “é a Ação que consiste em empregar Meios de Força Aérea para assegurar a integridade do patrimônio e das instalações de interesse da Força Aérea.” (Brasil, 2024, p. 49).

Assim, conforme a conceituação e composição de Segurança das Instalações no âmbito do COMAER, a DCA 125-5/2020, assevera:

A Seg Inst é composta por medidas ativas e passivas de segurança física, que têm o objetivo de garantir a integridade de instalações aeronáuticas, no que compreende a salvaguarda do pessoal, das instalações, dos equipamentos, da funcionalidade e do conhecimento da Força Aérea. (Brasil, 2019, p. 19).

Ainda a DCA 125-5/2020 esclarece que:

Para proteger o patrimônio, é requerida uma infraestrutura adequada e pessoal especializado. A infraestrutura requer barreiras e arruamentos perimetrais, iluminação de proteção, postos de controle de acesso, guaritas reforçadas, vigilância eletrônica, viaturas operacionais, aeronaves remotamente pilotadas e uma rede rádio dedicada. O pessoal especializado deve ser reduzido ao máximo, sendo empregado apenas no monitoramento da vigilância eletrônica e do controle de acesso, em sentinelas de meios de altíssima criticidade (Ex: paióis com munição ou armamento de interesse das OCRM, aeronaves presidenciais, de Controle Aéreo Antecipado, de defesa aérea

em alerta e Reabastecedoras) e em Equipes de Reação, com alta mobilidade, poder de fogo, capacidade de aquisição de alvos, capacidade de Comando e Controle (C2) e adequada proteção balística. (Brasil, 2019, p.19).

No contexto abordado, a segurança é considerada uma necessidade essencial e um direito humano, enquanto a defesa constitui um conjunto de ações destinadas a preservar essa segurança. O Grupo de Segurança e Defesa de Alcântara (GSD-AK) é responsável por proteger as instalações e realizar atividades policiais relacionadas à Aeronáutica. A DCA 125-5/2020 destaca que a segurança das instalações é uma missão fundamental da Infantaria da Aeronáutica, visando a soberania e integridade territorial.

O Sistema de Segurança e Defesa do COMAER (SISDE) coordena as ações de segurança em tempos de paz e conflito, com o Comando de Preparo (COMPREP) como eixo central. A DCA 1-1/2024 reforça a importância da segurança das instalações como atividade para garantir a proteção do patrimônio e instalações da Força Aérea.

As diretrizes enfatizam a necessidade de medidas de segurança ativas e passivas, com estruturas como barreiras de proteção e sistemas de vigilância eletrônica, além de pessoal qualificado para monitoramento eficaz e respostas rápidas. Assim, a DCA 205-4/2020 e diretrizes associadas formam uma base sólida para estratégias de proteção das operações e bens da Aeronáutica, ressaltando a importância da coordenação entre diferentes unidades na segurança e defesa da Força Aérea Brasileira.

Em resumo, a DCA 205-4/2020, que “tem por finalidade orientar a Segurança e Defesa nas Organizações Militares do COMAER”, e a NSCA 205-3/2024, que estabelece o “Sistema de Segurança e Defesa do Comando da Aeronáutica (SISDE)”, formam o núcleo do arcabouço normativo específico da SEGDEF.

A DCA 205-4 define SEGDEF como o “Conjunto de medidas que contribuem para a preservação do poder combatente da Força Aérea Brasileira... a fim de garantir o grau de segurança desejado das instalações, dos equipamentos e do pessoal”. Seus princípios de guerra aplicados à SEGDEF, como economia de meios e massa, objetivo, ofensiva e prontidão, devem nortear o planejamento da segurança no CLA. A premissa de que a priorização da proteção deve se basear na importância relativa e vulnerabilidade relativa coloca o CLA em um patamar de máxima atenção, dada sua singularidade estratégica e os riscos associados, especialmente no contexto do AST.

A NSCA 205-3/2024, ao detalhar o SISDE, estabelece o COMPREP como Órgão Central e as Unidades de Segurança e Defesa (USEGDEF), como o GSD-AK no CLA, como órgãos operacionais. A norma enfatiza a necessidade de gerenciamento de riscos e a elaboração

de Planos de Segurança das Instalações (PSI) e Planos de Segurança Orgânica e Defesa (PSOD). No CLA, a aplicação destes planos deve ser particularmente rigorosa, considerando a necessidade de proteger não apenas os ativos da FAB, mas também tecnologia de parceiros internacionais sob o AST.

A natureza dual do CLA (militar-estratégica e comercial-internacional) impõe desafios à aplicação da DCA 205-4 e da NSCA 205-3, onde a definição de SEGDEF focada na preservação do poder combatente da FAB precisa ser ampliada no contexto do CLA para incluir a proteção de tecnologia e interesses de parceiros, bem como a viabilização de operações comerciais. Isso requer uma harmonização de protocolos de segurança da FAB com requisitos internacionais, a proteção de ativos de terceiros e uma gestão cuidadosa do acesso e da transparência versus o sigilo militar. A capacidade do SISDE e do GSD-AK de responder a essa complexidade é um fator crítico para a SEGDEF eficaz do CLA.

3.2.2 O Suporte Integrado de Segurança das Instalações (DCA 205-9) como Modelo de Modernização para a SEGDEF do CLA

A Diretriz do Comando da Aeronáutica DCA 205-9, que institui a “Implantação do Suporte Integrado de Segurança das Instalações nas Organizações Militares do COMAER” (SISI), representa a mais recente evolução normativa da FAB para a segurança de instalações e oferece um modelo fundamental para a modernização e otimização da SEGDEF no CLA.

O SISI é definido como “a integração da infraestrutura de Segurança das Instalações com os meios de Segurança Eletrônica [...] todos interligados, por meio de um sistema eficiente de comando e controle e de inteligência, a equipes de pronta resposta (Equipes de Reação)”. Esta abordagem integrada é crucial para o CLA, dada sua complexidade e os requisitos do AST.

A DCA 205-9 está alinhada com o PCA 11-47/2024, que já orienta a revisão do modelo de segurança com foco em novas tecnologias de vigilância eletrônica, controle de acesso e detecção de intrusão; a adoção de forças de reação rápida. A implementação do SISI no CLA, através de um “Projeto SISI” específico e de uma comissão de implantação multidisciplinar, permitirá a materialização dessas orientações estratégicas, adaptando-as à vasta área, à diversidade de instalações sensíveis e à necessidade de integração com múltiplos atores no Centro. A padronização de sistemas, como o Software de Controle de Acesso e Informações (SCAI), e a previsão de recursos, são aspectos normativos do SISI que nortearão a modernização da SEGDEF em Alcântara.

Contudo, ao se analisar o arcabouço normativo que rege a capacitação inicial do pessoal que atuará no Centro, como a TCA 37-15 (Cursos do DCTA para o ano de 2025), observa-se que o Curso de Preparação para Operações de Lançamento (CPOL) ainda se concentra em aspectos eminentemente técnicos e operacionais. Esta constatação evidencia uma lacuna entre a evolução da doutrina de SEGDEF, que caminha para um modelo integrado e estratégico, e a formação prática, que ainda não incorpora plenamente a segurança como um pilar fundamental da capacitação, lacuna essa que será abordada em detalhe no capítulo 5.

4 FUNDAMENTOS DA SEGURANÇA CORPORATIVA ESTRATÉGICA (SCorpE)

A segurança, em um contexto organizacional moderno, transcende a mera proteção física e reativa, elevando-se a um patamar estratégico que se interliga diretamente aos objetivos, à sustentabilidade e à competitividade das instituições. Por natureza, é um “estado, qualidade, condição daquilo que está seguro, isento de perigo, acautelado” (Mandarini, 2005, p. 13).

No âmbito do Estado, essa atividade ganha contornos específicos, moldados pela missão constitucional de cada órgão. Na Força Aérea Brasileira (FAB), como já visto, a Segurança e Defesa (SEGDEF) é definida como o conjunto de medidas para a preservação do poder combatente, garantindo a proteção de instalações, equipamentos e pessoal de interesse do Comando da Aeronáutica (COMAER).

De forma análoga, no âmbito do Poder Judiciário, o Plano de Segurança Orgânica (PSO) do Conselho da Justiça Federal tem por finalidade, *in verbis*:

Normatizar as atividades, rotinas e práticas para fortalecer as atividades de segurança, com foco em salvaguardar e proteger o patrimônio tangível e intangível do Conselho da Justiça Federal, bem como magistrados, servidores, colaboradores, prestadores de serviço e visitantes. (Conselho da Justiça Federal, 2021, p. 3).

Para uma análise aprofundada da segurança no âmbito da FAB e, especificamente, do CLA, é fundamental estabelecer uma base conceitual sólida, diferenciando e interligando os termos que compõem o universo da segurança. Mandarini (2005) apresenta uma clara distinção entre as modalidades de segurança, o que é crucial para entender a amplitude do tema no contexto militar e aeroespacial.

Em sua dimensão mais ampla, o anseio por segurança é uma aspiração universal da sociedade, um pilar para a manutenção da vida social digna e para o exercício de direitos fundamentais como a vida e a liberdade. No Brasil, a Segurança Pública é tradicionalmente compreendida como a “condição de segurança provida pelo Estado, às suas expensas, mediante utilização de instituições específicas e integrantes de sua própria estrutura organizacional” (Mandarini, 2005, p. 13).

Contudo, ressalta que limitações diversas, sejam elas orçamentárias, políticas ou legais, frequentemente impedem o Estado de prover essa segurança de forma plena. Diante dessa lacuna, surge a Segurança Não-pública, ou seja, aquela condição de segurança que não é provida pelo Estado, porém providenciada e custeada pelo próprio interessado (pessoa física ou jurídica) e prestada por funcionário (ou empregado), particulares ou pela iniciativa privada.

Essa modalidade se desenvolveu no Brasil, especialmente a partir do final da década de 1960 e início da década de 1970, em resposta à incapacidade do Estado de garantir a segurança de setores como os bancos, frente a um aumento da criminalidade.

Cumprido destacar que essa consolidação se deu pela Lei nº 7.102/83, que dispõe sobre a segurança de estabelecimentos financeiros e estabelece normas para a constituição e funcionamento de empresas de segurança privada que exploram serviços de vigilância e transporte de valores, estabelecendo os fundamentos e exigências para a atividade de segurança privada no país.

Dentro do guarda-chuva da Segurança Não-Pública, Mandarinini (2005, p. 14) distingue dois ramos principais com base no tipo de “interessado” ou “tomador” da segurança, onde a Segurança Privada (ou pessoal) refere-se à condição de segurança não provida pelo Estado, providenciada e custeada pelo próprio interessado, pessoa física. Este ramo lida com as ações de segurança tomadas no ambiente individual das pessoas, como a proteção de executivos, familiares, comitivas ou dignitários (Segurança VIP). A eficácia da segurança pessoal depende intrinsecamente da cooperação e conscientização do indivíduo protegido, exigindo que este aceite a interferência em suas rotinas diárias e compreenda os riscos envolvidos.

No âmbito da Segurança Não-pública, a Segurança Corporativa (ou empresarial) emerge como a condição de segurança não provida pelo Estado, providenciada e custeada pelo próprio interessado, pessoa jurídica (Mandarinini, 2005, p. 14). Este conceito é o foco central deste estudo, pois aplica-se diretamente à proteção de organizações estratégicas como a FAB e o CLA, cujas missões transcendem o interesse privado e se alinham à defesa nacional.

A segurança corporativa, nesse contexto, ultrapassa a mera proteção patrimonial, abrangendo um espectro mais amplo de ativos e processos. A intersecção entre as definições é crucial, pois a atividade de segurança atua na minimização de riscos e ameaças, buscando administrar e maximizar a relação custo-benefício de sua implementação (Mandarinini, 2005, p. 14).

A atividade de segurança é, portanto, conceituada como uma “modalidade de prestação de serviço, executada pelos próprios Recursos Humanos (funcionários), por particulares (terceiros) ou por empresas privadas e especializadas” (Mandarinini, 2005, p. 14). Seu objetivo primordial é minimizar riscos e ameaças, buscando um estado de equilíbrio entre as ações de proteção e a rotina das instituições e para isso, envolve o planejamento da prevenção e da reação contra eventos adversos, além de coordenar e estabelecer a integração do sistema homem versus técnicas versus tecnologia (Mandarinini, 2005, p. 14).

Essa integração é um pilar na doutrina moderna de segurança, como se observa na Diretriz do Comando da Aeronáutica (DCA) 205-9, que institui o Suporte Integrado de Segurança das Instalações (SISI) a partir da conjugação de infraestrutura, segurança eletrônica e equipes de reação especializadas (Brasil, 2025, p. 4).

É fundamental ressaltar que a Atividade de Segurança, em especial a corporativa, não substitui nem concorre com a Segurança Pública, mas a complementa, atuando onde o Estado não pode ou não é conveniente operar. Conforme Mandarini (2005, p. 14), a atividade de segurança não possui Poder de Polícia, que é uma prerrogativa inerente ao Estado.

Contudo, ao analisar a segurança de instalações estatais, como as militares, a natureza desse poder se torna mais complexa. As Forças Armadas, por serem órgãos da administração pública direta, são detentoras tanto do poder de polícia administrativa quanto do poder de polícia judiciária (Modesto; Neves, 2025, p. 187). O poder de polícia administrativa manifesta-se na capacidade de impor medidas para preservar a ordem interna e a disciplina, enquanto o poder de polícia judiciária se refere à competência para investigar e processar crimes militares, conforme o Código Penal Militar (Modesto; Neves, 2025, p. 187).

Essa prerrogativa justifica a atuação do Exército na proteção das áreas adjacentes aos seus aquartelamentos, não apenas como uma faculdade legal, mas como uma necessidade estratégica para a segurança orgânica e a defesa do Estado (Assis, 2020, p. 209). Portanto, enquanto a segurança corporativa privada atua de forma complementar e sem poder de polícia, a segurança de uma organização militar como o CLA é exercida com base em prerrogativas estatais que lhe conferem a autoridade para regular e controlar suas áreas de interesse em prol da segurança nacional.

4.1 A EVOLUÇÃO DA SEGURANÇA: DA ERA INDUSTRIAL À ERA DO CONHECIMENTO

A concepção de segurança evoluiu drasticamente com a transição da Era Industrial para a Era do Conhecimento. Na Era Industrial, a segurança era reativa e focada na proteção do patrimônio contra ameaças externas, com a Era do Conhecimento, caracterizada pela velocidade na transmissão de informações e pela crescente dependência tecnológica, a segurança tornou-se uma “atividade corporativa, [...] exercida como gestão de riscos e prevenção de perdas, contra ameaças externas e internas” (Mandarini, 2005, p. 32).

Essa nova realidade, conforme destacado por Assumpção e Costa (2019, p. 128), transformou a sociedade de um estado “simples, controlável, previsível, lento, estável e

baseado em instituições sólidas para um ambiente complexo, fora de controle, imprevisível, rápido, instável e pautado sobre o indivíduo”. A análise e o gerenciamento dos riscos passaram a ser responsabilidade de todos na organização, exigindo uma visão sistêmica e a participação de todos os colaboradores.

A transição da Era Industrial para a Era do Conhecimento, que se acentuou a partir dos anos 1960, trouxe profundas mudanças no enfoque da segurança. Vejamos o quadro comparativo (tabela 6) que ilustra essas diferenças.

Tabela 6 – Quadro Comparativo Era Industrial x Era do Conhecimento

ERA INDUSTRIAL	ERA DO CONHECIMENTO
Mudanças lentas, produtos de vida longa, produção destrutiva, consumidor pouco informado e não-participativo	Inovação contínua, velocidade, criatividade, preocupação com o meio ambiente, consumidor participativo e informado
Empresas voltadas para o produto, buscando posição no mercado; toda a atenção voltada para a produção e a produtividade	Empresas voltadas para o cliente, buscando posicionar-se em sua mente; toda a atenção dirigida à relação que então se estabelece
A qualidade apenas como um item a mais, vista como a conformidade com as especificações do produto	Gestão pela qualidade total, vista agora, também, como a conformidade com as necessidades do cliente
Ênfase na tarefa; organização em estruturas rígidas e burocráticas	Ênfase no negócio e no conhecimento; estruturas organizacionais mais ágeis
Má divisão do trabalho; dificuldade de entendimento do conjunto pelos empregados e clientes	Trabalho em equipe; relações internas estabelecidas na forma de liderança e colaboração
Exercício do poder pela pressão da norma, do controle, da centralização	Exercício do poder diluído pela delegação, cessão de autonomia (empowerment)
A segurança como um departamento, voltada para o produto e o patrimônio, exercida como atividade policial para proteção contra ameaças externas	A segurança como uma atividade corporativa, voltada para as pessoas e os ativos, exercida como gestão de riscos e prevenção de perdas, contra ameaças externas e internas
Atribuições mal delimitadas; atuação como força de reação, tendente a invadir a esfera da autoridade policial	Atribuições bem definidas; atuação como unidade de informações gerenciais que estabelece matrizes de demandas e de recursos
Estruturas hierarquizadas, subordinação, verticalidade e homogeneidade	Estruturas sistêmicas, equipes de trabalho, horizontalidade e heterogeneidade
Atuação isolada, soluções pontuais, setoriais, compartimentação; proteção contra os riscos e ameaças não-empresariais	Atuação integrada, soluções globais, compartilhamento; proteção contra riscos e ameaças empresariais ou não-empresariais

Fonte: Adaptado de Mandarini (2005, p. 32).

Na Era Industrial, a ênfase estava na produção, na produtividade e na qualidade como conformidade com especificações, a organização era rígida, burocrática, com má divisão do trabalho e exercício do poder pela pressão e centralização. Com relação à segurança, era vista como um departamento voltado para o produto e o patrimônio, atuando de forma reativa e policialesca contra ameaças externas.

Com a Era do Conhecimento, o cenário mudou drasticamente. A necessidade de conhecimentos para a sobrevivência do homem, antes ligada a guerras e conflitos de interesse, transformou-se no marco definitivo de uma nova era, impulsionada pelo advento da informática e da globalização. Nesse novo contexto, a segurança passou a ser uma atividade corporativa, com foco no negócio e no conhecimento, e estruturas organizacionais mais ágeis. A gestão da segurança concentra-se na gestão de riscos e prevenção de perdas, atuando contra ameaças externas e internas.

O novo perfil da atividade de segurança na Era do Conhecimento exige que a análise e o gerenciamento dos riscos empresariais (do próprio negócio) e não-empresariais (alheios ao negócio) sejam responsabilidade de todos na organização, e não apenas de segmentos específicos. Mandarini (2005, p. 8) enfatiza que essa nova concepção não admite a segurança como um componente isolado, mas exige “ativa participação na discussão do todo institucional, buscando aumentar sua visão sistêmica, melhorar sua capacidade de identificação de riscos e ameaças e adotar as melhores práticas preventivas para reduzir suas possíveis consequências”.

A segurança deve atuar em todas as frentes, da matriz de riscos e ameaças ao negócio, às angústias e insatisfações dos empregados, clientes e fornecedores. Essa realidade ratifica a necessidade de constante atualização e especialização dos profissionais de segurança. O mercado da segurança, no Brasil, tornou-se extremamente exigente quanto aos custos, à funcionalidade e à eficiência dos projetos de segurança, o que impulsiona o emprego cada vez maior de técnicas e tecnologias e, progressivamente, a substituição da mão-de-obra por sistemas integrados, mais eficientes e economicamente viáveis.

4.2 RAMOS DA SEGURANÇA CORPORATIVA

A atividade de segurança, seja no âmbito privado ou corporativo, direciona suas ações para proteger “sujeitos” e “objetos”. O sujeito, ou seja, o tomador da segurança, define o ramo de atuação. Assim, conforme Mandarini (2005, p. 21-22), existem dois ramos principais: o ramo da segurança das pessoas físicas (Segurança Privada) e o ramo da segurança das pessoas jurídicas (Segurança Corporativa).

