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

OSVALDO JOSÉ DE JESUS SILVA, Cap Eng

Uma análise da governança de riscos cibernéticos na FAB sob a ótica dos modelos PRINCE2, PMBOK e Três Linhas de Defesa

Rio de Janeiro
2023

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

OSVALDO JOSÉ DE JESUS SILVA, Cap Eng

Uma análise da governança de riscos cibernéticos na FAB sob a ótica dos modelos PRINCE2, PMBOK e Três Linhas de Defesa

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

Orientador: Prof. Dr. Newton Hirata

Rio de Janeiro
2023

Silva, Osvaldo José de Jesus

S586 Uma análise da governança de riscos cibernéticos na FAB sob a ótica dos modelos PRINCE2, PMBOK, e três linhas de defesa. / Osvaldo José de Jesus Silva. – Rio de Janeiro: Universidade da Força Aérea, 2023.

110 f.: il., enc.

Orientador: Prof. Dr. Newton Hirata

Dissertação (mestrado) – Universidade da Força Aérea, Rio de Janeiro, 2023.

Referências: f. 101-108

1. Governança Cibernética. 2. Riscos Cibernéticos. 3. Defesa Cibernética. I. Título. II. Hirata, Newton. III. Universidade da Força Aérea.

CDU: 355.45

OSVALDO JOSÉ DE JESUS SILVA Cap QOENG CMP

Uma análise da governança de riscos cibernéticos na FAB sob a ótica dos modelos PRINCE2, PMBOK e Três Linhas de Defesa

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
gov.br
NEWTON HIRATA
Data: 12/12/2023 13:43:54-0300
Verifique em https://validar.iti.gov.br

Presidente, Prof. Dr. NEWTON HIRATA (CPF: 878.550.119-00) – UNIFA

Documento assinado digitalmente
gov.br
PEDRO ARTHUR LINHARES LIMA
Data: 12/12/2023 17:47:50-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. PEDRO ARTHUR LINHARES LIMA (CPF: 492.480.907-10) – UNIFA

Documento assinado digitalmente
gov.br
HELIO CAETANO FARIAS
Data: 13/12/2023 23:50:33-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. HÉLIO FARIAS (CPF: 221.057.152-85) – ECEME

Rio de Janeiro

Dezembro de 2023

DEDICATÓRIA

Dedico este trabalho a minha filha Aurora, a pequena que veio iluminar minha vida. Obrigado por mostrar a grandeza das coisas mais simples.

AGRADECIMENTOS

Agradeço a Deus pois sem ele eu não teria forças para essa longa jornada.

Agradeço o incentivo e o apoio da minha família, nos vários momentos de imersão nos estudos, por compreenderem minha ausência e apoiarem na minha jornada.

Agradeço a meu orientador, Prof. Dr. Newton Hirata pela incansável orientação, paciência, equilíbrio e apoio para a conclusão deste trabalho.

Agradeço a todos os Professores e Membros do PPGCA da UNIFA, e companheiros de turma, pelo conhecimento adquirido, experiências compartilhadas e crescimento profissional alcançado. Os senhores foram fundamentais para o meu amadurecimento pessoal e profissional.

Agradeço à CISCEA - Comissão de Implantação do Sistema de Controle do Espaço Aéreo, pela concessão para realização deste curso, mesmo com a criticidade e emergência nos projetos conduzidos por esta Comissão. Sem sua valorização da formação do militar ali presente não seria possível esta consecução.

RESUMO

Os riscos cibernéticos estão presentes em todas as organizações e têm impactado diretamente nos projetos desde sua concepção até a operação dos sistemas. A gestão desses riscos tem sido um desafio crescente, dado o avanço da tecnologia e a interdependência dos sistemas. E a Força Aérea Brasileira (FAB) não é exceção nesse cenário. As diversas legislações que abordam o tema dentro da FAB nem sempre conseguem colocar em prática todos os aspectos de segurança cibernética que o atual contexto de guerra irregular e assimétrica exige. Considerando a evolução das guerras, aquela caracterizada como cibernética se encaixa em um cenário de conflito assimétrico e irregular de 3ª e 4ª geração, em que o conhecimento e domínio do ciberespaço são primordiais para o ataque e a defesa no campo de batalha. Nessa perspectiva, o trabalho busca mostrar que os modelos PRINCE2, PMBOK servem para identificar e gerenciar os riscos cibernéticos de forma prática e assertiva de um sistema da FAB pois vão considerar o risco cibernético desde a concepção do sistema até sua operação. Já o modelo das Três Linhas de Defesa irá aprimorar a gestão de riscos cibernéticos por meio do tratamento e monitoramento de incidentes e da melhoria contínua das linhas de defesa dentro da FAB permitindo uma retroalimentação integrada das partes envolvidas nos projetos em termos de riscos cibernéticos.

Palavras-chave: Governança Cibernética; Riscos Cibernéticos; Defesa cibernética.

ABSTRACT

Cyber risks are present in all organizations and have a direct impact on projects from conception to system operation. The management of these risks has been a constant challenge for FAB as well as for several organizations that deal with the subject in the world. The various legislations that address the issue within the FAB are not always able to put into practice all aspects of cybersecurity that the current context of irregular and asymmetric warfare requires. Considering the evolution of wars cyber warfare fits into a 3rd and 4th generation asymmetric and irregular conflict scenario where knowledge and mastery of cyberspace are essential for attack and defense in the field. of battle. This work seeks to show that the PRINCE2, PMBOK models can identify and manage cyber risks in a practical and assertive way of a FAB system as they will consider cyber risk from the conception of the system to its operation. The Three Lines of Defense model will improve cyber risk management through incident handling and monitoring and continuous improvement of lines of defense within the FAB, allowing integrated feedback from the parties involved in projects that contain cyber risks.

Keywords: *Cyber Governance; Cyber Risks; Cyber Defense.*

LISTA DE SIGLA E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
CDCiber	Centro de Defesa Cibernética
CISCEA	Comissão de Implantação do Sistema de Controle do Espaço
COMAER	Comando da Aeronáutica
COSO	*Committee of Sponsoring Organizations of the Treadway*
DCTA	Departamento de Ciência e Tecnologia Aeroespacial
DECEA	Departamento de Controle do Espaço Aéreo
DoD	*Department of Defense* (USA)
DCA	Diretriz do Comando da Aeronáutica
EMAER	Estado-Maior da Aeronáutica
EUA	Estados Unidos da América
END	Estratégia Nacional de Defesa
FA	Forças Armadas
FAB	Força Aérea Brasileira
MD	Ministério da Defesa
OM	Organização Militar
PND	Política Nacional de Defesa
SERPRO	O Serviço Federal de Processamento de Dados
SISCEAB	Sistema de Controle do Espaço Aéreo Brasileiro
SMDC	Sistema Militar de Defesa Cibernética
SQL	*Structured Query Language* (Linguagem de Consulta Estruturada)
TCU	Tribunal de Contas da União

SUMÁRIO

1. Introdução..... 11
1.1 Objetivos.....13
1.1.1 Objetivo Geral.....13
1.1.2 Objetivos Específicos.....14
1.2 Delimitação do Estudo.....14
1.3 Justificativa..... 14
1.4 Metodologia.....19
2. Referencial Teórico e Modelos para tratamento e gerenciamento de riscos cibernéticos.....21
2.1 Guerra irregular, guerra assimétrica, guerra de 4ª geração e guerra cibernética.....24
2.2 Modelo de Avaliação de Riscos segundo o PMBOK..... 38
2.3 Modelo de Avaliação de Riscos segundo o PRINCE2.....44
2.4 Modelo de Avaliação de Riscos segundo as Três Linhas de Defesa.....51
2.4.1 A Primeira Linha de Defesa..... 53
2.4.2 A Segunda Linha de Defesa.....54
2.4.3 A Terceira Linha de Defesa.....56
2.4.4 Representações esquemáticas do Modelo das Três Linhas de Defesa..... 58
3 Revisão Documental: Defesa cibernética, gerenciamento de riscos cibernéticos, segurança da Informação e qualidade na Força Aérea Brasileira.....62
3.1 Defesa cibernética na Força Aérea Brasileira.....64
3.1.1 As três linhas de defesa na Força Aérea Brasileira: Tratamento de Incidentes cibernéticos na FAB e Auditoria Interna.....69
3.2 Os modelos PMBOK e PRINCE2 na Força Aérea Brasileira.....75
3.3 Política do Comando da Aeronáutica para Segurança da Informação.....84
3.4 Procedimentos para Segurança da Informação no Comando da Aeronáutica..... 87
3.5 Garantia Governamental da Qualidade para Segurança da Informação no Comando da Aeronáutica.....89
4. Análise dos modelos Três Linhas de Defesa, PRINCE 2 e PMBOK.....91
4.1 Análise do Modelo Três Linhas de Defesa.....91
4.2 Análise dos Modelos PRINCE 2 e PMBOK.....93
5. Considerações Finais.....98
Referências..... 101
ANEXO A - Mapa de Ataques digitais.....109

1. Introdução

As Forças Armadas são fundamentais na constituição do Estado porque elas garantem os princípios básicos para sua existência, em particular, segurança e soberania. O Estado precisa ser soberano frente ao demais estados, deve manter seus poderes constitucionais em funcionamento e necessita manter a ordem interna. Da perspectiva brasileira, tais princípios são assegurados no artigo 142 da Constituição (1988):

> Art. 142. As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.