Independentemente do ramo, as medidas e procedimentos de segurança visam proteger um objeto, que pode ser um ser humano ou um bem. Esses objetos são convencionalmente chamados de ativos, e sua diversidade define os dois segmentos da Atividade de Segurança: Segurança das Pessoas e Segurança dos Ativos.

Logo, a Segurança Orgânica (SO) constitui um pilar essencial dentro da Segurança Corporativa Estratégica. De forma ampla, a SO é o conjunto integrado de medidas de caráter eminentemente defensivo e preventivo, com o objetivo de proteger os ativos institucionais e garantir o funcionamento seguro das atividades (Assumpção; Costa, 2019).

Essa concepção é amplamente adotada e detalhada no setor público. A doutrina de Segurança Institucional do Ministério Público, por exemplo, define a Segurança Orgânica por meio de seus quatro pilares: segurança de recursos humanos, segurança da documentação e do material, segurança de áreas e instalações e segurança da informação (Dalabrida, 2019, p. 10). Essa estrutura visa ao controle das vulnerabilidades para evitar danos decorrentes de ameaças ou ações hostis.

Em um contexto de segurança pública, a SO é vista como um segmento da Contrainteligência que atua produzindo normas e procedimentos para garantir a integridade das operações, prevenindo qualquer risco ao Serviço de Inteligência em sua integralidade (Kinopp; Maba, 2023).

A eficácia da Segurança Orgânica depende de um planejamento detalhado, formalizado em um Plano de Segurança Orgânica (PSO). O Plano do Conselho da Justiça Federal (CJF), por exemplo, define o PSO como o documento de caráter procedimental utilizado para descrever as ações operacionais de segurança, tanto de natureza rotineira quanto excepcionais, de modo a contemplar as necessidades e especificidades locais (Conselho da Justiça Federal, 2021).

Para o CLA, a implementação robusta da SO e a elaboração de um PSO são vitais, dada a natureza estratégica de suas operações. Conforme preconizado em doutrinas de segurança e inteligência, como as apresentadas no material de Introdução à Segurança Estratégica (INE.EAD) e, por analogia, em normativas como a Resolução CNMP Nº 156/2016 (que institui a Política de Segurança Institucional no MP), a SO se desdobra em segmentos interdependentes, vejamos:

Tabela 7 – Segmentos da Segurança Orgânica (SO) no Contexto do CLA

Segmento da Segurança Orgânica	Descrição e Abrangência
Segurança de Pessoal	Engloba o conjunto de normas e procedimentos para a proteção das pessoas (recursos humanos) em todos os níveis, assegurando sua integridade física e moral e promovendo comportamentos alinhados à salvaguarda de informações sigilosas. Abrange todo o ciclo funcional, desde o recrutamento até o desligamento.
Segurança da Documentação e do Material	Visa à proteção de todos os documentos (físicos ou digitais) e materiais de valor estratégico. O objetivo é salvaguardá-los contra acesso não autorizado, perda, dano, espionagem ou sabotagem, considerando todo o seu ciclo de vida.

Segurança das Comunicações	Abrange as medidas e técnicas para proteger as informações durante sua transmissão e recepção (eletrônica, rádio, etc.), com foco em garantir a confidencialidade, integridade e autenticidade, prevenindo interceptações e interferências.
Segurança de Áreas e Instalações	Consiste no conjunto de medidas físicas, eletrônicas e procedimentais para proteger os locais onde se desenvolvem atividades críticas ou se manuseiam dados e materiais sigilosos. Envolve delimitação de perímetros, controle de acesso, detecção de intrusão, vigilância e planos de emergência.

Fonte: O Autor.

A eficácia da SO depende de um planejamento detalhado, usualmente formalizado em um Plano de Segurança Orgânica (PSO), que deve ser dinâmico e adaptado às particularidades e aos riscos específicos da organização. Para o CLA, a implementação robusta de cada um desses componentes da SO é vital, dada a natureza estratégica e sensível de suas operações.

4.2.1 Segurança das Pessoas na Organização Militar

A Segurança das Pessoas pode ser dividida em geral ou institucional, sendo que a segurança geral é voltada para a proteção de indivíduos ou grupos específicos, como executivos, familiares, comitivas, autoridades e artistas (Segurança VIP), já a segurança institucional, no contexto corporativo, foca nas atividades relacionadas à seleção, acompanhamento do exercício funcional e comportamento dos Recursos Humanos (Mandarini, 2005).

Mandarini (2005, p. 22-24, 28) enfatiza que a segurança pessoal não se concretiza contra a vontade ou sem a cooperação do indivíduo protegido, que precisa estar ciente dos riscos e aceitar as intervenções em suas rotinas. Além disso, a segurança pessoal deve ser prudente, sensata e focada em “evitar problemas”, prevenindo acidentes e atuando em situações de crise ou emergência, com a integridade física e o bem-estar do protegido como preocupações fundamentais.

No ambiente corporativo e militar, a Segurança da Gestão das Pessoas (SGP) é o foco da segurança das pessoas, direcionada aos Recursos Humanos (RH) - empregados orgânicos, funcionários das instituições que mantêm vínculo empregatício - e aos Executivos, membros da alta administração responsáveis pela gestão das corporações.

A FAB, através de suas Diretrizes do Comando da Aeronáutica (DCA) e Normas de Sistema do Comando da Aeronáutica (NSCA), estabelece uma série de procedimentos para a gestão de pessoal que, embora não usem explicitamente o termo SGP, alinham-se aos seus princípios ao abordar a segurança na seleção, no desempenho funcional e nos afastamentos, visando mitigar riscos internos e externos.

O Sistema de Segurança e Defesa do Comando da Aeronáutica (SISDE), por exemplo, tem como objetivo principal padronizar normas e procedimentos que garantam a segurança do pessoal, o que demonstra a aplicação prática dos conceitos de SGP.

4.2.2 Segurança dos Ativos: Além do Patrimônio Físico

O conceito de ativos na segurança corporativa estratégica vai além do sentido restritivo de patrimônio (bens móveis e imóveis). Ativo é “todo e qualquer item que possa ser economicamente considerado, ao qual possa ser associada uma idéia de valor, ainda que minimamente expressivo”. Mandarini (2005, p. 29) classifica os ativos em:

- a) **Bens tangíveis:** como o patrimônio produtivo (instalações, máquinas, equipamentos, produtos acabados, documentos e materiais diversos; sistemas de informática – softwares e hardware; bens móveis e imóveis) e o patrimônio financeiro (recursos, financiamentos, ações, aplicações).
- b) **Bens intangíveis:** como o patrimônio social e institucional (RH, meio ambiente, imagem, segredos das empresas; planejamentos, estratégias, dados e conhecimentos – informações) e o patrimônio comercial (know-how, processos, logística, mercado, marcas, fornecedores e clientes; imagem, credibilidade e confiança na empresa). Essa visão abrangente sobre o que constitui um “ativo” é compartilhada por outras doutrinas de segurança no âmbito estatal. A Política de Segurança Institucional do Ministério Público, por exemplo, considera como ativos a serem protegidos “o elemento humano (pessoas), as áreas e as instalações, os materiais, as informações e a imagem do Ministério Público” (Souza *et al.*, 2019, p. 6).

Para a FAB, especialmente no CLA, a segurança dos ativos intangíveis é de criticidade elevada, além das instalações físicas e equipamentos de lançamento, o conhecimento científico-tecnológico, os planejamentos de missões, os dados sensíveis e a própria imagem da instituição são ativos de valor inestimável. A proteção desses ativos, tangíveis e intangíveis, é um dos pilares da segurança corporativa estratégica, dada a sua expressão de valor e seu impacto direto na continuidade e sucesso do negócio.

As diretrizes da FAB, como a DCA 205-4/2020 (Brasil, 2020), ao abordar a proteção de instalações, equipamentos e pessoal, indiretamente reconhecem a amplitude desse conceito de ativos, embora a terminologia possa variar.

Indo além da classificação geral de Mandarinini, a aplicação prática da Segurança Orgânica em instituições públicas levou a um detalhamento maior do que constitui um ativo a ser protegido. No modelo desenvolvido para a segurança pública do Piauí, por exemplo, Menezes *et al.* (2022) propõem uma lista de nove ativos, que incluem não apenas “Pessoas”, “Instalações” e “Informações Sigilosas”, mas também categorias imateriais como “Clima Organizacional”, “Imagem Institucional” e “Equidade de Gênero”.

Essa abordagem expansiva é particularmente relevante para a FAB e para o CLA, onde, além dos ativos físicos e tecnológicos, o conhecimento, a imagem institucional e o próprio bem-estar do efetivo (clima organizacional) são de valor inestimável.

4.3 SEGURANÇA CORPORATIVA E OS SEGMENTOS DA ATIVIDADE DE SEGURANÇA

A Segurança Corporativa Estratégica (SCorPE) pode ser aplicada à gestão da Segurança e Defesa (SEGDEF) de Organizações Militares como o CLA por meio da análise de seus diferentes segmentos. Esses segmentos são desdobramentos funcionais das dimensões da segurança e permitem uma abordagem sistêmica, direcionada à prevenção de perdas. A seguir, analisam-se os principais segmentos da atividade de segurança sob a ótica da SCorPE e sua aplicação à SEGDEF do CLA.

Para uma compreensão abrangente da SCorPE, é essencial entender sua estrutura. Conforme Mandarinini (2005, p. 84), a amplitude dos ativos organizacionais exige uma nova visão, vejamos:

Tendo em vista que os ativos ultrapassam o universo restrito dos bens móveis e imóveis e abrangem todo o amplo espectro dos bens tangíveis e intangíveis, a Segurança Ativa se divide em segmentos de segurança corporativa, que reunimos em três grandes grupos de medidas e procedimentos: Segurança da Gestão das Áreas e Instalações (SGAI); Segurança da Gestão dos Processos (SGProc); Segurança da Gestão do Conhecimento (SGC). Mandarinini (2005, p. 84).

Figura 6 - Os quatro grandes segmentos da Segurança Corporativa.

Fonte: Adaptado de Mandarinini, (2005, p. 84).

A metodologia de segmentação da Segurança Corporativa, conforme detalhada por Mandarinini (2005, p. 85), abrange um espectro amplo de medidas e procedimentos direcionados a diferentes eixos de gestão, vejamos conforme a Tabela 8:

Tabela 8 – Segmentação da Segurança Corporativa.

Eixo de Gestão	Subdivisões
Segurança da Gestão das Áreas e Instalações	-
Segurança da Gestão das Pessoas	-
Segurança da Gestão dos Processos	Segurança das Operações
	Segurança dos Planejamentos
	Segurança dos Insumos
Segurança da Gestão do Conhecimento	Segurança da Informação
	Segurança dos Suportes
	Segurança das Telecomunicações
	Segurança da Tecnologia da Informação

Fonte: Adaptado de Mandarinini (2005, p.85-86)

4.3.1 Segurança da Gestão das Áreas e Instalações (SGAI)

Segurança da Gestão das Áreas e Instalações (SGAI) é o segmento da SCorpE responsável pela proteção dos bens tangíveis de uma organização, como seu patrimônio produtivo, que inclui instalações, máquinas e equipamentos. Seu objetivo é prevenir acessos

não autorizados, danos e interferências às áreas e instalações, baseando a proteção nos riscos identificados (Mandarini, 2005).

Essa visão é corroborada pela doutrina de segurança institucional no setor público. Caron e Bueno (2019, p. 76) definem a segurança de áreas e instalações como o conjunto de normas, medidas e procedimentos voltados à proteção extensiva das dependências da instituição, notadamente naquelas em que são elaborados, tratados, manuseados ou guardados as informações sigilosas e os materiais sensíveis. A premissa fundamental é que a proteção deve ser compatível com os riscos identificados.

A SGAI envolve um conjunto de medidas protetivas e de controle de acesso que diferenciam locais perigosos, visando a segurança das pessoas, de locais sensíveis, focados na proteção de ativos. A implementação dessas medidas baseia-se na avaliação da criticidade de cada Área Interna da Organização Militar (AIDA), considerando seus impactos nos processos, pessoas, meio ambiente e sociedade (Mandarini, 2005, p. 89).

De fato, a segurança de áreas e instalações visa a “prevenir acessos não autorizados, danos e interferências”, e a proteção “deve ser compatível com os riscos identificados” (Caron; Bueno, 2019, p. 76).

Dentre o conjunto de normas e medidas destinadas a garantir o funcionamento da instituição, as ações para áreas e instalações são as que exigem maior integração, pois grande parte da atividade institucional se concentra nesse ambiente (Caron; Bueno, 2019, p. 68).

Para uma gestão eficaz, as áreas são classificadas segundo sua natureza e sensibilidade. Caron e Bueno (2019) propõem uma classificação prática, vejamos:

Tabela 9 – Classificação das Áreas.

Classificação	Descrição
Áreas Livres	Destinadas ao atendimento ao público em geral, como a recepção de uma edificação.
Áreas Restritas	Ultrapassam o limite da área livre, exigindo medidas de controle para o acesso, como gabinetes e salas de reuniões.
Áreas Críticas	Guardam infraestruturas essenciais ao funcionamento da instituição, como servidores de dados, geradores de energia e salas de controle, sendo pontos de interesse para ações de sabotagem.
Áreas Sigilosas	Locais onde são tratados, manuseados ou guardados documentos, materiais ou informações sensíveis, cujo acesso é permitido apenas mediante credencial de segurança específica.

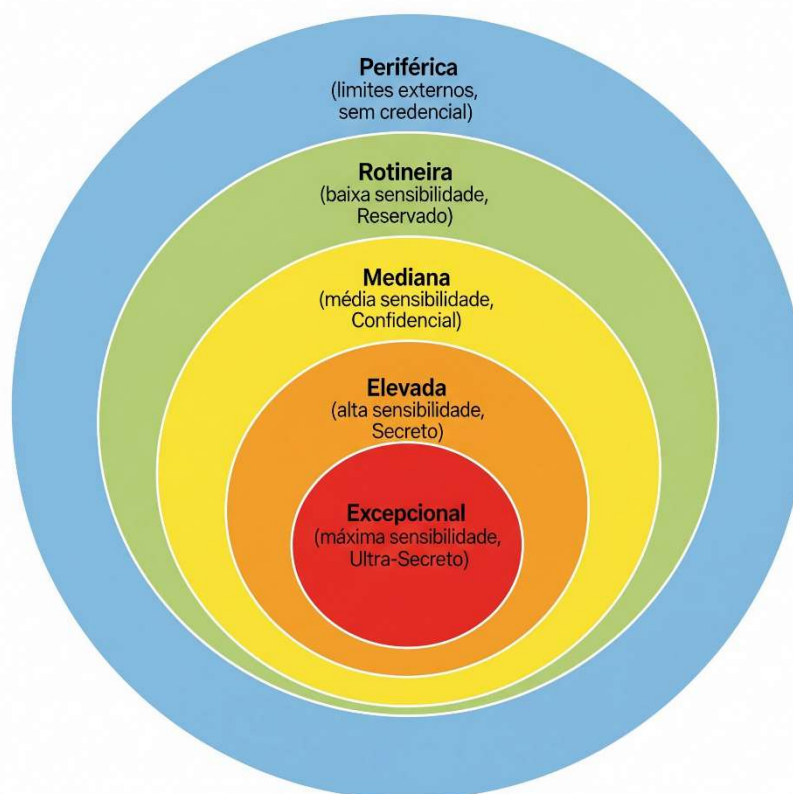
Fonte: Adaptado de Caron e Bueno (2019, p. 76)

Diferentemente de Caron e Bueno (2019), Mandarini (2005, p. 90-91) propõe a Teoria dos Círculos Concêntricos para estruturar a Segurança da Gestão das Áreas e Instalações (SGAI), organizando a segurança em camadas, partindo de uma Segurança Periférica nos

limites externos, e avançando para níveis progressivamente mais restritos – Rotineira, Mediana, Elevada e Excepcional – à medida que se aproxima do núcleo de maior sensibilidade ou periculosidade. Cada nível corresponde a requisitos de acesso e credenciamento mais rigorosos, refletindo a importância e a criticidade das Áreas, Instalações, Dependências e Ambientes (AIDA) protegidas.

O modelo de Círculos Concêntricos de Mandarini (2005, p. 91-93) com sua organização de segurança em cinco níveis hierárquicos: Periférica (limites externos, sem credencial), Rotineira (baixa sensibilidade, Reservado), Mediana (média sensibilidade, Confidencial), Elevada (alta sensibilidade, Secreto) e Excepcional (máxima sensibilidade, Ultra-Secreto) implementa uma defesa em profundidade, onde cada nível define o tipo de AIDA, o público autorizado e o grau de credenciamento exigido.

Figura 7 - Teoria dos Círculos Concêntricos.



Fonte: Adaptado de Mandarini, (2005, p. 92).

Retomando a classificação dos ativos e áreas, tal definição se torna um passo fundamental na SGAI. Mandarini (2005, p. 91) estabelece as definições de sensível e perigoso da seguinte forma:

Consideram-se sensíveis todos os materiais, equipamentos, processos, operações, áreas, instalações, dependências e ambientes (AIDA), cargos ou funções, dados, informações ou conhecimentos cujo valor, natureza ou importância exerça, direta ou indiretamente, grave influência sobre a regularidade, normalidade ou continuidade da atividade institucional. Consideram-se perigosos todos os materiais, equipamentos, processos, operações, AIDA, cargos ou funções cujo grau individual de perigo implique, direta ou indiretamente, risco ou ameaça para as instalações, as pessoas, o meio ambiente ou a sociedade. Mandarini (2005, p. 91).

Cada nível da teoria de Mandarini corresponde a requisitos de acesso e credenciamento mais rigorosos, materializando o princípio da defesa em profundidade, que consiste na aplicação de diferentes medidas de proteção, complementares e redundantes (Ramos, 2006, apud Caron; Bueno, 2019, p. 78). A materialização dessa proteção ocorre por meio de componentes práticos:

- I. **Barreiras:** São obstáculos, de qualquer natureza, a fim de impedir o ingresso de pessoas ou bens desautorizados (Brasil, 2009, apud Caron; Bueno, 2019, p. 81). Podem ser naturais (acidentes geográficos) ou artificiais, que englobam proteções estruturais (muros, cercas), eletroeletrônicas (alarmes, sensores) e humanas (postos de vigilância).
- II. **Controle de Acesso:** É o pilar operacional da SGAI, um processo que permite ou proíbe que pessoas ou bens acessem as dependências da organização (Caron; Bueno, 2019, p. 82). A autenticação para acesso a áreas críticas deve, idealmente, combinar múltiplos fatores, como “algo que você possui” (cartão), “algo que você sabe” (senha) e “algo que você é” (biometria), aumentando a confiabilidade do sistema (Mattos, 2003; Niles, 2004, apud Caron; Bueno, 2019, p. 84).
- III. **Deteção de Intrusão e Monitoramento Eletrônico:** A tecnologia moderna materializa-se em sistemas de Circuito Fechado de Televisão (CFTV) de alta resolução, sensores de movimento e sistemas de alarme, compondo o sistema eletrônico que se destina a identificar a intrusão ou a violação (Caron; Bueno, 2019, p. 85). É crucial que o monitoramento ocorra em tempo real e que os dados sejam armazenados de forma segura.
- IV. **Planejamento de Emergência:** Por fim, a SGAI deve incluir um robusto planejamento que visa prevenir, controlar e limitar os efeitos de acidentes e incêndios, além de ameaças externas e do meio ambiente (Caron; Bueno, 2019, p. 86). Este planejamento se desdobra em planos de contingência, controle de danos e evacuação, os quais devem ser avaliados e testados periodicamente para garantir sua eficácia.

No contexto do CLA, a Teoria dos Círculos Concêntricos de Mandarini, ilustrada também pela DCA 11-45, deve ser aplicada considerando a criticidade das áreas de manuseio de tecnologia AST e das plataformas de lançamento. Os critérios de segurança e os tipos de barreiras (físicas, eletrônicas e procedimentais) devem ser dimensionados para neutralizar ameaças de natureza militar e proteger ativos de alto valor estratégico e tecnológico, incluindo aqueles sob salvaguardas internacionais.