Adicionalmente à Constituição Federal, a Estratégia Nacional de Defesa esclarece que o setor cibernético é estratégico para o país assim como o aeroespacial e o nuclear. O documento em sua versão de 2012 registra que esses três setores extrapolam as fronteiras entre desenvolvimento e defesa, entre o civil e o militar. Além disso, as três Forças devem atuar em rede para que os setores espacial e cibernético tenham tecnologia própria para monitorar o país a partir do espaço (Brasil, 2012c, p.3).

No contexto do posicionamento de defesa do Estado é fundamental a preocupação com os fatores que garantam sua soberania. Nesse sentido, a guerra cibernética é um tema sensível porque representa o conflito do futuro e do presente, como uma ameaça real. Em um cenário complexo e instável em termos de segurança internacional como se vive atualmente, destacam-se a inovação e a assimetria de atores e ações, em que qualquer indivíduo a partir de seu computador, em qualquer lugar do mundo, tem a possibilidade de infligir um ataque cibernético.

Segundo a revista *Em Discussão* (2014) do Senado Federal, as denúncias em 2013 do ex-técnico da CIA (Central de Inteligência Americana), Edward Snowden, levantaram grande preocupação sobre espionagem de vários países, inclusive o Brasil. As primeiras denúncias realizadas por Snowden foram publicadas no jornal *The Guardian.* Ele mostrou como os Estados Unidos utilizavam programas de vigilância para espionar americanos e não americanos incluindo a ex-presidente Dilma Rousseff e a chanceler alemã Angela Merkel, utilizando os servidores de empresas como Google, Apple e Facebook.

Essa espionagem moderna que ocorre por meio dos recursos da tecnologia da informação e da comunicação, as chamadas TICs, leva a uma espécie de “guerra fria

cibernética". Os atores precisam se proteger de ameaças capazes de gerar caos, pânico, prejuízos econômicos de grande magnitude e colapso dos mais variados sistemas, o que pode significar também, criar medidas de contra-ataque. O site "Digital Attack Map", por exemplo, desenvolvido pela empresa Arbor Networks em parceria com a Google, apresenta em tempo real as tentativas de ataques DDoS (*Distributed Denial of Service*). Tratam-se de ataques distribuídos de negação de serviço, uma tentativa de tornar os recursos de um sistema indisponíveis para os seus usuários por meio da inundação do sistema com uma grande quantidade de requisições proveniente de diversos locais diferentes (Anexo A).

Outro fator que chama a atenção na nova guerra é que o cenário cibernético está passando de secundário para principal:

> O Departamento de Defesa dos Estados Unidos (DoD) prevê a necessidade de bombardear coisas no mundo físico para se defender contra ataques cibernéticos, ou para redirecionar um inimigo às redes que os guerreiros cibernéticos americanos controlam, Clarke e Knake (2015, p. 42).

Os Estados Unidos estão preocupados com esse cenário de guerra, baseados em informações e recursos tecnológicos e computacionais. De acordo com Dornelles Jr (2014), China e Estados Unidos são os únicos pólos de poder no Leste Asiático. O autor mostra que o avanço militar chinês impactou a distribuição de poder na região, "considerando os inventários militares e seus meios de emprego (táticas assimétricas de antiacesso e negação de área), especialmente na esfera aeronaval". A utilização dos meios de antiacesso e negação de área terrestres, navais e aéreos seria precedida por ataques ao sistema de C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*) das forças estadunidenses posicionadas no teatro de operações. Dornelles Jr (2014) explica que "a rede de computadores inimiga seria atacada pelo ELP (Exército Popular de Libertação) por meio de guerra cibernética, isto é, ataques de vírus, poluição de informação, coleta de informações etc."

Os chineses perceberam que seriam incapazes de derrotar os EUA em sua superioridade numérica. A partir de então a China começou a reduzir o efetivo de suas forças armadas e a investir em novas tecnologias. Clarke e Knake (2015, p. 45) mostram que uma dessas tecnologias foi a *wangluohua* termo chinês que quer dizer *"*networkization*"* ou desenvolvimento centrado em redes, para lidar com o "novo campo de batalha nos computadores". Segundo os autores, essa tecnologia permitiria o domínio da informação representando a derrota de uma força superior que a perdesse ou a vitória de uma força inferior que a possuísse.