A não observância ou a falha na implementação eficaz dos princípios e componentes da Segurança da Gestão das Áreas e Instalações (SGAI) no contexto singular do Centro de Lançamento de Alcântara (CLA) pode resultar em “perdas” de diversas naturezas e magnitudes, comprometendo seriamente os objetivos da Segurança e Defesa (SEGDEF), da Força Aérea Brasileira (FAB) e do Programa Espacial Brasileiro (PEB).

A Análise de Riscos e a Prevenção de Perdas são componentes essenciais da Segurança da Gestão das Áreas e Instalações (SGAI), conforme aponta Mandarini (2005, p. 93). A SGAI deve se concentrar particularmente nas ameaças de origem humana contra o patrimônio físico – como sabotagem, roubo ou negligência – sem, contudo, desconsiderar os riscos naturais e eventos imprevisíveis, devendo se buscar a identificação e avaliação da criticidade dos riscos, seguida de um diagnóstico formal, sendo a base para estabelecer as ações preventivas necessárias à proteção das AIDA.

A gestão da Segurança da Gestão das Áreas e Instalações (SGAI) transcende os limites físicos da instituição, exigindo uma análise estratégica da “Vizinhança” (influência direta) e dos “Arredores” (influência indireta). Mandarini (2005, p. 97-99) ressalta a inevitabilidade da convivência e a necessidade de conhecer profundamente o perfil socioeconômico e político do entorno, prezando pelo estabelecimento de relações cordiais e monitoramento constante, ao mesmo tempo que alerta para a máxima cautela no envolvimento direto em problemas comunitários e, especialmente, na contratação de pessoal local para funções críticas. O objetivo final é alcançar uma relação equilibrada, onde a instituição se integra sem submeter seus imperativos de segurança às pressões externas.

A SGAI fundamenta-se, ainda, em ações de Segurança Passiva, caracterizadas por uma postura eminentemente defensiva contra ameaças potenciais ou reais. Conforme Mandarini (2005, p. 99), essa abordagem, embora defensiva, não exclui o uso pontual de medidas mais ativas.

A eficácia da Segurança Passiva reside na integração de quatro componentes essenciais: o Serviço de Vigilância, centrado no elemento humano; a Segurança Física, que

materializa as barreiras e proteções; a Segurança Eletrônica, utilizando tecnologia para detecção e monitoramento; e os Controles de Acesso, que gerenciam a circulação de pessoas e bens - Mandarinini (2005, p. 99). A sinergia entre esses componentes é crucial para construir um sistema de proteção robusto e em camadas.

O Serviço de Vigilância é um pilar tradicional e indispensável da SGAI, tendo o homem como sua principal ferramenta, mesmo na era tecnológica. Mandarinini (2005, p. 99-100) destaca a evolução da vigilância, que passou de simples postos de observação para uma participação ativa na gestão de sistemas integrados. A decisão entre vigilância orgânica ou terceirizada envolve uma análise complexa que transcende os custos, considerando fatores como a sensibilidade das áreas, o rodízio de pessoal e a necessidade de especialização. Complementarmente, a Segurança Física materializa a proteção através de meios como portas, portões, eclusas e, crucialmente, barreiras – sejam elas naturais (rios, elevações) ou artificiais (muros, cercas, fossos), podendo ser agravadas para aumentar sua eficácia, sendo que a ostensividade desses meios atua como um importante fator de dissuasão.

Já a Segurança Eletrônica representa o componente tecnológico da SGAI, oferecendo capacidades avançadas de detecção e resposta. Segundo Mandarinini (2005, p. 102-107), os sistemas eletrônicos tipicamente integram sensores, centrais de processamento e centrais de monitoramento. Os sensores, ou detetores de intrusão, são diversificados, cobrindo detecção por abertura, ruptura, manipulação, vibração, movimento (infravermelho, micro-ondas, ultrassom, dupla tecnologia) e ruídos, aplicáveis a ambientes internos, externos e perimetrais (cercas eletrificadas, cabos enterrados). Sistemas como CFTV e monitoramento por satélite (GPS) ampliam a capacidade de vigilância remota. Contudo, cumpre destacar a rápida obsolescência tecnológica, exigindo um planejamento cuidadoso de atualização e investimento.

Os Controles de Acesso são o conjunto de medidas e procedimentos que regulam a circulação e o acesso a tudo e a todos dentro da instituição. Mandarinini (2005, p. 108-115) diferencia os controles procedimentais (resultantes de rotinas, como crachás, passes, uniformes) dos controles propriamente ditos (especificamente designados para limitar acesso). Estes últimos podem ser pessoais (vigilantes, porteiros), instrumentais (cancelas, catracas, portas automáticas, eclusas, portais detetores, cartões, biometria) ou mistos. A escolha e implementação desses controles devem considerar o nível de segurança exigido, o fluxo, a tecnologia e os custos, sendo a biometria (íris, digitais, etc.) um recurso crescente para áreas de alta segurança. A gestão eficaz desses controles, incluindo a manutenção e o claviculário, é vital para a integridade do sistema.

Além dos pilares principais, a SGAI deve se preocupar com elementos de suporte que impactam diretamente a segurança. Mandariní (2005, p. 115-117) aponta a iluminação (normal e de emergência) como um fator crítico, cuja gestão (avaliação, manutenção, segurança dos sistemas) compete à SGAI para garantir visibilidade adequada e dissuasão.

A dualidade entre prevenção e assunção de riscos, conforme exposta por Mandariní (2005), adquire contornos críticos no CLA, dada a natureza das operações, que envolvem tecnologias de altíssimo valor (muitas sob o AST) e riscos operacionais elevados, o foco primário da SGAI no CLA deve ser a prevenção, materializada em robustos investimentos em sistemas de segurança física, eletrônica, cibernética e de pessoal.

Contudo, a assunção também se faz presente, não apenas pela contratação de seguros para cobrir cargas úteis e lançamentos comerciais, mas pelo reconhecimento de que certos riscos (como falhas catastróficas ou eventos naturais extremos) nunca podem ser totalmente eliminados.

O gerenciamento de riscos no CLA, portanto, exige uma análise de custo-benefício contínua e metodologicamente quantificada, para justificar os investimentos em segurança e embasar decisões estratégicas que garantam a continuidade operacional sem comprometer a viabilidade econômica e os acordos internacionais.

A localização geográfica e o contexto sociopolítico do CLA, em Alcântara, Maranhão, tornam a estratégia de Apoio Mútuo fundamental, embora seja uma instalação militar com significativa capacidade orgânica, a segurança do Centro não pode prescindir da colaboração com os órgãos de Segurança Pública (Polícias Federal e Militar) para lidar com ameaças externas, com a Marinha do Brasil para o controle da área marítima, e com a Agência Brasileira de Inteligência (ABIN) para a antecipação de ameaças.

Essa rede de colaboração é a base para a eficácia da Segurança Ativa, permitindo que a Força Aérea Brasileira (FAB) não apenas utilize suas forças de reação internas, mas também acione, de forma coordenada e estratégica, os recursos do Estado para responder a incidentes, gerenciar crises ou neutralizar ameaças, sempre ponderando a necessidade de discrição versus a demonstração de força, conforme o cenário exigir.

A complexidade operacional e os múltiplos vetores de ameaça no CLA tornam a Integração de Sistemas um requisito indispensável, e não apenas uma tendência. A visão de Mandariní (2005) de um grande sistema gestor traduz-se, na prática, na necessidade de um Centro de Operações de Segurança (COS) avançado em Alcântara.

Tal centro deve ser capaz de consolidar e correlacionar, em tempo real, informações provenientes de fontes díspares: sensores perimetrais, câmeras de CFTV, sistemas de controle

de acesso (incluindo biometria e registros AST), dados de inteligência, relatórios de vigilância humana, alertas de cibersegurança e status dos sistemas de emergência (iluminação, incêndio). Somente através dessa integração é possível obter a consciência situacional necessária para uma tomada de decisão rápida e eficaz, otimizar o emprego dos recursos de segurança e garantir o cumprimento dos rigorosos padrões exigidos para as operações aeroespaciais internacionais.

4.3.2 Segurança da Gestão das Pessoas (SGP)

A Segurança da Gestão das Pessoas (SGP) dedica-se a minimizar os riscos associados aos Recursos Humanos (RH) em todo o ciclo de vida do colaborador. No setor público, a Segurança de Pessoas visa proteger a integridade física e moral dos integrantes da instituição (Bandeira, 2019, p. 42), sendo o fator humano tanto o melhor ativo de segurança, mas também a sua maior vulnerabilidade (Mitnick apud Caron; Bueno, 2019, p. 90).

No âmbito do setor público, o conceito análogo, a Segurança de Pessoas, é compreendida como o conjunto de medidas que objetivam proteger a integridade não só física, mas também moral dos integrantes da Instituição (Bandeira, 2019, p. 42) e constitui um dos ativos organizacionais a serem protegidos (Menezes *et al.*, 2022, p. 82).

O foco da SGP é, portanto, gerenciar as vulnerabilidades inerentes ao fator humano. Afinal, as pessoas são para a instituição o seu melhor ativo de segurança, mas também a sua maior vulnerabilidade, o elo mais fraco da corrente (Mitnick apud Caron; Bueno, 2019, p. 90). Fragilidades individuais, negligência ou a suscetibilidade à Engenharia Social — técnica de manipulação para obter informações — transformam as pessoas em um ponto a ser explorado por ameaças (Caron; Bueno, 2019, p. 90).

A SGP abrange desde o processo de recrutamento e seleção, passando pela investigação de antecedentes, credenciamento, acompanhamento funcional e comportamental, até os procedimentos de desligamento. Essa abordagem é essencial para mitigar ameaças internas, como vazamento de informações, sabotagem ou cooptação por inteligência adversa, um risco sempre presente em organizações estratégicas como o CLA (Bandeira, 2019)

No CLA, onde coexistem militares, servidores civis, funcionários terceirizados e pessoal de nações parceiras (AST), uma SGP robusta é essencial. Ela transcende a mera administração de pessoal, alinhando-se ao conceito de Segurança Corporativa Estratégica como um pilar para a prevenção de ameaças internas, a proteção eficaz de tecnologias e

informações sensíveis, e, acima de tudo, para assegurar a confiabilidade, o sigilo e o comprometimento de cada indivíduo com a segurança integral da missão aeroespacial brasileira em Alcântara.

A complexidade operacional do Centro de Lançamento de Alcântara (CLA) implica, frequentemente, o recurso à terceirização para diversas atividades-meio. No entanto, essa prática exige uma extensão rigorosa dos princípios da Segurança da Gestão das Pessoas (SGP). Mandarinini (2005, p. 144-146) alerta para os novos problemas trazidos pela terceirização, como a falta de compromisso com os objetivos da empresa e as dificuldades no controle de pessoal, recomendando expressamente que funções e atividades sensíveis, ligadas à alta gestão ou aos segredos da empresa, não sejam terceirizadas.

É fundamental, portanto, que os processos de contratação incluam a verificação minuciosa dos antecedentes de todos os empregados terceirizados que terão acesso às instalações ou informações. Essa diligência é ainda mais crítica no contexto do Acordo de Salvaguardas Tecnológicas (AST), onde a proteção exige um controle intransigente, ecoando a cautela que Mandarinini (2005, p. 98) sugere ao empregar pessoal da vizinhança em pontos críticos ou sensíveis.

Dada sua relevância estratégica, o CLA é palco frequente de visitas de autoridades, delegações internacionais e parceiros comerciais. A SGP, portanto, deve estabelecer protocolos claros e rigorosos, pois, como destaca Mandarinini (2005, p. 147-148), é crucial a intensa participação da SCorp nesses eventos, contribuindo com levantamento de informações, preparando locais, prevendo varreduras, cadastramentos, planejando os deslocamentos e outras ações de segurança. Isso envolve desde o cadastramento prévio até o acompanhamento constante e a definição de zonas de acesso, equilibrando a necessidade de relacionamento com a proteção rigorosa de informações e ativos, minimizando as janelas de vulnerabilidade.

A diversidade do capital humano no CLA amplia o espectro de potenciais ameaças internas, dessa forma a SGP deve ainda desenvolver e implementar procedimentos robustos para a gestão de ilícitos, considerando que a fraude é a matriz dos principais ilícitos praticados contra as corporações, como aponta Mandarinini (2005, p. 148-149).

A negligência ou ineficácia na aplicação dos preceitos da Segurança da Gestão das Pessoas (SGP) no ambiente complexo e sensível do CLA pode originar um espectro diversificado de “perdas”, com potencial para comprometer desde a segurança da informação até a integridade das operações e a eficácia da Segurança e Defesa (SEGDEF) como um todo.

A prevenção de atos como desfalques, falsificações, furtos ou vazamentos exige controles internos, auditorias e programas de conscientização, além da capacidade de investigar e responder a tais incidentes. Adicionalmente, é crucial possuir planos de contingência para gerenciar crises como ameaças ou coações, garantindo a proteção dos indivíduos e dos interesses estratégicos do Centro.

Nesse complexo cenário do CLA, onde coexistem militares, servidores civis, funcionários terceirizados e pessoal de nações parceiras (AST), uma SGP robusta e proativa é absolutamente essencial. Ela transcende a mera administração de pessoal, alinhando-se ao conceito de Segurança Corporativa Estratégica como um pilar para a prevenção de ameaças internas, a proteção eficaz de tecnologias e informações sensíveis, e, acima de tudo, para assegurar a confiabilidade, o sigilo e o comprometimento de cada indivíduo com a segurança integral da missão aeroespacial brasileira em Alcântara.

Os processos de recrutamento, investigação de antecedentes, credenciamento (especialmente para acesso a áreas e informações do AST) e monitoramento contínuo do pessoal (militar, civil, terceirizado e estrangeiro) devem ser excepcionalmente rigorosos. A SGP deve se alinhar com as diretrizes de contrainteligência da FAB para prevenir ameaças internas e garantir a confiabilidade do efetivo envolvido em operações e tecnologias sensíveis.

4.3.3 Segurança da Gestão dos Processos (SGProc)

A Segurança da Gestão dos Processos (SGProc) dedica-se a proteger a dinâmica da atividade institucional, abrangendo o conjunto de todos os procedimentos e atividades que levam ao produto ou serviço final. No setor público, a Segurança dos Procedimentos é considerada uma das prioridades para garantir a integridade dos ativos organizacionais (Menezes *et al.*, 2022, p. 85). A eficácia da SGProc reside na integração de seus três componentes: a Segurança das Operações (SOp), a Segurança do Planejamento (SPlj) e a Segurança dos Insumos (SInsu).

A Segurança da Gestão dos Processos (SGProc), como um dos pilares fundamentais da Segurança Corporativa Estratégica delineada por Mandarinini (2005, p. 156), dedica-se a proteger a dinâmica da atividade institucional, abrangendo o conjunto de todos os procedimentos e atividades que levam ao produto ou serviço final, entendendo-os como fluxos contínuos e inter-relacionados.

Com enfoque na SInsu, este se estende a proteção a todos os itens empregados, com foco naqueles de alta sensibilidade ou periculosidade. Para o CLA, ela rege a segurança no

transporte de componentes de foguetes, no manuseio de propelentes e tecnologias AST, e no descarte de resíduos. A Segurança dos Materiais e Equipamentos é, de fato, uma das políticas prioritárias em diagnósticos de segurança de unidades públicas (Menezes et al., 2022, p. 85)

A gestão dos processos no CLA envolve uma série de subsegmentos operacionais cruciais para a eficácia da SEGDEF, os quais se desdobram nas seguintes dimensões:

4.3.3.1 Segurança das Operações (SOp)

A Segurança das Operações (SOp) dedica-se a proteger as atividades e procedimentos centrais de uma instituição, com foco naquelas consideradas sensíveis (que afetam a continuidade do negócio) e perigosas (que implicam riscos físicos) (Mandarini, 2005, p. 156-165). A SOp atua sobre essa dualidade, buscando determinar o gênero e o grau de ameaça para estabelecer uma escala de criticidade que guiará as ações de segurança. No CLA, as operações de preparação, integração e lançamento de veículos aeroespaciais são, por natureza, simultaneamente sensíveis e perigosas, exigindo a máxima atenção da SOp para prevenir perdas.

O ponto de partida é a Análise do Processo Institucional, um estudo detalhado do fluxo de atividades para identificar, em cada etapa, as operações sensíveis e/ou perigosas. Mandarini (2005, p. 157-158) diferencia as operações que influenciam indiretamente a continuidade (onde a SOp atua mais em apoio técnico) daquelas sensíveis de fato, que impactam diretamente a regularidade e a continuidade. Estas últimas, junto com as perigosas, são o foco prioritário da SOp, dado o potencial de perdas que podem acarretar. É essencial, nessa fase, a colaboração com as equipes técnicas para listar procedimentos, mapear locais, definir situações críticas e estabelecer parâmetros claros de atuação.

Uma vez identificadas as operações críticas, a SOp busca determinar seu gênero e grau de criticidade. O gênero define se a operação é sensível, perigosa ou ambas, identificando quem suportaria os danos (a empresa, a sociedade ou ambos). O grau de criticidade, por sua vez, é obtido por meio de uma análise de risco que avalia a probabilidade e o impacto de eventos adversos (Mandarini, 2005, p. 158-159).

Para quantificar e priorizar, Mandarini (2005, p. 159-160) propõe uma Escala de Criticidade, que pode ser adaptada a cada instituição. Um exemplo dessa abordagem é apresentado na tabela abaixo:

Tabela 10 - Escala de Criticidade.

NÍVEL	SENSIBILIDADE DE FATO	PERICULOSIDADE	CRITICIDADE
1	Não dificultam o processo operacional	Não causam dano às pessoas/ambiente	1
2	Causam baixa dificuldade ao processo	Causam leve dano às pessoas/ambiente	2
3	Causam média dificuldade ao processo	Causam médio dano às pessoas/ambiente	3
4	Causam alta dificuldade ao processo	Causam grave dano às pessoas/ambiente	4
5	Impedem a operação da instituição	Causam gravíssimo dano às pessoas/ambiente	5

Fonte: Adaptado de Mandarini (2005, p. 159-160)

A criticidade final de uma operação é calculada somando-se os valores de Sensibilidade e Periculosidade, sugerindo-se ainda a aplicação de pesos a um dos critérios, caso a instituição deseje priorizar, por exemplo, a sensibilidade sobre a periculosidade, ou vice-versa. Essa escala fornece uma base objetiva para decidir a oportunidade, urgência, amplitude e profundidade das medidas de SOp e para justificar os investimentos necessários em segurança (Mandarini, 2005, p. 160-161).

Com base nessa criticidade, a SOp propriamente dita implementa medidas específicas. Para as operações perigosas, mesmo que o dano material seja pequeno, a SOp intervém devido ao potencial impacto nos ativos intangíveis (imagem, credibilidade), atuando em conjunto com as áreas técnicas e estabelecendo rotinas de emergência (Mandarini, 2005, p. 161-163). Para as operações sensíveis de fato, o “coração do negócio”, a SOp atua de forma ainda mais intensa e abrangente, implementando medidas como controle de fluxogramas, compartimentação, rodízios e ações contra sabotagem, visando garantir, acima de tudo, a regularidade e a continuidade do processo (Mandarini, 2005, p. 163-165).

No CLA, onde as operações de preparação e lançamento de veículos aeroespaciais são intrinsecamente sensíveis - dado o valor estratégico das cargas úteis, das tecnologias envolvidas, especialmente sob o AST, e das informações de missão, e perigosas - devido ao manuseio de grandes volumes de propelentes e sistemas pirotécnicos, falhas na Segurança das Operações (SOOp) podem desencadear “perdas” de consequências graves e multifacetadas, minando os objetivos da Segurança e Defesa (SEGDEF),

4.3.3.2 Segurança do Planejamento (SPlj)

A Segurança do Planejamento (SPlj) inicia sua atuação na própria gênese das atividades institucionais (Mandarini, 2005, p. 166-174). No CLA, a SPlj assume uma importância crítica, pois o planejamento de campanhas de lançamento, a integração de novas tecnologias (especialmente sob o AST) e os próprios planos de segurança são, por definição, altamente sensíveis. A SPlj no CLA deve garantir que os princípios de Confidencialidade e Compartimentação sejam rigorosamente aplicados, controlando o acesso à informação entre diferentes equipes, órgãos (FAB, AEB, INPE) e parceiros internacionais, para prevenir vazamentos que poderiam comprometer missões, acordos estratégicos e a segurança nacional.