Para Clarke e Knake (2015, p.45), os estrategistas chineses confluíam para a percepção de que a guerra cibernética poderia ser utilizada pela China para equilibrar suas limitações qualitativas militares em relação aos EUA. Estes autores explicam como os estrategistas chineses estão articulando suas forças para essa nova guerra:

> O Major General Wang Pufeng escreveu abertamente sobre a meta de *zhixinniquam*, o "domínio da informação", enquanto o Major General Dai Qingmin, do Estado Maior, afirmou que tal domínio só poderia ser alcançado com um ataque cibernético preventivo. Esses estrategistas criaram a "Rede Integrada de Guerra Eletrônica", algo semelhante ao modismo da Guerra Centrada a Redes que acontecia no Pentágono.

A guerra cibernética difere da guerra eletrônica, dentre outras características, pela utilização dos meios para atingirem o alvo. Enquanto a guerra eletrônica utiliza a energia eletromagnética como meio de aniquilar ou reprimir as forças inimigas, a guerra cibernética utiliza o ciberespaço, ou seja, o espaço das comunicações por redes de computação. Um caça sobrevoando uma zona de combate pode tanto ser atingido por um ataque eletrônico e ficar à mercê do inimigo, quanto toda a frota pode ser atingida por um ataque cibernético em sua rede apoiadora de radares e comunicações e perder a guerra completamente.

O tema é importante para o Poder Aeroespacial porque poderá melhorar o gerenciamento dos riscos cibernéticos na Força Aérea Brasileira, pois será levantado de que maneira as três linhas de defesa, o PMBOK e o PRINCE2 contribuam não apenas para a compreensão dos ataques cibernéticos, mas também para a identificação de pontos de melhorias e possível criação de medidas e políticas que ajudem a mitigar os riscos de ataques cibernéticos.

Sinteticamente, a questão problema levantada é: Como utilizar os modelos PRINCE2, PMBOK e das três linhas de defesas para identificar, tratar e gerenciar os riscos cibernéticos de um sistema da Força Aérea Brasileira?

1.1 Objetivos

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é analisar a utilização dos modelos PRINCE2, PMBOK e de Três Linhas de Defesa na melhoria da gestão de riscos cibernéticos no Comando da Aeronáutica visando aprimorar a governança e mitigar os riscos cibernéticos

evidenciados por ataques em potencial aos ativos de Tecnologia da Informação da Força Aérea Brasileira.

1.1.2 Objetivos Específicos

- Identificar como está estruturada a defesa cibernética na Força Aérea Brasileira.
- Compreender como os modelos PMBOK, PRINCE2 e Três Linhas de Defesa tratam a gestão de riscos cibernéticos.
- Analisar a utilização dos modelos PMBOK, PRINCE2 e Três Linhas de Defesa na Força Aérea Brasileira.

1.2 Delimitação do Estudo

A motivação do estudo foi tentar compreender de que forma os ataques cibernéticos[1] contra os ativos de Tecnologia da Informação da Força Aérea podem ser mitigados a partir da gestão dos riscos cibernéticos. Isso significa, de alguma forma, identificar e monitorar os riscos cibernéticos em potencial. É possível considerar cenários catastróficos se dados, informações e sistemas mantidos e conectados eletronicamente não forem devidamente protegidos contra qualquer tipo de vulnerabilidade.

A preocupação com a segurança cibernética é muito mais do que uma questão comercial envolvendo empresas e o cidadão ou a proteção da FAB (Força Aérea Brasileira) e todos os seus recursos e sistemas. Trata-se de uma questão de soberania nacional, uma vez que a segurança do país pode ser ameaçada. Portanto, optou-se por propor um estudo que analisasse as melhores práticas de gestão de riscos e como essas práticas sob o aspecto do PMBOK, PRINCE2 e das Três linhas de defesa poderiam melhorar a governança de riscos cibernéticos na Força Aérea Brasileira.

1.3 Justificativa

[1] Podem ser de diversos tipos, por exemplo: worm, injeção de código, scan, fraude, DoS, Invasão, inclusive um ataque sobre uma vulnerabilidade nunca explorada até o momento, chamado de ataque *Zero Day*.

O presente trabalho se enquadra na Linha de Pesquisa: Relação entre Estados, Pensamento Estratégico Contemporâneo e Poder Aeroespacial, Núcleo Temático: Pensamento Militar Contemporâneo, Tema de Pesquisa: Conflitos do Século XXI e Poder Aeroespacial.