A determinação do nível de sensibilidade é um passo crítico na SPlj, pois orienta a intensidade das medidas de segurança. Mandarini (2005, p. 169-171) propõe a criação de uma escala, similar à da SOP, utilizando parâmetros como a influência do plano no produto, no negócio, na segurança e nos custos, permitindo uma classificação objetiva e a priorização das ações.

Independentemente do nível, dois princípios são basilares para planejamentos sensíveis: a Confidencialidade, que restringe o número de pessoas com acesso, e a Compartimentação, que limita o acesso à informação estritamente necessária (*need-to-know*). Estes princípios devem permear todas as fases do planejamento, desde o esboço preliminar até a sua manutenção.

A SPlj atua através de um conjunto de ações normativas e específicas. As normativas disciplinam todo o processo de planejamento na instituição, definindo quem pode autorizar, justificar, interromper ou encerrar planos. Já as ações específicas, aplicadas aos planejamentos sensíveis, robustecem a segurança com medidas técnicas e procedimentais adicionais. Mandarini (2005, p. 172-174) lista exemplos como o estabelecimento de controles rigorosos sobre pessoal, documentos, recursos, locais de reunião, comunicações (incluindo varreduras), e a exigência de termos de confidencialidade.

A SPlj, portanto, não apenas implementa, mas também opina sobre o nível de sensibilidade e as medidas adequadas, exigindo, para sua eficácia, um forte comprometimento da alta gestão e confiança nos profissionais de segurança.

A determinação cuidadosa dos níveis de sensibilidade e a aplicação de medidas específicas – desde a segurança física dos locais de planejamento até a segurança das comunicações e a verificação de pessoal – são essenciais para prevenir vazamentos que poderiam comprometer missões, acordos estratégicos e a segurança nacional.

4.3.3.3 Segurança dos Insumos (SInsu)

A Segurança dos Insumos (SInsu), como parte integrante da Gestão de Processos, estende a proteção corporativa a todos os itens empregados na produção ou prestação de serviços. Mandarini (2005, p. 177-195) esclarece que, embora o universo de insumos seja vasto, a SInsu foca naqueles que se destacam por sua sensibilidade (valor, importância para o negócio) ou periculosidade (risco físico).

Garante o recebimento, armazenamento e manuseio seguros de propelentes (altamente perigosos) e tecnologias AST (altamente sensíveis), integrando-se à SGAI para a proteção de paiois e almoxarifados. A Segurança dos Materiais e Equipamentos é, de fato, uma das políticas prioritárias identificadas em diagnósticos de segurança de unidades públicas, com alta recorrência de preocupação (Menezes *et al.*, 2022, p. 85).

O primeiro passo da SInsu é, portanto, determinar o nível de criticidade de cada item, considerando tanto os riscos a que estão sujeitos (roubo, sabotagem) quanto os riscos que podem gerar (inflamáveis, tóxicos). Essa classificação orientará a profundidade das medidas de segurança em todas as fases: aquisição, transporte, recebimento, armazenamento, uso e descarte.

A SInsu adota abordagens distintas para insumos “em prateleira” (armazenados ou em almoxarifado) e “em uso”, para os insumos em prateleira, Mandarini (2005, p. 181-185) enfatiza a necessidade de procedimentos sistemáticos de controle (inventários, auditorias, controle de condições ambientais) e medidas de segurança específicas, coordenadas com a SGAI, para garantir a integridade, inviolabilidade e incolumidade. Já para os insumos em uso, a segurança foca no controle do emprego e utilização, na responsabilidade do usuário e na manutenção preventiva, aplicando medidas como rodízios, sistemas de chaves duplas e controles específicos para itens como armamentos ou substâncias perigosas, sempre buscando minimizar riscos durante a operação (Mandarini, 2005, p. 185-186).

Um dos focos mais detalhados da SInsu, conforme Mandarini (2005, p. 186-195), é a Segurança do Insumo em Deslocamento, crucial no contexto logístico atual e particularmente relevante no Brasil devido aos riscos no transporte rodoviário de cargas (TRC). A SInsu deve avaliar a necessidade de discrição (para itens sensíveis) ou ostensividade (para itens perigosos ou por exigência legal). Vejamos a tabela 11, Discrição vs. Ostensividade no Transporte, adaptado de Mandarini (2005, p. 187).

Tabela 11: Descrição vs. Ostensividade no Transporte.

ITEM	DISCRIÇÃO	OSTENSIVIDADE	FUNDAMENTO
Armamento (pistolas)	Desejável (Sensibilidade)	Indesejável	O baixo grau de perigo do material em si.
Munição	Desejável (Pequenas qtd.)	Necessária (Grandes qtd. / Lei)	O grau de perigo define o perfil da segurança.
Tóxico (gás)	Indesejável	Desejável (Periculosidade)	O elevado grau de perigo do material em si.
Pequenos Valores	Desejável (Valor)	Indesejável	O baixo grau de perigo do material em si.
Material Contagioso	Indesejável	Necessária	O elevado grau de perigo do material em si.
Grandes Valores	Dispensável	Conveniente	A ostensividade atua como desestimulador.

Fonte: Adaptado de Mandarinini (2005, p. 187)

O planejamento logístico deve incluir uma minuciosa análise de segurança, considerando a modalidade de transporte, itinerários, pontos de apoio e, no caso do TRC, a implementação de um Plano de Gerenciamento de Riscos (PGR), que envolve cadastro de motoristas, rastreamento (GPS), escolta armada, centrais de monitoramento e planos de contingência, visando mitigar os altos índices de roubo e desvio de cargas.

A atuação da SInsu, segundo Mandarinini (2005, p. 189-191), abrange todo o ciclo de vida do insumo, se iniciando na aquisição e contratação, onde participa da verificação de fornecedores para evitar produtos de má qualidade, falsificados ou de origem ilícita, passa pelo recebimento e expedição, com procedimentos rigorosos de conferência e registro, especialmente para ICSP e se estende até o descarte, tratando o lixo classificado – rejeitos sensíveis (HDs, documentos) ou perigosos (químicos, sucatas) – com rotinas específicas de recolhimento, manuseio e destruição, garantindo que mesmo os resíduos não se tornem uma vulnerabilidade para a instituição.

Para o Centro de Lançamento de Alcântara (CLA), a SInsu é de importância capital. Ela rege a segurança no transporte de componentes de foguetes e satélites (muitas vezes sensíveis e de alto valor) pelas rodovias do Maranhão até o Centro, exigindo um robusto PGR. Garante o recebimento, armazenamento e manuseio seguros de propelentes (altamente perigosos) e tecnologias AST (altamente sensíveis), integrando-se à SGA para a proteção de paióis e almoxarifados.

A SInsu também supervisiona a aquisição de componentes, assegurando sua procedência e qualidade, e o descarte seguro de resíduos perigosos ou classificados, fechando o ciclo de proteção dos processos vitais para as operações em Alcântara, sendo vital para a

Segurança e Defesa (SEGDEF) e para prevenir “perdas” que podem afetar desde a logística até a segurança das operações finais.

4.3.4 Segurança da Gestão do Conhecimento (SGC)

Na transição para a Era do Conhecimento, a Segurança Corporativa Estratégica (SCorpE) reconhece o conhecimento – definido por Mandarinini (2005, p. 201-203) como o significado obtido da análise e interpretação de dados e informações para subsidiar o processo decisório – como um diferencial competitivo e estratégico para nações e empresas.

Esta visão é compartilhada pela doutrina de inteligência, que define a Atividade de Inteligência como o exercício de ações especializadas para obtenção e análise de dados, produção de conhecimentos e proteção de conhecimentos para o país (ABIN, 2020, apud Kinopp; Maba, 2023, p. 28587).

Suas principais características são a multidisciplinaridade, clareza, objetividade e, crucialmente, a oportunidade, permitindo decisões mais seguras e menos baseadas em oportunismo, especialmente em domínios como geopolítica, economia, militar e científico-tecnológico.

No setor público, a Segurança das Informações é um dos ativos prioritários a serem protegidos (Menezes *et al.*, 2022, p. 83). Para tal, a Contraineligência atua para proteger as informações e o próprio planejamento e execução das atividades do Serviço de Inteligência (ABIN, 2020, apud Kinopp; Maba, 2023, p. 28585).

A obtenção de dados e informações para a produção do conhecimento envolve, segundo Mandarinini (2005, p. 203-204), duas abordagens distintas: a “Coleta”, referente à obtenção de dados disponíveis em fontes abertas ou não protegidas, e a “Busca”, que implica um esforço especializado para adquirir informações protegidas.

A SGC prioriza a proteção dos conhecimentos considerados “segredos da empresa”, o que exige uma sistemática para determinar o nível de sensibilidade de cada informação. Este processo requer uma profunda interação com todos os segmentos da SCorp (SGAI, SGP, SGProc), consolidando os perfis de sensibilidade e periculosidade de diversos itens para estabelecer uma disciplina de classificação sigilosa dos conhecimentos em toda a instituição.

Mandarinini (2005, p. 205-207) propõe uma metodologia para o Ciclo da Produção dos Conhecimentos, especialmente os sensíveis, que se divide em cinco fases: Planejamento (definição do escopo e segurança), Reunião (coleta e busca), Análise e Síntese (avaliação e integração dos dados), Interpretação (delineamento do significado) e

Formalização/Utilização. Dada a natureza intangível do conhecimento, a SGC mantém uma relação intrínseca com os demais pilares, especialmente com a Segurança dos Suportes (SSup), que protege os meios físicos da informação, e a Segurança da Tecnologia da Informação (STI), que salvaguarda o conhecimento digitalizado.

Para uma compreensão e implementação eficazes, a Segurança da Gestão do Conhecimento pode ser dividida em segmentos inter-relacionados. Mandarini (2005, p. 208-209) sugere quatro componentes principais: a Segurança da Informação, que trata dos procedimentos e medidas de segurança dos dados e informações em si; a Segurança dos Suportes, focada nos meios físicos (papel, mídias digitais) onde a informação reside; a Segurança das Telecomunicações, responsável pela proteção do recebimento e difusão dos conhecimentos; e a Segurança da Tecnologia da Informação, que cuida da segurança do conhecimento em formato digital, abrangendo a cibersegurança. Juntos, esses segmentos formam a espinha dorsal da proteção do capital intelectual e estratégico da organização.

No contexto do Centro de Lançamento de Alcântara (CLA), a SGC é de importância transcendental tendo em vista que as operações aeroespaciais, envolvem um volume massivo de conhecimento sensível – desde dados técnicos de veículos lançadores e satélites, informações estratégicas de missões, até tecnologias protegidas pelo Acordo de Salvaguardas Tecnológicas (AST). A aplicação rigorosa dos princípios da SGC – incluindo a classificação da informação, o controle de acesso ao conhecimento (“Busca” vs. “Coleta”), a proteção dos sistemas de TI contra ciberameaças, a segurança das comunicações com os veículos em voo e a proteção física dos documentos e mídias – é imperativa. Uma falha na SGC poderia comprometer não apenas uma missão específica, mas a segurança nacional, a credibilidade internacional do Brasil e a viabilidade de acordos estratégicos como o AST.

Portanto, no contexto do CLA, onde o conhecimento tecnológico, operacional e estratégico é um dos ativos mais valiosos e cuja proteção é um dos pilares da Segurança e Defesa (SEGDEF), falhas na Segurança da Gestão do Conhecimento (SGC) podem gerar “perdas” de consequências estratégicas e de longo alcance.

4.4 A SEGURANÇA CORPORATIVA ESTRATÉGICA (SCorpE): PILARES E APLICAÇÃO NA FAB

A Segurança Corporativa Estratégica (SCorpE) representa a culminação da evolução da segurança no ambiente empresarial, transcendendo a mera prevenção de perdas para se posicionar como um elemento fundamental para a competitividade e o valor do negócio.

Mandarini (2005, sem paginação) define a SCorpE como um modelo que objetiva estabelecer singular proteção à produção ou à prestação de serviços, vai além; elabora planejamentos integrados, mantém suas ações coordenadas e institui programas de educação para segurança.

A aplicação da SCorpE no contexto da Força Aérea Brasileira (FAB) e, especificamente, no Centro de Lançamento de Alcântara (CLA), requer uma cuidadosa adaptação dos seus fundamentos. Diferentemente do ambiente corporativo, onde a finalidade primária é a proteção do negócio e a maximização do valor para acionistas, a SEGDEF no CLA visa primordialmente a manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da Pátria, conforme estabelecido pela DCA 11-45, e preservar o poder combatente da Força Aérea Brasileira, como orienta a NSCA 205-3.

Assim, o conceito de “perdas” transcende o financeiro, englobando dimensões estratégicas, de soberania e de segurança nacional. Adicionalmente, a natureza das ameaças ao CLA – como espionagem estatal, sabotagem de infraestrutura crítica e ciberataques avançados – possui um espectro distinto das ameaças corporativas convencionais. A cultura organizacional militar, com seus valores de Patriotismo, Disciplina e Comprometimento, e sua estrutura de comando, também moldam a forma como a SCorpE deve ser implementada, diferindo das práticas empresariais. A gestão de recursos públicos e os imperativos legais específicos do setor de defesa, incluindo os rigorosos requisitos do Acordo de Salvaguardas Tecnológicas - AST, impõem camadas adicionais de complexidade que demandam uma tradução e, por vezes, uma reinterpretação dos princípios da SCorpE para o cenário militar aeroespacial.

Esta abordagem estratégica é crucial porque, em primeiro lugar, salvaguarda e garante acesso, com oportunidade, ao diferencial de competitividade que distingue o produto ou serviço: o conhecimento. Para a FAB, isso se traduz na proteção de informações sensíveis e no know-how tecnológico relacionado ao programa espacial brasileiro, essencial para o Poder Aeroespacial. Além disso, a SCorpE protege e contribui para a manutenção da regularidade, normalidade e continuidade da produção ou serviço, ou seja, do próprio negócio, sendo a continuidade das operações de lançamento e a integridade das missões espaciais no CLA exemplos diretos desse pilar. A abordagem também facilita a tomada de decisão, pois um sistema de segurança estratégico fornece subsídios para que a alta gestão tome decisões informadas, mitigando riscos e otimizando recursos a partir de um profundo conhecimento dos processos.

Por fim, a SCorpE previne riscos e evita prejuízos, embora a FAB não opere com fins lucrativos no sentido comercial, a prevenção de acidentes e perdas resulta em economia de

recursos públicos e na preservação da capacidade operacional, o que pode ser interpretado como um ganho em eficiência e eficácia da gestão pública.

Conforme Perrow (1999), o risco de acidentes é inerente a sistemas de alto risco como as operações espaciais, o que reforça a necessidade de um planejamento robusto para mitigar perdas. Nesse sentido, o perfil da SCorpE é caracterizado por ações coordenadas e integradas por um núcleo multidisciplinar de recursos humanos com capacidade técnica para participar e contribuir com as decisões estratégicas das empresas, demonstrando sua inequívoca vocação para aumentar a aderência ao produto ou serviço, agregar competitividade aos processos e valor ao negócio (Mandarini, 2005, sem paginação).

4.4.1 Cultura Organizacional, Filosofia e Política de Segurança na FAB

A eficácia das ações de segurança em uma organização está intrinsecamente ligada à sua cultura. Mandarini (2005, p. 15-16) destaca que toda empresa possui características próprias e específicas que a diferenciam, e que o delineamento dessa cultura é indispensável para a implementação de estratégias de segurança adequadas.

A cultura organizacional da FAB, fortemente influenciada por valores militares, hierarquia, disciplina e um profundo senso de missão nacional, fornece a base sobre a qual a Filosofia e a Política de Segurança e Defesa (SEGDEF) são construídas. Contudo, para que a segurança seja efetiva, é preciso ir além da conformidade com as normas e desenvolver uma verdadeira “cultura de segurança”. Conforme ressaltado na doutrina de segurança institucional, o êxito de qualquer programa de segurança depende do desenvolvimento de uma sadia mentalidade de segurança entre todos os funcionários (Bessa, 2002, apud Caron; Bueno, 2019, p. 90).

Essa cultura produz reflexos administrativos e operacionais em todos os segmentos, tornando indispensável o seu delineamento para a implementação de estratégias de segurança adequadas.

No âmbito da Força Aérea Brasileira (FAB) e, por conseguinte, na abordagem da SEGDEF do Centro de Lançamento de Alcântara (CLA), a Filosofia e a Política de Segurança devem transcender uma visão meramente patrimonial ou restrita à segurança física, alinhando-se com a concepção mais ampla de SEGDEF preconizada pelo Comando da Aeronáutica (COMAER).

A Filosofia de Segurança da FAB, refletida em sua doutrina, deve permear todas as ações no CLA, enfatizando a SEGDEF como um componente essencial do Poder

Aeroespacial e da soberania nacional. Esta filosofia precisa estar alinhada à concepção ampla de SEGDEF do COMAER, que, conforme a DCA 205-4, envolve a preservação do poder de combate da FAB e a garantia do grau de segurança desejado das instalações, dos equipamentos e do pessoal (Brasil, 2020).

A Política de SEGDEF da FAB, materializada em seu arcabouço normativo (como as DCA's e NSCA's), traduz essa filosofia em regras e diretrizes claras para cada segmento da organização. Conforme Mandarini (2005), para serem eficazes, as políticas necessitam ser formalizadas e apoiadas pela alta gestão.

Nesse sentido, a cultura organizacional deve fomentar o entendimento de que a segurança é responsabilidade de todos e um pilar para o cumprimento da missão, incentivando o envolvimento do público interno, desenvolvendo uma cultura de segurança, com o objetivo de estabelecer atitudes favoráveis, frente às exigências de segurança (Farah, 2013, apud Caron; Bueno, 2019, p. 90).

4.4.2 Endomarketing e Educação para Segurança na FAB

A implementação bem-sucedida de um planejamento de segurança depende fortemente da cooperação, participação e envolvimento do público interno (PI). Para engajar o efetivo, Mandarini (2005) propõe o uso do Endomarketing, que consiste em ações de marketing desenvolvidas especificamente para o público interno, com o objetivo de “vender” a importância da segurança e facilitar a integração das medidas e procedimentos nos processos diários.

Complementar ao endomarketing, a Educação para Segurança é um programa de disciplinas direcionado para o público interno das instituições, elaborado com a finalidade de desenvolver, nos RH e na alta administração, uma mentalidade de segurança que atenda às necessidades corporativas (Mandarini, 2005, p. 73-74).

Este conceito é fundamental e amplamente defendido na segurança institucional. A Resolução nº 156 do CNMP, por exemplo, destaca a necessidade do desenvolvimento da cultura de segurança entre os integrantes da Instituição (Dalabrida, 2019, p. 19), pois o fator humano é frequentemente o elo mais fraco da cadeia de segurança.

O objetivo da educação para segurança vai além de simplesmente ensinar procedimentos; busca “educar” e envolver o público interno no esforço corporativo para aprimorar a segurança.

Nesse sentido, os programas de treinamento e de sensibilização sobre a importância da segurança são partes do conjunto de medidas para proteção dos ativos corporativos e uma maneira de despertar a responsabilidade nas pessoas (Bessa, 2002, apud Caron; Bueno, 2019, p. 86).

Complementar ao endomarketing, a Educação para Segurança é um programa de disciplinas direcionado para o público interno das instituições, elaborado com a finalidade de desenvolver, nos RH e na alta administração, uma mentalidade de segurança que atenda às necessidades corporativas (Mandarini, 2005, p. 73-74).

A Educação para Segurança é parte integrante das políticas setoriais e, na prática, apresenta o planejamento de segurança elaborado para a instituição, demonstrando a importância da participação de cada RH em sua implementação.