Parte-se da premissa de que os padrões PRINCE2, PMBOK e o Modelo de Três Linhas de Defesa possuem elementos suficientes para melhorar a gestão de riscos na Força Aérea Brasileira. Sabe-se, por meio da Doutrina base da Força Aérea Brasileira que a Tarefa Básica de Exploração da Informação descrita na DCA 1-1 é uma das atividades essenciais de Força Aérea (Brasil, 2012a, p.46).

Considerando a evolução das guerras conforme descrito por Visacro (2011, p.54) a guerra cibernética se encaixa em um cenário de conflito assimétrico e irregular de 3ª e 4ª geração em que o conhecimento e o domínio do ciberespaço são primordiais para o ataque e defesa no campo de batalha.

Levy (1999) explica que o ciberespaço não compreende apenas materiais, informações e seres humanos. É também constituído e povoado por seres estranhos, meio textos, meio máquinas, meio atores, meio cenários: os programas. Um programa, ou software, é uma lista bastante organizada de instruções codificadas, destinadas a fazer com que um ou mais processadores executem uma tarefa. Por meio dos circuitos que comandam, os programas interpretam dados, agem sobre informações, transformam outros programas, fazem funcionar computadores e redes, acionam máquinas físicas, viajam, reproduzem-se etc. De fato, as novas tecnologias têm um enorme impacto na sociedade.

O desenvolvimento das cibertecnologias é encorajado por Estados que buscam fortalecer suas capacidades militares. É também uma das grandes questões da competição econômica mundial entre as empresas gigantes da eletrônica e de software e entre países, regiões, parceiros e blocos econômicos. De acordo com Clarke e Knake (2015, p.38), em 2009 o Comandante da Força Aérea dos Estados Unidos, o General Norton Schwartz declarou aos seus oficiais que:

> [...]o ciberespaço é vital para a luta atual e para uma vantagem militar futura dos Estados Unidos, sendo a intenção da Força Aérea dos Estados Unidos fornecer uma gama completa de recursos no ciberespaço. O ciberespaço é um domínio disputado, e a luta já está acontecendo hoje.

Além da Força Aérea, da Marinha e do Exército dos Estados Unidos há também unidades de guerra cibernética, controladas pelo Comando Cibernético, criado em 2009. Até mesmo os Estados Unidos enfrentam dificuldades em estruturar seu comando cibernético.

Clarke e Knake (2015, p.40) mostram que a missão do Comando Cibernético é defender o Departamento de Defesa (DoD) e talvez alguns outros órgãos do governo, mas não há planos ou recursos para defender a infraestrutura civil. Os dois ex-diretores da NSA acreditam que essa missão deve ser tratada pelo Departamento de Segurança Interna (DHS), mas afirma que nem o DHS nem o Pentágono possuem capacidade de defender o ciberespaço corporativo que faz a maior parte do país funcionar.

Em uma análise mais aprofundada, a Estratégia Militar Nacional para Operações Cibernéticas dos EUA revela alguns problemas criados pela guerra cibernética. Segundo Clarke e Knake (2015, p.41):

> [...]sobre a geografia do ciberespaço, a estratégia reconhece implicitamente o problema da soberania ('a falta de fronteira geopolítica... permite que ocorram operações em quase qualquer lugar'), bem como a presença de alvos civis 'o ciberespaço atravessa fronteiras geopolíticas... e é firmemente integrado às operações de infraestrutura crítica e à atuação do comércio'.

Os Estados estão mais familiarizados em reconhecer sua soberania em termos de territórios físicos. O avanço das fronteiras cibernéticas leva os países a definirem limites conflitantes no ciberespaço que consideram violação de sua soberania. Um dos princípios da guerra seria não atingir civis diretamente, mas a complexidade a guerra cibernética implica impacto direto em infraestruturas críticas civis como alvo.