O programa abrange partes comuns a todos os segmentos (procedimentos, responsabilidades em casos de eventos como incêndio ou alagamento), partes específicas para cada segmento corporativo (administração, finanças, logística) e partes relativas a cada um dos segmentos da Segurança Corporativa (SGP, SGAI, SGProc, SGC). Um exemplo bem conhecido é o programa de Segurança do Trabalho. O desenvolvimento de um bom programa de educação para segurança é essencial para promover uma mentalidade de segurança corporativa, que contemple o comportamento do público interno em situações gerais, dentro e fora da empresa.

A aplicação dessas estratégias de Endomarketing e Educação para Segurança no Centro de Lançamento de Alcântara é particularmente vital para mitigar os riscos associados ao fator humano e para consolidar uma cultura de Segurança e Defesa (SEGDEF) proativa e resiliente, alinhada com os objetivos da SCorpE e as normativas da FAB.

No ambiente do CLA, que congrega um efetivo diversificado (militares de várias especialidades, servidores civis, funcionários de empresas terceirizadas e, potencialmente, técnicos de nações parceiras sob o AST), a implementação de um programa robusto de educação para segurança é um imperativo para a eficácia da Segurança e Defesa (SEGDEF).

Este programa deve transcender os treinamentos pontuais, estabelecendo um currículo contínuo e adaptado a cada público, abordando desde a doutrina de Segurança e Defesa (SEGDEF) da FAB (conforme DCA 205-4 e NSCA 205-3) e os princípios da SCorpE, até os protocolos específicos de segurança física, da informação (incluindo os do AST) e de emergência. A meta é educar e envolver o público interno no esforço corporativo para aprimorar a segurança institucional, fomentando a mentalidade coletiva de segurança preconizada pela NSCA 205-3/2024 e pela DCA 205-4/2020.

Paralelamente, ações de Endomarketing devem ser empregadas para vender a importância da Segurança e Defesa (SEGDEF) ao público interno do CLA, utilizando os canais de comunicação da FAB para disseminar uma visão positiva da segurança, não como um entrave, mas como um valor essencial e um facilitador do sucesso das missões. Campanhas de conscientização sobre riscos específicos (como espionagem ou ciberameaças), o reconhecimento de boas práticas e a promoção de uma cultura onde o reporte de vulnerabilidades é incentivado, são exemplos de como o endomarketing pode fortalecer o comprometimento de todos com a Segurança e Defesa (SEGDEF) no Centro.

A aplicação dessas estratégias de Endomarketing e Educação para Segurança no CLA é, portanto, vital para mitigar os riscos associados ao fator humano e para consolidar uma cultura de SEGDEF proativa e resiliente, alinhada com os objetivos da SCorpE e as normativas da FAB.

4.5 DIÁLOGO COM A TEORIA DA ESTRATÉGIA CORPORATIVA

A aplicação da SCorpE a um ativo de defesa se enriquece ao dialogar com teorias clássicas da estratégia corporativa, onde a segurança atua para garantir a vantagem competitiva.

O modelo das Cinco Forças Competitivas de Michael Porter (1979) analisa a rivalidade entre concorrentes, poder de barganha de fornecedores e compradores, ameaça de novos entrantes e de produtos substitutos. Uma SEGDEF robusta no CLA atua para mitigar essas forças: uma base segura reduz a ameaça de novos entrantes, aumenta o poder de barganha com clientes e fortalece a posição contra rivais.

O conceito de Cadeia de Valor (*Value Chain*) de Porter (1985) desagrega a organização em suas atividades para identificar fontes de vantagem competitiva. A Segurança da Gestão dos Processos (SGProc) de Mandarini complementa essa visão ao inserir a segurança como uma atividade de apoio transversal que protege cada elo da cadeia, especialmente a segurança da cadeia de suprimentos (*supply chain security*), um risco crescente no setor aeroespacial (Santos *et al.*, 2013).

Montgomery (2012) reforça que a estratégia deve ser uma responsabilidade central do líder, que é o estrategista principal. Essa visão alinha-se à necessidade de o Comandante do CLA e o Alto Comando da FAB assumirem a SEGDEF não como uma questão puramente tática, mas como um pilar da estratégia do Centro, essencial para a sustentação de sua vantagem competitiva e para o cumprimento de seu propósito estratégico.

4.5.1 A Teoria das Organizações de Alta Confiabilidade (HRO)

O CLA não é um ambiente corporativo convencional; é um sistema sociotécnico complexo onde uma falha pode ter consequências catastróficas, como a tragédia de 2003 demonstrou dolorosamente. Para analisar a dimensão da segurança operacional e cultural em tal ambiente, a Teoria das Organizações de Alta Confiabilidade (*High-Reliability Organizations* - HRO), desenvolvida por pesquisadores como Karl Weick e Kathleen Sutcliffe, é indispensável.

A teoria HRO foi concebida a partir do estudo de organizações que operam com sucesso em ambientes de risco extremo, como porta-aviões, controle de tráfego aéreo e usinas nucleares. Sua introdução no arcabouço teórico permite analisar o CLA não apenas sob a ótica da gestão de riscos, mas sob a ótica da criação de uma cultura de confiabilidade e do que Weick e Sutcliffe (2007) definem como “atenção plena coletiva” (*collective mindfulness*). Os cinco princípios da HRO são diretamente aplicáveis ao CLA:

Tabela 12 - Princípios das Organizações de Alta Confiabilidade (HRO).

Princípio	Descrição
Preocupação com a Falha	Uma vigilância crônica e constante, onde pequenas anomalias e quase-acidentes não são descartados, mas tratados como sintomas de potenciais falhas sistêmicas. Este princípio oferece uma lente poderosa para reexaminar as causas do acidente de 2003, que, segundo o relatório, envolveram a dificuldade em perceber a deterioração da segurança.
Relutância em Simplificar Interpretações	A prática de questionar pressupostos e buscar ativamente perspectivas diversas para compreender a complexidade das operações, evitando explicações simplistas que podem mascarar riscos profundos.
Sensibilidade às Operações	Manter uma consciência situacional aguçada e em tempo real sobre o que de fato acontece na linha de frente das operações, valorizando o conhecimento prático dos técnicos e operadores.
Compromisso com a Resiliência	A capacidade não apenas de prevenir falhas, mas de detectá-las, contê-las e se recuperar delas rapidamente, aprendendo e se fortalecendo no processo.
Deferência à Expertise	Em situações de crise ou anomalia, a autoridade decisória migra para a pessoa com o conhecimento mais relevante para resolver o problema, independentemente de sua posição hierárquica formal.

Fonte: Adaptado de Weick e Sutcliffe (2007).

A combinação da SCorpE com a teoria HRO cria um modelo analítico muito mais poderoso. A SCorpE fornece a estrutura para gerenciar a segurança, enquanto a HRO fornece a cultura e a mentalidade necessárias para que essa estrutura funcione sob alta pressão.

5 ANÁLISE E OTIMIZAÇÃO DA SEGURANÇA E DEFESA DO CLA: UM DIÁLOGO ENTRE ESTRATÉGIA, CULTURA E GEOPOLÍTICA

A Segurança e Defesa (SEGDEF) do Centro de Lançamento de Alcântara (CLA) se encontra, atualmente, em um dilema estratégico. Por um lado, sua indiscutível importância para a soberania nacional e para o Poder Aeroespacial Brasileiro é ampliada pelo Acordo de Salvaguardas Tecnológicas (AST), por outro lado, a complexidade operacional, as vulnerabilidades latentes e um ambiente de ameaças diversificadas demandam uma constante atualização de sua proteção. Como evidenciado por este estudo, a SEGDEF no CLA vai além da simples vigilância física; ela se estabelece como o componente essencial que assegura a capacidade do Brasil no setor espacial.

Para decifrar este desafio, uma única lente teórica não é suficiente. Assim, a análise atual propõe um modelo integrado que dialoga com três pontos de vista essenciais. A espinha dorsal metodológica é estabelecida pela Segurança Corporativa Estratégica (SCorPE), de Mandarini (2005). No entanto, a Teoria das Organizações de Alta Confiabilidade (HRO), de Weick e Sutcliffe (2007), aprofunda sua robustez, enquanto a dimensão geopolítica da Astropolitik, de Everett Dolman (2001), a contextualiza.

O modelo SCorPE de Mandarini (2005) fornece a arquitetura gerencial desta análise. Ao traduzir a missão de segurança em um sistema de gestão para prevenir “perdas”, ele permite desmembrar a proteção do CLA em seus componentes funcionais: a gestão de áreas e instalações (SGAI), de pessoas (SGP), de processos (SGProc) e do conhecimento (SGC). Esta abordagem oferece um método claro para o diagnóstico de vulnerabilidades. No entanto, o foco da SCorPE em processos e estruturas encontra seu complemento indispensável na dimensão humana e cultural.

É precisamente nesta lacuna entre o procedimento prescrito e a prática humana que a Teoria das Organizações de Alta Confiabilidade (HRO) se torna vital. Weick e Sutcliffe (2007) advertem que planos e normas são insuficientes em ambientes de altíssimo risco. O trágico acidente com o VLS-1 em 2003 é a dolorosa lição: o relatório, ao apontar a “dificuldade em identificar a deterioração da segurança”, revelou não apenas uma falha processual, mas uma fundamental falha de percepção e cultura. A ausência de uma “atenção plena coletiva” e de uma preocupação crônica com a falha – pilares da HRO – cria o terreno fértil para que riscos latentes evoluam até a catástrofe. A HRO oferece, assim, o alicerce cultural sem o qual a estrutura gerencial da SCorPE não se sustenta no ambiente operacional do CLA.

Se a HRO mergulha na cultura interna do CLA, a Astropolitik de Everett Dolman (2001) projeta a análise para o grande tabuleiro da geopolítica global. Ela responde à pergunta fundamental: por que a segurança de Alcântara é uma questão transcendental para o Brasil? Ao posicionar a Órbita Baixa Terrestre (LEO) como o “Heartland” estratégico do século XXI, Dolman revela as vantagens geográficas do CLA não como um mero diferencial competitivo, mas como a chave para um pivô de poder na arena espacial. A Astropolitik, portanto, redimensiona o conceito de “perdas estratégicas” de Mandarinini: uma falha de segurança no CLA deixa de ser um prejuízo operacional ou financeiro para se tornar um revés geopolítico que compromete a soberania e a projeção de poder do Brasil no mundo.

Em suma, esta integração teórica resulta em um modelo analítico multiescalar. A SCorpE de Mandarinini oferece o arcabouço metodológico para planejar, executar e controlar a segurança (o como fazer). A HRO de Weick e Sutcliffe estabelece o fundamento cultural de resiliência e atenção plena, essencial para que o sistema funcione sob a pressão de operações de alto risco (o como ser). Por fim, a Astropolitik de Dolman provê o imperativo estratégico que justifica e orienta todo o esforço de segurança, conectando-o à soberania nacional (o porquê fazer). A proposição de um Plano Diretor de Segurança Estratégica (PDSE) para o CLA, portanto, deve ser edificada sobre a união indissociável destes três pilares, garantindo uma proteção gerencialmente sólida, culturalmente resiliente e estrategicamente orientada.

5.1 PLANEJAMENTO ESTRATÉGICO DA SEGURANÇA NO AMBIENTE AEROESPACIAL

Em um ambiente de risco inerente e de importância estratégica como o Centro de Lançamento de Alcântara (CLA), a segurança não pode ser um conjunto de ações reativas e isoladas; ela deve e precisa ser o alicerce do planejamento. É neste ponto que a Segurança Corporativa Estratégica (SCorpE), conforme delineada por Mandarinini (2005), oferece o fundamento para essa transformação. É nesse momento que a Segurança Corporativa Estratégica (SCorpE), como descrita por Mandarinini (2005), fornece a base para essa mudança. Em vez de responder a incidentes de forma reativa, a SCorpE implementa um planejamento contínuo que precede, orienta e integra todas as ações de segurança, alinhando-as tanto aos objetivos institucionais da FAB quanto aos compromissos internacionais do Brasil. Dessa forma, o planejamento estratégico da SEGDEF se estabelece como a base para prever riscos, destinar recursos de maneira eficaz e assegurar a resiliência operacional do Centro.

Incorporar a perspectiva da SCorpE ao CLA implica considerar o planejamento da SEGDEF como um processo dinâmico, intimamente ligado aos objetivos estratégicos da FAB e do Programa Espacial Brasileiro (PEB). Este procedimento requer uma avaliação cuidadosa dos contextos interno e externo para desenvolver estratégias de redução de riscos e criar planos de ação pormenorizados. Mandarinini (2005, p. 68) enfatiza a relevância de que o planejamento estratégico em segurança leve em conta os diversos níveis organizacionais, uma abordagem que se adapta perfeitamente à estrutura da FAB e do CLA:

- a) **Nível Institucional (Estratégico):** No âmbito do Alto Comando da Aeronáutica e dos órgãos superiores (como o Estado-Maior da Aeronáutica – EMAER, e o Comando de Preparo – COMPREP, como órgão central do SISDE), são definidas as diretrizes gerais, a filosofia e a política de SEGDEF para todas as organizações militares, incluindo o CLA. Estas orientações de mais alto nível devem estar alinhadas à missão e visão da Força (DCA 11-45), aos objetivos do PEMAER (PCA 11-47), e refletidas em documentos normativos como a DCA 205-4 e a NSCA 205-3. É neste nível que se estabelece a prioridade estratégica do CLA e se alocam os recursos macro para sua SEGDEF.
- b) **Nível Departamental (Tático):** No âmbito do próprio CLA e dos comandos diretamente envolvidos em sua operação e segurança (como o Comando do CLA e o Grupo de Segurança e Defesa de Alcântara - GSD-AK), as diretrizes estratégicas são traduzidas em planos táticos específicos. Estes planos devem detalhar a aplicação da SEGDEF nas diferentes áreas (plataformas de lançamento, áreas de integração de satélites, laboratórios, perímetro), processos (preparação para lançamento, manuseio de tecnologia AST, transporte de materiais perigosos) e sistemas (segurança da informação, controle de acesso, vigilância eletrônica) do Centro. A elaboração do Plano de Segurança Orgânica e Defesa (PSOD) do CLA e dos Planos de Segurança das Instalações (PSI) específicos se enquadra neste nível.
- c) **Nível Executivo (Operacional):** Neste nível, os planos táticos são desdobrados em procedimentos operacionais padrão (POPs), ordens de serviço, instruções de trabalho e responsabilidades individuais e setoriais. É aqui que se define o “como fazer” da SEGDEF no dia a dia do CLA, detalhando as ações de vigilância, controle, resposta a incidentes e manutenção dos sistemas de segurança, sob a responsabilidade direta do GSD-AK e dos demais setores envolvidos.

A efetividade da SEGDEF no CLA depende, fundamentalmente, da integração entre esses três níveis de planejamento. A implementação eficaz das diretrizes do Comando da Aeronáutica no campo depende da articulação consistente entre os níveis estratégico, tático e operacional. De acordo com a NSCA 205-3, esse planejamento deve ser um ciclo contínuo de “planejamento – execução – avaliação – controle – atualização”, garantindo a adaptação às alterações no cenário de ameaças e nas demandas operacionais.

5.1.1 Proposta de Inclusão do Módulo de SEGDEF no Curso de Preparação para Operações de Lançamento (CPOL)

Um dos pilares para a consolidação de uma cultura de segurança robusta e proativa, conforme os preceitos da Segurança Corporativa Estratégica (SCorPE), é a Educação para Segurança. No contexto do Centro de Lançamento de Alcântara (CLA), uma oportunidade singular para a implementação deste pilar se apresenta por meio do Curso de Preparação para Operações de Lançamento (CPOL), ofertado pelo próprio CLA, conforme previsto na TCA 37-15 “Cursos do DCTA para o ano de 2025”.

Atualmente, o CPOL tem como finalidade capacitar o pessoal técnico para as atividades de lançamento e servir como curso de ambientação para todos os novos integrantes e parceiros do Centro. Sua estrutura contempla um módulo teórico (CPOL-I) e um módulo prático (CPOL-II), focados nos conceitos básicos do funcionamento dos diversos setores e estações do Centro de Lançamento de Alcântara durante a realização de seus lançamentos.

Apesar de sua importância, nota-se que o escopo atual do curso, conforme a normativa vigente, não contempla de forma explícita e aprofundada a dimensão da Segurança e Defesa, um componente crítico e indissociável da atividade de lançamento, especialmente considerando as vulnerabilidades do CLA e os requisitos do Acordo de Salvaguardas Tecnológicas (AST).

Dessa forma, como parte integrante do Plano Diretor de Segurança Estratégica (PDSE) aqui proposto, recomenda-se a criação e implementação de um Módulo de Segurança e Defesa (SEGDEF) obrigatório dentro da estrutura curricular do CPOL-I. Este módulo teria como objetivos:

- I. **Conectar a SEGDEF ao Poder Aeroespacial:** Apresentar aos alunos a concepção de que a SEGDEF não é um mero serviço de apoio, mas um elemento constitutivo e habilitador do Poder Aeroespacial, alinhado à Concepção Estratégica Força Aérea 100 (DCA 11-45) e ao Plano Estratégico Militar da Aeronáutica (PCA 11-47).

- II. **Disseminar a Mentalidade de Prevenção de Perdas:** Introduzir os fundamentos da SCorpE, com foco na identificação de riscos e na prevenção de “perdas” estratégicas, operacionais, de conhecimento e de recursos, conforme a abordagem de Mandarini (2005).
- III. **Apresentar as Ameaças Específicas ao CLA:** Instruir todos os participantes sobre as ameaças específicas ao Centro, incluindo espionagem, sabotagem, ciberataques e os riscos associados ao vazamento de tecnologias protegidas pelo AST.
- IV. **Promover a Responsabilidade Individual:** Enfatizar que a segurança é uma responsabilidade de todos, instruindo sobre a importância de condutas seguras no manuseio de informações, no controle de acesso, na comunicação e no reporte de atividades suspeitas ou anômalas.
- V. **Integrar a SEGDEF às Operações:** Demonstrar, na prática, como os procedimentos do SISI e do PDSE se integram à rotina operacional do lançamento, desde o planejamento até a execução.

A inclusão deste módulo no CPOl garantirá que todo profissional, militar ou civil, nacional ou estrangeiro, que venha a atuar nas operações do CLA, receba, desde o início de suas atividades, a capacitação necessária para compreender e internalizar a cultura de segurança estratégica. Esta medida transformaria o curso em uma poderosa ferramenta para a efetivação do PDSE, mitigando proativamente os riscos associados ao fator humano e fortalecendo a SEGDEF do CLA em todas as suas dimensões.

5.1.2 Planejamento de Contingências e Gerenciamento de Crises no CLA

O desenvolvimento e a manutenção de um sólido sistema de Planejamento de Contingências e Gerenciamento de Crises são essenciais e inseparáveis do planejamento estratégico da SEGDEF no CLA. Mandarini (2005, p. 58) destaca a importância fundamental do “Plano de Contingência Geral (PCG)”, um documento que deve ser abrangente, multidisciplinar e dinâmico, incluindo a prevenção, a preparação, a resposta e a recuperação de diversas situações de crise que possam afetar a organização, seus ativos, seu pessoal ou sua reputação. Dessa forma, Os “4 R's” da gestão de crises - Redução (mitigação de riscos e prevenção), Resposta (ações eficazes durante a crise), Recuperação (restauração da normalidade e das capacidades essenciais o mais rápido possível) e Resiliência (capacidade de

aprendizado e adaptação para fortalecer a organização contra futuras crises) - são princípios essenciais que devem guiar esse planejamento no CLA.