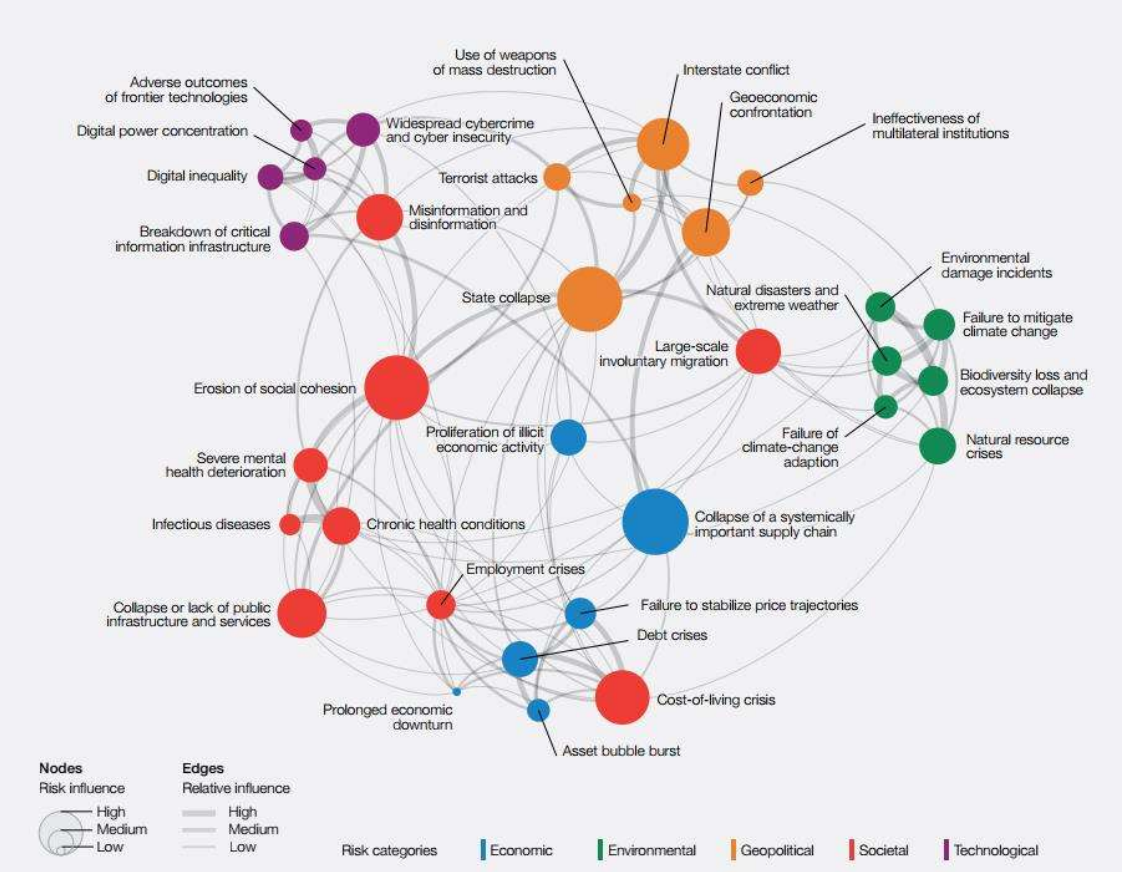
Battista et al. (2023), em uma publicação do Fórum Econômico Mundial, mostraram por meio do *The Global Risks Report 2023* a lista dos 10 riscos mais relevantes para os próximos 2 anos (curto prazo) e 10 anos (longo prazo) na Figura 1. Battista et al. (2023) explicam que a prospecção futura dos riscos apresentados se baseia em uma Pesquisa de Percepção de Riscos Globais (GRPS), a qual tem sustentado o Relatório de Riscos Globais do Fórum Econômico Mundial há quase duas décadas. Os autores esclarecem ainda que a pesquisa de 2023 reuniu *insights* importantes sobre o cenário global de riscos em evolução de mais de 1.200 especialistas do meio acadêmico, empresarial, governamental, da comunidade internacional e da sociedade civil. As respostas ao GRPS 2022-2023 foram recolhidas de 7 de setembro a 5 de outubro de 2022. As cores indicam diferentes áreas, sendo que a cor roxa representa os riscos ligados à área tecnológica. Nos períodos prospectados, seja curto ou longo, os riscos ligados insegurança cibernética e crimes cibernéticos figuram em oitava posição, colocando-se entre os 10 riscos globais mais relevantes.

Figura 1- Riscos globais classificados por gravidade no curto e longo prazo

Fonte: World Economic Forum 2023, Global Risks Reports.

Na Figura 2, pode-se observar que os riscos cibernéticos (cor roxa) possuem forte ligação com a falha de infraestruturas de informações críticas, ataques terroristas, desinformação e resultados adversos de tecnologias de fronteira. Battista et al. (2023) definem os resultados adversos de tecnologias de fronteira como consequências negativas intencionais ou não dos avanços tecnológicos sobre indivíduos, empresas, ecossistemas e/ou economias, como por exemplo: IA (Inteligência Artificial), interfaces cérebro-computador, biotecnologia, geoengenharia, computação quântica e metaverso.

Figura 2 - Mapa de interconexões dos Riscos Globais



Fonte: World Economic Forum 2008–2018, Global Risks Reports.

No Brasil, além de assegurado na END o desenvolvimento da defesa cibernética é fundamental para a proteção dos centros de gravidade e para manutenção da sua capacidade de impor sua vontade perante os demais Estados.