No contexto singular do Centro de Lançamento de Alcântara, o planejamento de contingências deve antever e preparar respostas para um espectro amplo e complexo de cenários adversos, tais como:

- I. **Acidentes Operacionais Graves:** Falha de um veículo lançador na plataforma ou durante a fase inicial do voo, com potencial para explosões, dispersão de propelentes tóxicos, queda de destroços em áreas povoadas ou ambientalmente sensíveis, resultando em perdas humanas, danos materiais extensos e contaminação ambiental.
- II. **Incidentes com Tecnologia Protegida pelo AST:** Comprometimento, dano ou destruição de componentes, veículos ou cargas úteis de origem norte-americana, exigindo protocolos de resposta específicos e comunicação coordenada com as autoridades dos EUA, conforme o Acordo de Salvaguardas.
- III. **Falhas Críticas em Sistemas Essenciais:** Interrupção prolongada dos sistemas de rastreio, telemetria e comando (RTC), sistemas de segurança de voo (destruição em voo), fornecimento de energia elétrica, ou redes de comunicação e dados, comprometendo a segurança ou a viabilidade de uma operação de lançamento.
- IV. **Desastres Naturais e Eventos Climáticos Extremos:** Considerando a localização costeira do CLA, é preciso prever o impacto de tempestades severas, inundações, descargas atmosféricas ou outros fenômenos que possam danificar instalações ou interromper operações.
- V. **Incidentes Graves de Segurança Física:** Tentativas de intrusão hostil em áreas críticas, atos de sabotagem contra infraestruturas ou equipamentos vitais, ataques terroristas, ou mesmo protestos violentos que ameacem a integridade do Centro e de seu pessoal.
- VI. **Ciberataques Significativos:** Tentativas de invasão ou disrupção dos sistemas de comando e controle de lançamento, redes de dados operacionais, sistemas de segurança eletrônica, ou roubo de informações classificadas (nacionais ou AST) por meios cibernéticos.
- VII. **Emergências Médicas e de Saúde Pública:** Incidentes envolvendo múltiplas vítimas (acidentes) ou surtos de doenças que possam afetar a capacidade operacional do efetivo.

A existência de planos de contingência detalhados, específicos para cada tipo de cenário, e integrados em um PCG para o CLA, é crucial. Estes planos devem definir claramente: cadeias de comando e responsabilidade em crise; protocolos de alerta e comunicação interna e externa (incluindo com Defesa Civil, Bombeiros, órgãos ambientais, Marinha, Exército e autoridades parceiras do AST); procedimentos de evacuação de áreas de risco; equipes de primeira resposta e suas atribuições; recursos materiais e logísticos necessários; e estratégias para a continuidade das operações essenciais ou para a sua rápida recuperação.

A eficácia desses planos depende de sua divulgação para o pessoal pertinente, de treinamentos regulares e de simulações realísticas, que permitam identificar falhas e aprimorar a capacidade de resposta da SEGDEF e de toda a organização do CLA. Tal preparação é essencial para minimizar as “perdas” decorrentes de eventos inesperados e para garantir a rápida restauração da normalidade, protegendo a vida, o patrimônio, o meio ambiente, a reputação da FAB e a continuidade das atividades estratégicas do Brasil no espaço.

5.1.3 Modularidade e Faseamento na Implementação da Segurança Estratégica no CLA

A implementação de um sistema de SEGDEF abrangente e otimizado para o Centro de Lançamento de Alcântara, dada sua complexidade, dimensão territorial e a diversidade de riscos a serem gerenciados, pode se beneficiar significativamente de uma abordagem que empregue a Modularidade do Planejamento e o Faseamento dos Trabalhos, conceitos apresentados por Mandarinini (2005, p. 71-72) como ferramentas para a gestão eficaz de projetos de segurança de grande envergadura.

A Modularidade do Planejamento permite que o sistema de SEGDEF do CLA seja concebido e implementado em componentes ou módulos interconectados, mas que podem ser desenvolvidos e implantados em etapas. Cada módulo pode focar em um aspecto específico da segurança (ex: segurança perimetral da área principal, segurança das plataformas de lançamento, sistema de controle de acesso para áreas AST, cibersegurança das redes operacionais, plano de contingência para acidentes com propelentes).

Esta abordagem permite priorizar a implementação de módulos para as áreas ou processos de maior risco ou criticidade – como aquelas diretamente impactadas pelo Acordo de Salvaguardas Tecnológicas ou os componentes vitais para os projetos do PESE – sem, contudo, perder a visão do sistema de segurança integrado e coeso que se deseja alcançar.

O Faseamento dos Trabalhos, por sua vez, complementa a modularidade ao estabelecer um cronograma realista e exequível para a pesquisa, desenvolvimento, aquisição, instalação,

teste e entrada em operação de cada módulo ou fase do planejamento de SEGDEF. Este faseamento deve considerar as restrições orçamentárias, a disponibilidade de recursos humanos e tecnológicos, as interdependências entre os diferentes módulos, e as janelas de oportunidade (ou restrição) impostas pelo cronograma de operações de lançamento do CLA. A implementação faseada facilita a gestão dos recursos, permite a incorporação de lições aprendidas de fases anteriores, possibilita ajustes no planejamento com base em avaliações parciais de eficácia e garante que os aprimoramentos na SEGDEF sejam alcançados de forma progressiva, controlada e sustentável.

Para o CLA, uma abordagem modular e faseada poderia significar, por exemplo:

- I. **Fase 1 (Diagnóstico e Priorização):** Realização de uma análise de riscos completa e detalhada (conforme será discutido na seção 5.2), identificação dos ativos mais críticos e das vulnerabilidades mais urgentes. Elaboração do Plano Diretor de Segurança Estratégica (PDSE) definindo a arquitetura geral e os módulos prioritários.
- II. **Fase 2 (Implementação dos Módulos Críticos):** Foco na implementação das medidas de segurança mais urgentes, como o reforço da segurança física e eletrônica das áreas diretamente relacionadas ao AST, a modernização do controle de acesso a informações e tecnologias sensíveis, e o fortalecimento das capacidades iniciais de resposta a crises.
- III. **Fases Subsequentes:** Expansão gradual do escopo para outras áreas e processos do Centro, implementação de tecnologias mais avançadas de vigilância e C2 de segurança, desenvolvimento de programas de treinamento e cultura de segurança mais abrangentes, e aprimoramento contínuo dos módulos já implantados, sempre com foco na melhoria contínua e na adaptação às novas ameaças e necessidades operacionais.

Esta abordagem pragmática e estruturada permite que a FAB avance na otimização da SEGDEF do CLA de forma planejada, gerenciável e alinhada com suas capacidades e prioridades estratégicas.

5.2 GESTÃO DE RISCOS NA SEGURANÇA E DEFESA DO CLA

A gestão de riscos é o cerne da Segurança Corporativa Estratégica e, consequentemente, da otimização da Segurança Orgânica. Mandarini (2005, p. 38) define a gestão de riscos como o processo de “identificar, analisar, avaliar, tratar e monitorar os riscos” que podem afetar os objetivos da organização.

No CLA, onde os riscos são inerentemente elevados e multifacetados – abrangendo desde riscos tecnológicos e operacionais até riscos de segurança física, cibernética e de imagem, uma gestão de riscos sistemática, proativa e documentada é indispensável para a tomada de decisão e a alocação eficaz de recursos de segurança. Este processo, conforme preconizado tanto pela SCorpE quanto implicitamente pelas normativas da FAB que exigem a análise de vulnerabilidades e ameaças para o planejamento da SEGDEF (DCA 205-4; NSCA 205-3), deve ser um ciclo contínuo e adaptativo.

5.2.1 Identificação, Análise e Avaliação de Riscos e Ameaças (Diagnóstico) no Contexto do CLA

O processo de gestão de riscos no CLA deve iniciar com um diagnóstico abrangente e contínuo, que contemple:

- I. **Identificação de Ativos Críticos:** Mapear detalhadamente todos os ativos tangíveis (plataformas de lançamento, veículos lançadores, satélites, laboratórios, sistemas de controle, tecnologia protegida pelo AST) e intangíveis (informações de projeto, dados de telemetria, planos de voo, conhecimento técnico do pessoal, reputação da FAB e do programa espacial) essenciais para as operações do CLA. Este mapeamento deve ser exaustivo e dinâmico, reconhecendo que o valor e a criticidade dos ativos podem mudar com a evolução dos projetos do PEB e dos acordos internacionais como o AST. A SCorpE preconiza a proteção de ativos tangíveis e intangíveis, sendo estes últimos, como o conhecimento e a reputação, de valor imensurável e central para a missão do CLA.
- II. **Identificação de Ameaças Específicas ao CLA:** Além das ameaças genéricas, identificar aquelas particulares ao contexto de Alcântara e às operações espaciais: espionagem industrial ou estatal visando tecnologias específicas, sabotagem de infraestruturas ou durante operações de lançamento, ciberataques direcionados aos sistemas de comando e controle, intrusões para furto de material ou coleta de informações, riscos decorrentes da proximidade de comunidades e de atividades ilícitas na região, e os riscos inerentes às próprias operações de lançamento (falhas de componentes, condições meteorológicas adversas, erro humano). A análise deve cobrir os “Riscos Não-Empresariais” e os “Riscos Empresariais” (Mandarini, 2005, p. 33-35). A identificação de ameaças deve ser alimentada continuamente pela atividade de

Inteligência de Segurança (conforme detalhado na seção 5.3) e considerar não apenas as ameaças diretas, mas também aquelas que podem surgir de instabilidades regionais, atores não-estatais com capacidades assimétricas, e a constante evolução das táticas de espionagem e ciberataque. A DCA 205-4 alerta para a necessidade de se preparar para ações de qualquer natureza que constituam ameaça. Modesto e Neves (2025), por exemplo, destacam o crescimento urbano desordenado no entorno dos quartéis e, principalmente, a utilização de drones para espionagem das instalações militares como novas e significativas ameaças que exigem estratégias modernas de controle do espaço aéreo de baixa altitude e de contrainteligência.

- III. **Identificação de Vulnerabilidades do CLA:** Com base nas auditorias, inspeções e na análise do Capítulo 4, detalhar as fragilidades específicas do CLA (perímetro, controle de acesso, segurança da informação, capacitação de pessoal, dependência de sistemas) que poderiam ser exploradas pelas ameaças. A identificação de vulnerabilidades deve ser um processo introspectivo e crítico, utilizando auditorias regulares de segurança, testes de penetração (físicos e lógicos), análise de incidentes anteriores (mesmo os de menor impacto) e feedback do pessoal que opera no dia a dia. Conforme Mandarini (2005), o reconhecimento das próprias fragilidades é o primeiro passo para uma segurança eficaz.
- IV. **Análise de Riscos (Probabilidade e Impacto):** Para cada cenário de risco (combinação de ativo, ameaça e vulnerabilidade), analisar a probabilidade de ocorrência e o impacto potencial, considerando as diversas dimensões de “perdas” discutidas por Mandarini (2005) – financeiras, operacionais, humanas, de imagem, de oportunidade, etc. A avaliação do impacto, crucial no CLA, deve ser multidimensional, quantificando não apenas perdas financeiras diretas, mas também os impactos estratégicos para a FAB (como a preservação do poder combatente), para o PEB (atrasos, perda de tecnologia), para a credibilidade internacional do Brasil (especialmente no contexto do AST), e para a segurança nacional. Esta análise deve considerar a interdependência dos sistemas, onde a falha em um componente pode ter efeitos cascata.
- V. **Avaliação e Priorização de Riscos:** Utilizar uma Matriz de Riscos para classificar os riscos (ex: baixo, médio, alto, crítico) e definir as prioridades para tratamento, focando naqueles que apresentam maior potencial de dano aos objetivos estratégicos da FAB e do CLA. A Matriz de Riscos utilizada deve ser adaptada às especificidades do CLA, incorporando critérios alinhados com a importância relativa e vulnerabilidade relativa preconizadas pela DCA 205-4. A priorização deve resultar em um plano de ação claro,

direcionando os recursos limitados para os riscos que representam a maior ameaça à missão e aos objetivos estratégicos. Este processo de avaliação deve ser formalizado e revisado periodicamente pela cadeia de comando responsável pelo CLA e pela SEGDEF, conforme as diretrizes do SISDE. A criticidade deste diagnóstico é amplamente reconhecida na doutrina de segurança institucional. Caron e Bueno (2019, p. 88), por exemplo, alertam que “a adoção de medidas de segurança sem a necessária análise dos riscos e dos aspectos envolvidos poderá causar o comprometimento, decorrente de sua insuficiência ou inadequação”.

5.2.2 Tratamento e Monitoramento Contínuo de Riscos no CLA

As estratégias de tratamento dos riscos identificados e avaliados no CLA devem ser selecionadas com base na sua eficácia e viabilidade. Essas estratégias, conforme preconizado pela SCorpE e pelas boas práticas em gestão de riscos, devem ser documentadas nos Planos de Segurança das Instalações (PSI) e no Plano de Segurança Orgânica e Defesa (PSOD) do Centro, conforme estabelecido pela NSCA 205-3/2024, e compreendem:

- I. **Reduzir o Risco:** É a principal estratégia, implementando ou aprimorando os controles de Segurança Orgânica (físicos, lógicos, procedimentais, humanos) para diminuir a probabilidade ou o impacto dos riscos. As propostas deste projeto visam, em grande medida, a redução dos riscos. Esta redução é alcançada através da implementação de um conjunto integrado de contramedidas, que podem incluir o fortalecimento da Segurança da Gestão das Áreas e Instalações (SGAI) com barreiras físicas e tecnológicas, o aprimoramento da Segurança da Gestão das Pessoas (SGP) por meio de treinamento e controles mais rigorosos, a otimização da Segurança da Gestão dos Processos (SGProc) para minimizar falhas operacionais, e o robustecimento da Segurança da Gestão do Conhecimento (SGC) para proteger informações sensíveis. A implementação do Suporte Integrado de Segurança das Instalações (SISI), conforme a DCA 205-9, é um exemplo de estratégia abrangente para a redução de riscos no CLA.
- II. **Evitar o Risco:** Em alguns casos, pode ser necessário modificar processos, descontinuar atividades de altíssimo risco não mitigável ou reavaliar parcerias que imponham riscos desproporcionais.
- III. **Transferir o Risco:** Explorar mecanismos como seguros para certos tipos de perdas materiais ou financeiras, ou cláusulas contratuais em parcerias que delimitem

responsabilidades (lembrando que a responsabilidade estatal primária permanece).

- IV. **Aceitar o Risco:** Riscos de baixo impacto e baixa probabilidade podem ser aceitos, desde que formalmente documentados e monitorados pela gestão do CLA e órgãos superiores da FAB. O tratamento dos riscos no CLA deve ser um processo dinâmico, integrado ao planejamento estratégico e orçamentário. As medidas de segurança implementadas devem ser objeto de auditorias e monitoramento contínuos para verificar sua eficácia e adequação frente à evolução das ameaças e das operações do Centro. Este monitoramento não deve ser apenas reativo, mas proativo, buscando identificar novas ameaças e vulnerabilidades antes que se materializem em incidentes. A NSCA 205-3/2024 preconiza um ciclo criterioso e contínuo de planejamento execução avaliação e controle - atualização para a SEGDEF, o que implica a revisão periódica e a atualização dos PSI's e do PSOD do CLA.

A Educação para Segurança, como destaca Mandarinini (2005, p. 73-74), é fundamental para este processo, pois um efetivo consciente e treinado é a primeira linha de defesa e um componente essencial para o monitoramento e reporte de anomalias, contribuindo para a mentalidade coletiva de segurança almejada pela DCA 205-4.

5.3 A ATIVIDADE DE INTELIGÊNCIA NO APOIO À SEGURANÇA E DEFESA DO CLA

A atividade de Inteligência, no contexto da SEGDEF do CLA, é a espinha dorsal da Segurança da Gestão do Conhecimento (SGC), conforme conceituada por Mandarinini (2005, p. 201-209). Não se trata apenas de uma função de apoio, mas de um processo proativo e contínuo que visa salvaguardar esse ativo vital que é o conhecimento estratégico, operacional e tecnológico do Centro.

A produção de Inteligência de Segurança deve seguir um ciclo metodológico, desde o planejamento das necessidades de conhecimento (orientadas pelos riscos e objetivos da SEGDEF), passando pela coleta e busca de dados (de fontes abertas e, quando legalmente amparado, de fontes protegidas), sua análise e integração, até a difusão de conhecimento acionável para os tomadores de decisão no CLA e na cadeia de comando da SEGDEF.

A Contrainteligência, por sua vez, atua como o escudo protetor desses ativos informacionais e do próprio processo de inteligência. No CLA, isso significa um esforço constante para:

- I. **Proteger o Conhecimento Sensível:** Implementar e fiscalizar rigorosamente os

protocolos de classificação, manuseio, armazenamento e descarte de informações sigilosas, especialmente aquelas relacionadas a projetos estratégicos do PEB, tecnologias do AST e planos de segurança. Isso se alinha diretamente à salvaguarda do conhecimento como pilar da SCorPE.

- II. **Neutralizar Ações de Inteligência Adversa:** Identificar, avaliar e neutralizar tentativas de espionagem, vigilância hostil, cooptação de pessoal ou qualquer outra ação de inteligência que vise comprometer a segurança do CLA, suas operações ou seus segredos.
- III. **Assegurar a Segurança das Comunicações e Sistemas:** Trabalhar em conjunto com os especialistas em Tecnologia da Informação para proteger as redes de dados, os sistemas de comando e controle e os canais de comunicação contra interceptação, intrusão ou manipulação.

A integração da atividade de Inteligência do CLA com o Sistema de Inteligência da Aeronáutica (SINTAER), conforme preconizado pela NSCA 205-3, e, mais amplamente, com o Sistema Brasileiro de Inteligência (SISBIN), é fundamental para garantir o fluxo de informações relevantes e a coordenação de esforços contra ameaças que transcendam a capacidade de análise local.

5.4 O SUPORTE INTEGRADO DE SEGURANÇA DAS INSTALAÇÕES (SISI) COMO MODELO NORMATIVO PARA A MODERNIZAÇÃO DA SEGDEF NO CLA

A otimização da Segurança e Defesa (SEGDEF) no Centro de Lançamento de Alcântara (CLA), para além da aplicação dos princípios da Segurança Corporativa Estratégica e da robusta gestão de riscos e inteligência, encontra um importante direcionamento normativo e prático nos recentes desenvolvimentos doutrinários da Força Aérea Brasileira (FAB). A Diretriz do Comando da Aeronáutica DCA 205-9, que institui a Implantação do Suporte Integrado de Segurança das Instalações nas Organizações Militares do COMAER (SISI), oferece um modelo de modernização essencial para as complexas necessidades do CLA.

O Suporte Integrado de Segurança das Instalações (SISI), conforme detalhado na DCA 205-9, é concebido como:

A integração da infraestrutura de Segurança das Instalações com os meios de Segurança Eletrônica, no tocante à vigilância, ao controle de acesso e à detecção de intrusão, todos interligados, por meio de um sistema eficiente de comando e controle

e de inteligência, a equipes de pronta resposta (Equipes de Reação), compostas por pessoal especializado e dotado de meios de proteção balística, mobilidade e capacidade de uso progressivo e proporcional da força. (Brasil, 2020, p.8)

Este modelo normativo visa a elevar o padrão de segurança das instalações da FAB, sendo sua aplicação no CLA não apenas pertinente, mas fundamental para enfrentar os desafios contemporâneos.

A relevância do SISI para o CLA é evidenciada por sua consonância com as orientações estratégicas de modernização. O Plano Estratégico Militar da Aeronáutica (PCA 11-47) já aponta para a necessidade de revisão do modelo de Segurança das Instalações, considerando o emprego de novas tecnologias de vigilância eletrônica, controle de acesso e detecção de intrusão e a adoção de forças de reação rápida. O SISI, portanto, materializa essa visão, propondo uma arquitetura de segurança que se baseia na sinergia de múltiplos componentes:

- I. **Infraestrutura de Segurança Física Resiliente:** Adequação e fortalecimento contínuo das barreiras perimetrais, guaritas, sistemas de iluminação e proteção física das edificações, conforme a análise de vulnerabilidades específica de cada OM.
- II. **Segurança Eletrônica Avançada e Integrada:** Implementação de um conjunto de tecnologias como CFTV com capacidade analítica, sensores de intrusão (perimetrais e internos), e sistemas de controle de acesso modernos e padronizados, como o Software de Controle de Acesso e Informações (SCAI), cuja implantação é coordenada pela DTI.
- III. **Comando e Controle (C2) de Segurança Centralizado:** A interligação de todos os meios de segurança eletrônica a um sistema eficiente de C2 permite uma consciência situacional aprimorada e a coordenação eficaz das ações de segurança.
- IV. **Inteligência como Suporte Decisório:** O SISI reconhece a inteligência como um componente vital, fornecendo subsídios para a análise de ameaças e a orientação das equipes de segurança.
- V. **Equipes de Pronta Resposta (Equipes de Reação) Especializadas:** O modelo SISI enfatiza a necessidade de Equipes de Reação compostas por pessoal especializado (Infantaria da Aeronáutica), com mobilidade e capacidade de uso progressivo e proporcional da força, para uma resposta rápida e eficaz a incidentes.