Segundo Raza (2013), o Brasil está despreparado em termos de inteligência cibernética em sua evolução tecnológica. Este autor explora o incidente de 2013 no qual o governo brasileiro foi alvo de espionagem pelos EUA e diz que o fato é muito pior do que foi retratado nos noticiários:

> É que as evidências divulgadas de inteligência cibernética, em larga escala, em âmbito global, postulam que as redes de comunicações e de controle de infraestruturas críticas foram todas violadas, permitindo – e, logicamente, construindo a condição – para o implante de bombas lógicas: dispositivos dormentes em softwares de sistemas críticos, colocados prontos para serem ativados em dadas circunstâncias pré-definidas, com capacidade de destruir as condições de sustentação da segurança em seus sete domínios: ambiental, tecnológico, sócio-humano, político-econômico, geoestratégico, tecnológico e informacional.

Em novembro de 2020, o Tribunal Superior Eleitoral do Brasil sofreu um ataque cibernético significativo, que tentou comprometer a integridade das eleições municipais. O ataque foi tratado rapidamente e as eleições ocorreram sem incidentes graves (TSE, 2020), mas foi um sinal de alerta importante.

Ainda em novembro de 2020, o Superior Tribunal de Justiça (STJ) foi vítima de um ataque de *ransomware*[2] que paralisou as operações da corte por alguns dias. Segundo Bosco (2020), o hacker responsável por invadir o sistema do STJ criptografou todo o acervo de processos do tribunal, além de ter bloqueado o acesso às caixas de e-mail de ministros e *backups*.

O Brasil registrou aumento de 37% no número de ciberataques no terceiro trimestre de 2022 colocando em segundo lugar, no ranking como país mais atingindo por ciberataques na América Latina (DCIBER, 2023). Dentre os ataques registrados, destacam-se: roubo de identidade, dados, fraudes e extorsão, detecção de senha, violação de acesso, infiltração de sistema, navegadores web e privados, e roubo de propriedade intelectual ou acesso não autorizado. Em síntese, os ciberataques existem e são uma realidade cada vez mais presente na vida de todos, por isso, a prevenção é fundamental para o enfrentamento e combate ao problema (DCIBER, 2023).

1.4 Metodologia

Devido ao grau de sigilo das informações tratadas não será feita uma abordagem que caracterize especificamente possíveis ataques cibernéticos na Força Aérea Brasileira, nem estudo de caso. Desta forma, o referencial metodológico utilizado é a abordagem qualitativa, com método de pesquisa hipotético-dedutivo, por meio de pesquisa bibliográfica, exploratória, descritiva e documental.

A hipótese da pesquisa é que: Os modelos PRINCE2, PMBOK e de Três Linhas de Defesa contribuirão para a Força Aérea Brasileira aprimorar a gestão dos riscos cibernéticos relacionados aos ativos de Tecnologia da Informação. Foi estudado como é conduzida a gestão dos riscos associados aos ataques cibernéticos de uma forma geral e em seguida o foco da análise foi a gestão dos riscos cibernéticos dentro da Força Aérea Brasileira.

[2] Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.

No Capítulo 2 realizou-se um estudo bibliográfico e documental sobre guerra irregular, assimétrica e cibernética, assim como a evolução das guerras de 1ª a 4ª geração. Também foi realizado um estudo sobre os modelos PMBOK e PRINCE2 para identificar como eles tratam o tema gerenciamento de riscos cibernéticos. Finalizando o capítulo, foi explorada a avaliação de riscos cibernéticos segundo o modelo das Três Linhas de Defesa.

No Capítulo 3 foi conduzida uma análise sobre a estruturação da defesa cibernética, das Três Linhas de Defesa, do PMBOK, do PRINCE2, da segurança da informação e da garantia governamental da qualidade na Força Aérea Brasileira no que tange ao tratamento de incidentes cibernéticos e avaliação dos riscos cibernéticos.

No Capítulo 4 verificou-se se os processos empregados na FAB estão consoantes ou não com o preconizado nos modelos de Três Linhas de Defesa, PRINCE 2 e PMBOK tanto no tratamento de incidentes cibernéticos como na avaliação e gerenciamento dos riscos cibernéticos. Com essa análise buscar-se-á identificar as principais vulnerabilidades e pontos fortes de segurança.

2. Referencial Teórico e Modelos para tratamento e gerenciamento de riscos cibernéticos

Neste capítulo apresenta-se a progressão da defesa cibernética o qual no decorrer da evolução das guerras, subitem 2.1, e também como as metodologias de gerenciamento de projetos PRINCE2, PMBOK além do Modelo de Três Linhas de Defesa tratam a Avaliação de Riscos e em especial, os riscos cibernéticos.