A DCA 205-9 estabelece que a implantação do SISI se dará por meio de um Projeto SISI, específico para cada OM, a ser elaborado e acompanhado por uma Comissão de

Implantação multidisciplinar, composta por representantes das áreas de Segurança e Defesa, Inteligência, TI, Infraestrutura, Logística e Administração, entre outras.

Para o CLA, a elaboração deste Projeto SISI deverá considerar não apenas as especificidades das áreas e edificações a serem protegidas, mas também os rigorosos requisitos impostos pelo Acordo de Salvaguardas Tecnológicas (AST) e a necessidade de proteger tecnologias e informações de valor estratégico para o Programa Espacial Brasileiro. A diretriz também orienta a adequada previsão e provisão de recursos financeiros e o faseamento da implantação, aspectos cruciais dada a magnitude dos investimentos necessários para o CLA.

A adoção do SISI como modelo para o CLA representa, assim, um caminho normativo e prático para a modernização e otimização da sua SEGDEF, alinhando o Centro com as mais recentes diretrizes da FAB para a segurança de suas instalações estratégicas.

5.5 PROPOSTA DE UM PLANO DIRETOR DE SEGURANÇA ESTRATÉGICA (PDSE) PARA O CLA: CONSOLIDANDO A OTIMIZAÇÃO DA SEGDEF

Com base na análise dos fundamentos da Segurança Corporativa Estratégica (SCorpE) e das demais doutrinas de segurança, na avaliação dos riscos inerentes ao CLA, no papel crucial da atividade de inteligência e no modelo SISI, torna-se evidente a necessidade de um instrumento que consolide e direcione estrategicamente todos esses elementos. Propõe-se, assim, a elaboração de um Plano Diretor de Segurança Estratégica (PDSE) específico para o Centro de Lançamento de Alcântara.

A elaboração de um plano dessa natureza, precedido por uma criteriosa análise de riscos, alinha-se às melhores práticas de segurança institucional. Conforme alertam Caron e Bueno (2019, p. 88), “a adoção de medidas de segurança sem a necessária análise dos riscos e dos aspectos envolvidos poderá causar o comprometimento, decorrente de sua insuficiência ou inadequação”. A estruturação do PDSE pode, portanto, inspirar-se em modelos já implementados com sucesso no setor público brasileiro. A própria

Resolução CNMP nº 156, de 13 de dezembro de 2016, que instituiu a Política de Segurança Institucional do Ministério Público, serve como um referencial robusto (Dalabrida, 2019). Essa normativa prevê a edição de um plano de Segurança Institucional e de planos de segurança orgânica, detalhando a composição desta última em segurança de pessoas, do material, das áreas e instalações e da informação, oferecendo uma estrutura lógica e abrangente que pode ser adaptada à realidade do CLA (Conselho Nacional do Ministério Público, 2019).

Vale ressaltar que as diretrizes e a estrutura fundamental deste PDSE, aqui delineadas, serão consolidadas e apresentadas como uma proposta de Manual de Segurança e Defesa para o Centro de Lançamento de Alcântara, constituindo o produto técnico-tecnológico desta dissertação, em consonância com as orientações para trabalhos acadêmicos da Universidade da Força Aérea (UNIFA).

O Plano Diretor de Segurança Estratégica (PDSE) para o CLA deve ser concebido como um instrumento dinâmico e abrangente, formalizado em documento normativo de alto nível (possivelmente uma Norma de Sistema do Comando da Aeronáutica - NSCA - específica ou um Plano do COMAER dedicado), que estabeleça a arquitetura, as diretrizes e os mecanismos de gestão da SEGDEF para o Centro. Sua elaboração deve ser um esforço multidisciplinar, envolvendo especialistas em segurança e defesa, e representantes das áreas operacional, técnica, de inteligência, de infraestrutura, jurídica e de relações institucionais do CLA e de outros órgãos da FAB.

Os elementos essenciais de um PDSE para o CLA, fundamentado nos princípios da SCorpE de Mandarini (2005) e nas normativas da FAB. Sua elaboração deve ser um esforço multidisciplinar, envolvendo não apenas especialistas em segurança e defesa, mas também representantes das áreas operacional, técnica, de inteligência, de infraestrutura, jurídica e de relações institucionais do CLA e de outros órgãos da FAB com interface com o Centro.

Um PDSE robusto para o CLA deve, primordialmente, assentar-se sobre uma Filosofia e Política de Segurança Estratégica claramente articulada. Isso implica uma declaração formal da filosofia que norteará todas as ações de SEGDEF, consagrando a segurança como um valor institucional intrínseco, uma responsabilidade compartilhada por todos os níveis e um elemento indissociável da missão do CLA. Derivada dessa filosofia, a Política de Segurança Estratégica do CLA detalharia os objetivos de longo prazo da SEGDEF, seu alinhamento explícito com os documentos magnos da Força, como a DCA 11-45 e o PCA 11-47, e os compromissos inequívocos com a proteção de ativos nacionais e de parceiros internacionais, conforme estipulado no Acordo de Salvaguardas Tecnológicas (AST).

A efetividade do PDSE dependerá de uma Estrutura de Governança da SEGDEF no CLA bem definida. Esta estrutura deve delinear a organização hierárquica e funcional da SEGDEF no Centro, especificando os papéis, responsabilidades e níveis de autoridade desde o Comando do CLA até o Grupo de Segurança e Defesa de Alcântara (GSD-AK) e os demais setores com interface de segurança. Recomenda-se, ainda, o estabelecimento de comitês ou conselhos de segurança multidisciplinares, com participação de diferentes áreas do CLA e,

quando pertinente, de órgãos externos, para fins de assessoramento estratégico, tomada de decisão colegiada em assuntos críticos e coordenação interagências.

No cerne do PDSE, deve estar uma Metodologia de Gestão de Riscos Contínua e Integrada. Conforme detalhado na seção 5.2, esta metodologia deve formalizar o ciclo de identificação, análise, avaliação, tratamento e monitoramento de riscos como o processo dinâmico que alimenta e direciona todas as ações de SEGDEF. É crucial o estabelecimento de critérios de risco e níveis de tolerância customizados para a realidade operacional e estratégica do CLA, levando em consideração os requisitos específicos do AST.

O PDSE deve traduzir essa gestão de riscos em Diretrizes Estratégicas para os Segmentos da Segurança Corporativa Estratégica (SCorpE) aplicados ao CLA.

Para a SGAI (Segurança da Gestão das Áreas e Instalações), o plano detalhará a aplicação da Teoria dos Círculos Concêntricos para a defesa em profundidade de todas as áreas do CLA. Isso inclui o estabelecimento de padrões rigorosos para a segurança física (barreiras, edificações seguras, iluminação de proteção) e para a segurança eletrônica (sistemas integrados de vigilância, detecção de intrusão, controle de acesso biométrico e por múltiplos fatores), com especificações claras e adaptadas para áreas AST e outras zonas de alta sensibilidade ou periculosidade.

No âmbito da SGP (Segurança da Gestão das Pessoas), o PDSE estabelecerá políticas e procedimentos para recrutamento seguro, investigações de antecedentes aprofundadas, sistemas de credenciamento diferenciados e dinâmicos, programas contínuos e adaptados de educação para segurança, e mecanismos de monitoramento comportamental para todo o pessoal (militar, civil, terceirizado e estrangeiro) com acesso ao CLA, com atenção especial aos requisitos do AST.

A SGProc (Segurança da Gestão dos Processos) será contemplada com medidas de segurança integradas aos processos críticos do CLA. Isso envolve a SOp (Segurança das Operações), com análise de criticidade e controles para cada fase das operações de lançamento; a SPLj (Segurança do Planejamento), com mecanismos para proteger o planejamento de missões e o desenvolvimento tecnológico, assegurando confidencialidade e compartimentação; e a SInsu (Segurança dos Insumos), com protocolos para o ciclo de vida seguro de todos os insumos estratégicos, perigosos ou classificados, incluindo Planos de Gerenciamento de Riscos (PGR) para o transporte de cargas críticas.

Para a SGC (Segurança da Gestão do Conhecimento), o PDSE definirá diretrizes para a classificação da informação, a proteção de dados estratégicos do PEB e tecnologias AST, a

segurança robusta das comunicações (incluindo telemetria e telecomando) e uma arquitetura de cibersegurança em camadas para todas as redes e sistemas de informação do CLA.

Um componente essencial do PDSE será a Implementação e Integração do Modelo SISI (Suporte Integrado de Segurança das Instalações). O plano detalhará como os componentes do SISI, conforme preconizado pela DCA 205-9 – infraestrutura física, meios eletrônicos, C2 de segurança, inteligência de apoio e Equipes de Reação – serão implementados, integrados e mantidos para constituir a espinha dorsal da SEGDEF física e tecnológica do CLA.

O PDSE também deverá incorporar e referenciar Planos de Contingência e Gerenciamento de Crises detalhados, como o Plano de Contingência Geral (PCG) do CLA e seus planos específicos para diferentes cenários. Estes devem prever estruturas de resposta claras, cadeias de comando para situações de crise, e protocolos eficazes de comunicação e cooperação com órgãos de resposta externos e parceiros do AST.

Fundamental para a sustentabilidade do PDSE será um robusto Programa de Cultura e Educação para Segurança e Defesa. Este programa utilizará estratégias de endomarketing e um currículo formal e contínuo de Educação para Segurança para consolidar uma cultura de SEGDEF proativa, onde a segurança é percebida como responsabilidade de cada indivíduo no CLA.

Finalmente, o PDSE deve instituir Mecanismos de Gestão, Auditoria e Melhoria Contínua. Isso inclui a definição de Indicadores Chave de Desempenho (KPIs) para a SEGDEF, o estabelecimento de um ciclo regular de auditorias de segurança (internas e externas), a análise sistemática de incidentes e lições aprendidas, e processos formais para a revisão e atualização periódica do próprio PDSE. Tais mecanismos são vitais para assegurar a relevância, eficácia e adaptação contínua do plano frente à evolução das ameaças, das tecnologias e dos objetivos estratégicos do CLA e da FAB.

A implementação de um PDSE com estas características no CLA representaria um passo fundamental para a otimização da SEGDEF, transformando-a em um sistema integrado, estratégico e proativo, capaz de proteger eficazmente este ativo vital para o Poder Aeroespacial Brasileiro e para os compromissos internacionais assumidos pelo país.

6 CONCLUSÃO

O crescente protagonismo do domínio aeroespacial para os interesses estratégicos das nações e a consolidação do Centro de Lançamento de Alcântara (CLA) como um ativo vital para o Programa Espacial Brasileiro (PEB) e para a inserção do Brasil no mercado global de lançamentos, especialmente após a ratificação do Acordo de Salvaguardas Tecnológicas (AST), evidenciaram a necessidade premente de uma Segurança e Defesa (SEGDEF) robusta, estratégica e otimizada. A complexidade das operações, o valor dos ativos envolvidos e os rigorosos requisitos de segurança impostos por parceiros internacionais demandam uma abordagem que transcenda a proteção física tradicional, integrando-se plenamente ao planejamento e à execução do Poder Aeroespacial.

Nessa perspectiva, surgiu o problema de pesquisa deste trabalho: “De que forma a Segurança e Defesa (SEGDEF) do Centro de Lançamento de Alcântara (CLA), quando otimizada pelos preceitos da Segurança Corporativa Estratégica, pode consolidar o Poder Aeroespacial Brasileiro e fortalecer a soberania nacional?”

Assim, para que a resposta ao problema de pesquisa fosse encontrada, o Objetivo Geral foi definido: avaliar a SEGDEF no CLA para sugerir um modelo de otimização estratégica que aumente a proteção, resiliência e capacidade operacional. Isso deve estar em conformidade com o Poder Aeroespacial Brasileiro, com as diretrizes do COMAER e com os princípios da Segurança Corporativa Estratégica (SCorPE), adaptados ao contexto militar e às particularidades do COMAER.

Nesta senda, o caminho foi percorrido com o auxílio de quatro Objetivos Específicos (OE) que foram assim definidos: 1) Descrever o Centro de Lançamento de Alcântara, sua importância estratégica no contexto do Poder Aeroespacial Brasileiro e os desafios contemporâneos à sua Segurança e Defesa, incluindo as implicações do Acordo de Salvaguardas Tecnológicas; 2) Caracterizar a Segurança e Defesa (SEGDEF) como dimensão constitutiva do Poder Aeroespacial Brasileiro, analisando seu impacto e o arcabouço normativo do COMAER; 3) Apresentar os fundamentos da Segurança Corporativa Estratégica (SCorPE) de Marcos Mandarini (2005) como referencial teórico para a otimização da Segurança e Defesa; e 4) Propor diretrizes e recomendações para a otimização da estrutura, dos processos e dos recursos de SEGDEF no CLA, com base na aplicação da SCorPE e em uma abordagem estratégica de gestão de riscos.

Considerando o OE 1, o Capítulo 2 desta dissertação descreveu o CLA como um ativo estratégico singular, detalhando suas vantagens geográficas e competitivas, e seu papel como

pilar do PEB e da projeção internacional do Brasil. Analisou-se também o AST e suas profundas implicações para a SEGDEF, assim como as vulnerabilidades e os desafios à proteção do Centro sob a ótica das “perdas” conceituadas por Mandarinini (2005). Esta análise ratificou que o AST, ao mesmo tempo que potencializa o CLA, eleva exponencialmente a complexidade e a criticidade de sua SEGDEF.

O Capítulo 3, em atendimento ao OE 2, caracterizou a SEGDEF como uma dimensão intrínseca e habilitadora do Poder Aeroespacial Brasileiro. Demonstrou-se como a proteção eficaz da infraestrutura terrestre é vital para mitigar as vulnerabilidades do Poder Aeroespacial e para a sua sustentabilidade. Foi detalhado o arcabouço normativo da FAB, incluindo a DCA 11-45 (Concepção Estratégica), o PCA 11-47 (PEMAER), a DCA 205-4 (SEGDEF no COMAER), a NSCA 205-3 (SISDE), e a DCA 205-9 (SISI), concluindo-se que, embora robusto, este arcabouço requer uma aplicação customizada e estratégica para as especificidades do CLA.

Em resposta ao OE 3, o Capítulo 4 apresentou os fundamentos da Segurança Corporativa Estratégica (SCorpE) de Marcos Mandarinini (2005) e demais autores como o referencial teórico para a otimização da SEGDEF. Foram explorados seus pilares, a evolução do conceito de segurança, seus ramos e, crucialmente, seus segmentos de gestão (SGAI, SGP, SGProc, SGC), bem como a importância da cultura organizacional, filosofia, política de segurança, endomarketing e educação para segurança. A análise aprofundada das “perdas” potenciais no CLA, à luz de cada segmento da SCorpE, ilustrou a aplicabilidade e a relevância deste referencial para o contexto em estudo.

Finalmente, o Capítulo 5, direcionado pelo OE 4, realizou a aplicação prática da SCorpE, propondo um modelo de otimização para a SEGDEF no CLA. Foram detalhadas abordagens para o planejamento estratégico da segurança (incluindo planos de contingência e gerenciamento de crises), uma metodologia aprofundada para a gestão de riscos no Centro, e o fortalecimento da atividade de inteligência como suporte crucial. Como ápice desta análise, propôs-se a adoção do modelo SISI (DCA 205-9) como base para a modernização tecnológica e operacional da segurança das instalações, e a elaboração de um Plano Diretor de Segurança Estratégica (PDSE) para o CLA, que integre todos esses elementos de forma coesa e estratégica.

Os Objetivos Específicos associados ao Objetivo Geral permitiram, assim, que a resposta ao problema de pesquisa fosse encontrada. Com base na análise sistêmica das normativas da FAB, na aplicação do referencial da SCorpE e na consideração dos desafios únicos do CLA, este autor conclui que a SEGDEF, quando otimizada por uma abordagem estratégica, integrada e proativa, formalizada em um Plano Diretor de Segurança Estratégica

(PDSE) e implementada com os recursos e a cultura adequados, atua decisivamente como um elemento habilitador e multiplicador do Poder Aeroespacial Brasileiro no CLA.

Tal otimização é essencial para fortalecer a projeção de poder e a soberania nacional, respondendo eficazmente aos desafios contemporâneos e aos requisitos de acordos como o AST. A hipótese central deste estudo – de que a aplicação não otimizada da SEGDEF compromete a gestão de riscos e a capacidade operacional – foi, portanto, confirmada, sendo a adoção da SCorpE e de um PDSE o caminho proposto para a superação dessa condição.

As principais contribuições deste estudo residem na aplicação da SCorpE ao contexto singular de uma infraestrutura aeroespacial crítica; no reforço da SEGDEF como componente estratégico de gestão de riscos e prevenção de perdas; na análise das implicações do AST para a segurança do CLA; e na proposição de um modelo de otimização consubstanciado no PDSE. Como produto técnico-tecnológico desta dissertação, em consonância com as diretrizes da UNIFA, as bases para este PDSE são detalhadas como uma proposta de Manual de Segurança e Defesa para o Centro de Lançamento de Alcântara.

Reconhecem-se como limitações do estudo a predominância de fontes secundárias e a ausência de pesquisa de campo, o que pode ter restringido a profundidade da análise de desafios operacionais específicos. Ademais, o detalhamento exaustivo do PDSE proposto extrapolaria o escopo desta dissertação.

Por fim, como recomendações à Força Aérea Brasileira, sugere-se: a efetiva elaboração e implementação do PDSE para o CLA; a priorização da implementação do modelo SISI no Centro; a reestruturação do Curso de Preparação para Operações de Lançamento (CPOL), com a inclusão de um módulo obrigatório de Segurança e Defesa, a fim de fortalecer a cultura de SEGDEF desde a capacitação inicial de todo o efetivo; o fortalecimento contínuo da gestão de riscos e da inteligência de segurança; e a garantia da alocação de recursos adequados. Para futuros estudos, recomenda-se estudos comparativos com outros centros de lançamento.

Conclui-se, portanto, que a Segurança e Defesa Estratégica é um investimento indispensável para que o Centro de Lançamento de Alcântara possa cumprir, com resiliência e eficácia, sua missão vital para o presente e o futuro do Poder Aeroespacial Brasileiro e para a consolidação do Brasil como um ator relevante no cenário espacial global.

REFERENCIAS

AGUIAR, Vladimir. Centro está preparado para lançamento de foguete após acidente. **Agência Brasil**, 2018. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2018-09/centro-esta-preparado-para-lancamento-de-foguete-apos-acidente>. Acesso em: 24 ago. 2025.

ALIBERTI, Marco; CAPPELLA, Andrea; HROZENSKY, Michael. **Space Power Assessment Framework and Index**: ESPI Report 72. Vienna: European Space Policy Institute, 2019.

ALMEIDA, André Luiz de. **A Evolução do Poder Aeroespacial Brasileiro**. 2006. Tese (Doutorado em Geografia Humana) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2006.

ANDRADE, Israel de Oliveira et al. **O Centro de Lançamento de Alcântara: Abertura para o mercado internacional de satélites e salvaguardas para a soberania nacional**. Brasília, DF: Ipea, 2018. (Texto para Discussão, n. 2423).

ASSIS, Cirelene Maria da Silva Rondon de. **A projeção do poder de polícia das Forças Armadas nas áreas adjacentes aos aquartelamentos**. Curitiba: Editora CRV, 2020.

ASSOCIAÇÃO BRASILEIRA DE DIREITO AERONÁUTICO E ESPACIAL. **Acordo que rege as Atividades dos Estados na Lua e em outros Corpos Celestes**. [S.l.]: SBDA, 1979.

ASSUMPÇÃO, Marcelo Neival Hillesheim de; COSTA, Gustavo Monteiro Muniz. Os desafios e oportunidades para a atividade de contrainteligência na era do conhecimento. *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro**. Brasília: CNMP, 2019. p. 124-141.

BANDEIRA, Débora Gomes. **O Acordo de Salvaguardas Tecnológicas entre o Brasil e os Estados Unidos sobre a Base de Alcântara: a possibilidade de desenvolvimento tecnológico do setor espacial brasileiro à luz da experiência brasileira na parceria com a Ucrânia**. 2020.

BANDEIRA, Jerusa Capistrano Pinto. A Contrainteligência no Ministério Público: Breves Considerações. *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro**. Brasília: CNMP, 2019. p. 38-49.

BARDIN, Laurence. **Análise de Conteúdo**. São Paulo: Edições 70, 2011.

BRASIL. Agência Espacial Brasileira. **Centros de Lançamento**. Brasília, DF: Agência Espacial Brasileira. Disponível em: <https://www.gov.br/aeb/pt-br/o-programa-espacial-brasileiro/centros-de-lancamento>. Acesso em: 17 maio 2025.

BRASIL. Agência Espacial Brasileira. **PDI|CEA - Programa de Desenvolvimento Integrado para o Centro Espacial de Alcântara**. Alcântara, MA: AEB, 2022.

BRASIL. Centro de Lançamento de Alcântara. **Cartilha institucional do Centro de Lançamento de Alcântara**. Alcântara, MA: CLA, 2016.

BRASIL. Centro de Lançamento de Alcântara. **Diretrizes de Integração de Operações**. Alcântara, MA: CLA, 2017.

BRASIL. Comando da Aeronáutica. Portaria GABAER/GC3 nº 1.563, de 23 de dezembro de 2024. Aprova a Doutrina Básica da Força Aérea Brasileira - DCA 1-1. **Boletim do Comando da Aeronáutica**, Brasília, DF, 23 dez. 2024.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 1.597/GC3, de 10 de outubro de 2018. Aprova a reedição da DCA 11-45 “Concepção Estratégica - Força Aérea 100”. **Boletim do Comando da Aeronáutica**, Brasília, DF, n. 180, 15 out. 2018.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 340/GC3, de 13 de março de 2020. Aprova a reedição da DCA 205-4 “Segurança e Defesa no Comando da Aeronáutica”. **Boletim do Comando da Aeronáutica**, Brasília, DF, n. 044, 17 mar. 2020.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria GABAER/GC3 nº 979, de 14 de maio de 2025. Aprova a DCA 205-9 “Implantação do Suporte Integrado de Segurança das Instalações nas Organizações Militares do COMAER”. **Boletim do Comando da Aeronáutica**, Brasília, DF.

BRASIL. Comando da Aeronáutica. Comando de Preparo. Portaria COMPREP nº 91/COMPREP, de 9 de abril de 2021. Aprova a reedição da NSCA 205-3 “Sistema de Segurança e Defesa do Comando da Aeronáutica”. **Boletim do Comando da Aeronáutica**, Brasília, DF, n. 081, 4 maio 2021.

BRASIL. Comando da Aeronáutica. Departamento de Ciência e Tecnologia Aeroespacial. Portaria DCTA/DCE nº 540, de 4 de outubro de 2024. Aprova a TCA 37-15 “Cursos do DCTA para o ano de 2025”.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria GABAER nº 1.453/GC3, de 5 de junho de 2024. Aprova o PCA 11-47 “Plano Estratégico Militar da Aeronáutica 2024-2033”. **Boletim do Comando da Aeronáutica**, Brasília, DF.

BRASIL. [Constituição (1988)]. Emenda Constitucional nº 85, de 26 de fevereiro de 2015. Altera a Constituição Federal para dispor sobre a ciência, a tecnologia e a inovação. **Diário Oficial da União**: seção 1, Brasília, DF, p. 2, 27 fev. 2015.

BRASIL. Decreto nº 9.283, de 7 de fevereiro de 2018. Regulamenta a Lei nº 13.243, de 11 de janeiro de 2016, que dispõe sobre a inovação e a pesquisa científica e tecnológica no ambiente produtivo. **Diário Oficial da União**: seção 1, Brasília, DF, p. 2, 8 fev. 2018.

BRASIL. Decreto nº 10.220, de 5 de fevereiro de 2020. Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América sobre Salvaguardas Tecnológicas Relacionadas à Participação dos Estados Unidos da América em Lançamentos a partir do Centro Espacial de Alcântara, firmado em Washington, D.C., em 18 de março de 2019. **Diário Oficial da União**, Brasília, DF, 6 fev. 2020.

BRASIL. Lei nº 7.102, de 20 de junho de 1983. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 21 jun. 1983.

BRASIL. Lei nº 13.243, de 11 de janeiro de 2016. Dispõe sobre a inovação e a pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 12 jan. 2016.

BRASIL. Ministério da Ciência e Tecnologia. **Relatório Final da Investigação do Acidente com o VLS-1 V03**. Brasília, DF, 2004.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. MCTI quer transformar o Maranhão em um novo polo do programa espacial brasileiro. **Ministério da Ciência, Tecnologia e Inovação**, 24 jan. 2025. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2025/01/mcti-quer-transformar-o-maranhao-em-um-novo-polo-do-programa-espacial-brasileiro>. Acesso em: 17 jun. 2025.

BRASIL. Ministério da Defesa. **Brasil Encerra Mais Uma Conferência de Ministros de Defesa das Américas**. [S.l.]: MD, 2022.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF: MD, 2023.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: MD, 2012.

CAMARGO, Aluísio Viveiro; SOUZA, Marcello Corrêa de. Espaço: a nova arena geopolítica-satélites, conflitos e consciência situacional espacial. 2023.

CARON, Ricardo; BUENO, Vani Antônio. Inteligência e Segurança Institucional: uma abordagem sobre a segurança de áreas e instalações no Ministério Público. *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro**. Brasília: CNMP, 2019. p. 68-94.

CELLARD, André. A análise documental. *In*: POUPART, Jean et al. (org.). **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. 4. ed. Petrópolis: Vozes, 2014. p. 295-316.

CHOAIRY, Antônio Cesar Costa. **Alcântara vai para o espaço: a dinâmica da implantação do Centro de Lançamento de Alcântara**. São Luís: EDUFMA: PROIN-CS, 2000.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro**. Brasília: CNMP, 2019.

COSTA, Artemio Macedo; BARBOSA, Zulene Muniz. A expansão do Centro de Lançamento de Alcântara no contexto do novo imperialismo. **Revista Brasileira de Desenvolvimento Regional**, v. 10, n. 1, p. 127-142, 2022.

COSTA, Liviomar Macatrão Pires. **Políticas Públicas para o Desenvolvimento da economia local, o Centro Espacial de Alcântara e sua abertura para o Mercado mundial: perspectivas de participação comunitária.** 2021.

DA SILVA OLIVEIRA, Guilherme Tadeu Berriel. “Lawfare” e cerceamento tecnológico: o caso do acordo de salvaguardas tecnológicas Brasil-EUA. **Revista da Escola de Guerra Naval**, v. 26, n. 1, 2020.

DALABRIDA, Sidney Eloy. Resolução nº 156, de 13 de dezembro de 2016: O processo de surgimento da normatização sobre segurança institucional do Ministério Público Brasileiro. *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contrainteligência no Âmbito do Ministério Público Brasileiro.** Brasília: CNMP, 2019. p. 8-21.

DOLMAN, Everett C. **Astropolitik: Classical Geopolitics in the Space Age.** London: Frank Cass, 2001.

DOS SANTOS LIMA, Matheus Felipe Alves. O Poder aeroespacial como meio de atuação geopolítica: o espaço mundial, o Brasil e a América do Sul. **Geopauta**, v. 8, p. e14167, 2024.

DURÃO, Otavio Santos Cupertino; CEBALLOS, Décio Castilho. Desafios Estratégicos Do Programa Espacial Brasileiro. **Desafios Do Programa Espacial Brasileiro**, p. 41-58, 2011.

JACOBINI, Leandro Tadeu Garcia. **Do código à soberania aérea: metodologias seguras no desenvolvimento de software para a Força Aérea Brasileira.** 2024.

JÚNIOR, João Paulo Soares Alsina. **Política externa e poder militar no Brasil: universos paralelos.** Rio de Janeiro: Editora FGV, 2009.

KINOPP, Iwersen Trzeciak; MABA, Ana Paula. Contrainteligência: o papel da Segurança Orgânica no processo de seleção, recrutamento e desligamento de agentes no Sistema de Inteligência da Polícia Militar do Paraná. **Brazilian Journal of Development**, Curitiba, v. 9, n. 10, p. 28583-28604, out. 2023.

LIMA, Matheus Felipe Alves dos Santos. O Poder aeroespacial como meio de atuação geopolítica: o espaço mundial, o Brasil e a América do Sul. **Geopauta**, Vitória da Conquista, v. 8, p. e14167, 2024.

MANDARINI, Marcos. **Segurança Corporativa Estratégica: Fundamentos.** Barueri, SP: Manole, 2005.

MARTINS, G. de A. **Estudo de caso: uma estratégia de pesquisa.** São Paulo, SP: Atlas, 2006.
MENEZES, Antônio Alberto Moraes de et al. **Política de segurança orgânica: Polícia civil e polícia militar do Piauí.** Teresina: Lamparina Editora, 2022.

MESQUITA, Ivan Muniz de. O poder aeroespacial e a estratégia nacional de defesa (END). **Revista da Escola Superior de Guerra**, v. 33, n. 67, p. 82-97, jan./abr. 2018.

MODESTO, Thiago de Souza; NEVES, Sérgio Alcântara. A segurança orgânica e o poder de polícia do exército nas áreas adjacentes dos quartelamentos. **Revista do Ministério Público Militar**, Brasília, a. 52, n. 46, p. 162-216, maio 2025.

MONTGOMERY, Cynthia A. **O estrategista**: seja o líder de que sua empresa precisa. Rio de Janeiro: Sextante, 2012.

MOURA, Carlos. *In*: AGÊNCIA ESPACIAL BRASILEIRA. Centro de Lançamento de Alcântara Completa 38 Anos. Publicado em 02 mar. 2021.

MUSSI, Diana Zatz. A base espacial de Alcântara. **ComCiência**, 28 maio 2024.

NOGUEIRA, João Rui Ramos. A importância estratégica do Espaço para a Segurança e Defesa: A NATO e a União Europeia. **Revista de Ciências Militares**, v. 2, 2014.

PADILHA, Luiz. Tecnologia brasileira é usada em lançamento de foguete sul-coreano em Alcântara. **MundoGEO**, [S.l.], 25 mar. 2023.

PERROW, Charles. **Normal Accidents**: Living with High-Risk Technologies. Princeton, NJ: Princeton University Press, 1999.

PORTER, Michael E. How competitive forces shape strategy. **Harvard Business Review**, v. 57, n. 2, p. 137-145, 1979.

PORTER, Michael E. **Competitive Advantage**: Creating and Sustaining Superior Performance. New York: Free Press, 1985.

ROCHA, Paulo Cesar Cardoso. **A relação entre a Gestão de Riscos Integrada em uma organização com infraestrutura crítica e as questões de Defesa Nacional**. 2019. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) – Escola Superior de Guerra, Brasília, DF, 2019.

ROSA, C. E. V. **Poder Aéreo**: Guia de Estudos. Rio de Janeiro: Editora Luzes, 2014.
SÁ, Odair Oliveira de. **A segurança das infraestruturas críticas de energia no Brasil**. 2017. Dissertação (Mestrado em Energia) - Instituto de Energia e Ambiente, Universidade de São Paulo, São Paulo, 2017.

SANTOS, Leonardo C. et al. Fatores de risco na cadeia de suprimentos da indústria aeroespacial. **Production**, v. 23, n. 4, p. 789-802, 2013.

SILVA, Bruna Sampaio et al. Propriedade intelectual e soberania nacional: análise do acordo de salvaguardas tecnológicas entre brasil e estados unidos para o centro espacial de alcântara. **ÍANDÉ: Ciências e Humanidades**, v. 4, n. 1, p. 22-33, 2020.

SIQUEIRA, Mauro Barbosa. Poder Aeroespacial Brasileiro: dissuasão como sentimento de segurança, coerção como medida eficaz à Defesa Nacional. **Revista da UNIFA**, v. 22, n. 25, 2009.

SOUZA, João Gabriel Araujo de. **A projeção internacional do Brasil e a transformação da Força Aérea**: as operações conjuntas e o caso da Escudo-tínia. 2024.

SOUZA, Marcelo Weitzel Rabello de et al. Apresentação. *In*: CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **Estudos de Segurança Institucional e Contraineligência no Âmbito do Ministério Público Brasileiro**. Brasília: CNMP, 2019. p. 6-7.

TV BRASIL. Conheça o Centro de Lançamento de Alcântara | Ciência é Tudo. **YouTube**, 27 nov. 2020. Disponível em: <https://www.youtube.com/watch?v=OYzBOrgjNYs>. Acesso em: 17 maio 2025.

UNIVERSIDADE DA FORÇA AÉREA. **Manual de trabalhos acadêmicos da Universidade da Força Aérea**. 7. ed. Rio de Janeiro: EDUNIFA, 2024.

UNIVERSIDADE FEDERAL DO MARANHÃO. **Contribuições da UFMA ao programa de desenvolvimento integrado do centro espacial de Alcântara PDI-CEA**. São Luís: UFMA, 2020.

VELLASCO, Fabiany Maria Made e. **Análise do arranjo institucional do Programa Nacional de Atividades Espaciais (PNAE) e seu impacto no desenvolvimento da indústria espacial brasileira: 1996-2018**. 2020. Dissertação (Mestrado em Governança e Desenvolvimento) - Escola Nacional de Administração Pública, Brasília, DF, 2020.

WEICK, Karl E.; SUTCLIFFE, Kathleen M. **Managing the Unexpected: Resilient Performance in an Age of Uncertainty**. 2. ed. San Francisco, CA: Jossey-Bass, 2007.

YIN, Robert K. **Estudo de caso: planejamento e métodos**. 2. ed. Porto Alegre: Bookman, 2001.

**ANEXO I – APRESENTAÇÃO DE PROPOSTA PARA O MANUAL DE
SEGURANÇA E DEFESA PARA OPERAÇÕES DE LANÇAMENTO NO CENTRO
DE LANÇAMENTO DE ALCÂNTARA**



**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE LANÇAMENTO DE ALCÂNTARA**

Ofício s/nº
Protocolo COMAER nº 67710.007563/2025-50

Alcântara, 1º de setembro de 2025.

Do 1º Ten QOCON TEC SED RAIMUNDO FELIPE DA SILVA COSTA
Ao Diretor do CLA

Assunto: Proposta de Manual de Segurança e Defesa para Operações de Lançamento no CLA.

1. Ao cumprimentá-lo respeitosamente, passo a tratar sobre a apresentação de proposta para o Manual de Segurança e Defesa para Operações de Lançamento no Centro de Lançamento de Alcântara.
2. Sobre o assunto, informo ao Senhor que este Militar é discente do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA), e tem como projeto de pesquisa "O Papel Estratégico da Segurança e Defesa no Poder Aeroespacial Brasileiro: Uma Análise do Centro de Lançamento de Alcântara".
3. Assim, conforme preconiza o Regulamento do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA) deverá ser entregue ao término uma Produção Bibliográfica, Técnica e Tecnológica, a qual seria, em caso de aprovação desta Direção, o presente Manual, elaborado por este discente em coordenação com Senhor Comandante do Grupo de Segurança e Defesa de Alcântara (GSD-AK), Maj Inf Diego da Costa Diamante.
4. Ressalto que aplicabilidade do manual foi preliminarmente verificada nas Operações Falcão I e II do corrente ano, realizadas por este Centro, observando-se ainda que o mesmo será apresentado em forma física ao Senhor, por tratar de informações de pesquisa e desenvolvimento científicos ou tecnológicos, possuindo caráter sigiloso, conforme preconiza o §1º do Art. 7º da Lei nº 12.527 de 18 de novembro de 2011 e o Inciso II do Art. 6º do Decreto nº 7.724 de 14 de maio de 2012.
5. Alfim, coloco-me à disposição por intermédio do contato telefônico (86) 99932-6778 e e-mail: silvacostarfsc@fab.mil.br.

RAIMUNDO FELIPE DA SILVA COSTA 1º Ten QOCON TEC SED

ANEXO II – APROVAÇÃO DO MANUAL DE SEGURANÇA E DEFESA PELO CENTRO DE LANÇAMENTO DE ALCÂNTARA

INFORMAÇÃO DE PESQUISA E DESENVOLVIMENTO – ACESSO RESTRITO
§1º Art. 7º da Lei nº 12.527, de 18 de novembro de 2011
Inciso II do Art. 6º do Decreto nº 7.724, de 16 de maio de 2012



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL
CENTRO DE LANÇAMENTO DE ALCÂNTARA
GRUPO DE SEGURANÇA E DEFESA DE ALCÂNTARA

Manual de Segurança e Defesa para Operações de Lançamento no Centro de Lançamento de Alcântara.

Elaborado por:

Documento assinado digitalmente
gov.br RAIMUNDO FELIPE DA SILVA COSTA
Data: 09/09/2025 12:16:07-0300
Verifique em <https://validar.itl.gov.br>

RAIMUNDO FELIPE DA SILVA COSTA – 1º Ten TEC SED
Adjunto do Coordenador de Segurança Orgânica do CLA

Revisado por:

Documento assinado digitalmente
gov.br DIEGO DA COSTA DIAMANTE
Data: 10/09/2025 10:35:04-0300
Verifique em <https://validar.itl.gov.br>

DIEGO DA COSTA DIAMANTE – Maj Inf
Coordenador de Segurança Orgânica do CLA

Aprovado por:

**CLOVIS MARTINS DE
SOUZA:26738463871**

Assinado digitalmente por: CLOVIS MARTINS DE SOUZA:26738463871
ID: C=BR, O=ICP-Brasil, OU=Ministério da Defesa, OU=03277610000125, OU=Certificado PF A3,
CN=CLOVIS MARTINS DE SOUZA:26738463871
E-mail: clovis.martins@defesa.gov.br
Data: 2025.08.31 17:04:30-0300
Fonte: PDF Reader Versão: 20252.0

CLÓVIS MARTINS DE SOUZA - Cel Av
Coordenador Geral de Operação do CLA

Alcântara – MA, 08 de agosto de 2025.

INFORMAÇÃO DE PESQUISA E DESENVOLVIMENTO – ACESSO RESTRITO
§1º Art. 7º da Lei nº 12.527, de 18 de novembro de 2011
Inciso II do Art. 6º do Decreto nº 7.724, de 16 de maio de 2012

**ANEXO III – PORTARIA DE APROVAÇÃO DO MANUAL DE SEGURANÇA E
DEFESA PELO CENTRO DE LANÇAMENTO DE ALCÂNTARA**



**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE LANÇAMENTO DE ALCÂNTARA**

**PORTARIA CLA Nº 81/SAP , DE 25 DE SETEMBRO DE 2025.
Protocolo COMAER nº 67710.008453/2025-13**

Aprova o Manual de Segurança e Defesa
para Operações de Lançamento do Centro
de Lançamento de Alcântara.

O DIRIGENTE MÁXIMO DO CENTRO DE LANÇAMENTO DE ALCÂNTARA, no uso de suas atribuições e de acordo com o Regimento Interno - RICA 21-91/2023 - BCA Nº 108, de 15 JUN 2023 e Regulamento dos Centro de Lançamento - PORTARIA GABAER Nº 206/GC3, DE 28 DEZ 2021, resolve:

Art. 1º Aprovar o “Manual de Segurança e Defesa para Operações de Lançamento do Centro de Lançamento de Alcântara”;

Art. 2º Esta Portaria entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.


CLOVIS MARTINS DE SOUZA Cel Av
Diretor do CLA