O modelo PMBOK está detalhado no subitem 2.2. Basicamente o PMBOK, *Project Management Body of Knowledge* ou Corpo de Conhecimento em Gerenciamento de Projetos, em português, é um guia reconhecido e utilizado no campo do gerenciamento de projetos. Foi desenvolvido pelo *Project Management Institute* (PMI) e oferece um conjunto de melhores práticas, diretrizes e padrões para o gerenciamento de projetos. No contexto desse trabalho, essas práticas serão discutidas no domínio cibernético.

O modelo PRINCE2 está detalhado no subitem 2.3. O PRINCE2 significa *Projects IN Controlled Environments 2* ou Projetos em Ambientes Controlados 2, em português, é uma metodologia de gerenciamento de projetos amplamente utilizada, especialmente no Reino Unido e em outros países. Ela fornece um conjunto estruturado de princípios, processos e diretrizes para o gerenciamento de projetos. O PRINCE2 foi desenvolvido pela Office of Government Commerce (OGC) do Reino Unido e é uma abordagem flexível que pode ser aplicada a projetos de diferentes tamanhos e tipos. No contexto desse trabalho analisa-se esse modelo aplicado ao domínio cibernético.

O modelo das Três Linhas de Defesa está detalhado no subitem 2.4. Em linhas gerais, trata-se de um modelo de governança para se mitigar os riscos nas organizações. Foi lançado pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO[3]) aplicado pela ECIIA (*European Confederation of Institutes of Internal Auditing*) em conjunto com a FERMA (*Federation of European Risk Management Associations*) e utilizado pelo Tribunal de Contas da União do Brasil. Este modelo é utilizado como ferramenta de controle gerencial para se evitar erros, fraudes e tentativas de desvios que possam ameaçar as operações de uma organização de alguma forma. Atualmente, esse modelo vem também sendo discutido no campo cibernético.

[3] é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa.

A guerra é o ato de obrigar o inimigo a fazer nossa vontade. Clausewitz (1984) explica que para fazer oposição à força inimiga, precisa-se munir de invenções da arte e da ciência. Quanto mais arranjos, habilidades e técnicas forem desenvolvidos, mais preparado estará para a guerra. Trazendo essa perspectiva para o cenário contemporâneo, considerando as ameaças cibernéticas, é fundamental preparar estratégicas de defesa e é essencial explorar as vulnerabilidades cibernéticas inimigas. Negligenciar o aspecto cibernético implica em fornecer grande vantagem ao oponente em um confronto.

Para Clarke e Knake (2015, p.11) a guerra cibernética é definida como ações de um estado-nação para invadir computadores ou redes de outra nação com a intenção de causar danos ou transtornos. De acordo com Graça (2014), a guerra cibernética é uma atividade que não enxerga fronteiras e que não respeita sequer a declaração efetiva de guerra. Diante disso, Graça (2014) defende a necessidade da regulação da guerra cibernética para reforçar o Estado democrático de direito, equilibrando direitos assegurados pela Carta Magna, como o direito à privacidade, como meio de fortalecer a democracia brasileira. Jorge (2012) defende o "poder cibernético" – e de novas formas de guerra e espionagem – a "guerra cibernética" e a espionagem cibernética – como instrumentos para alcançar objetivos de política externa, exemplificando o caso do Estados Unidos no ataque cibernético ao Irã com a finalidade de atrasar o programa nuclear.

Portanto, entende-se que a guerra cibernética se define como o conjunto de procedimentos tomados por um Estado contra redes e sistemas computacionais de outro Estado pretendendo causar avarias ou parada de seus sistemas, colocando assim o ciberespaço como o novo campo de batalha. Dessa forma, quem possuir maior domínio do ciberespaço conseguirá mais poder.

Para Winter (2006), Maquiavel foi um dos grandes responsáveis pela noção moderna de poder. Winter (2006) traz a visão mais clara sobre Maquiavel apesar de muitos terem uma noção pejorativa sobre o termo maquiavelismo, pautado sobre o princípio de que os fins justificam os meios, logo o Príncipe poderia fazer qualquer coisa para se manter no poder. Winter (2006) mostra que as ações do governante estariam pautadas no bem coletivo e não nos interesses particulares, separando moral individual e moral política. Dessa forma, o que determina se uma atitude é ética é a sua finalidade política.

Nesse contexto, as ações cibernéticas de defesa e ataque são perfeitamente plausíveis e necessárias desde que estejam fundamentadas nos objetivos políticos de um Estado, e venham refletir no bem coletivo da sociedade. No caso, proteção de controles computacionais

ligados a pontos vitais do país como centro de abastecimento de água e energia, telecomunicações, transporte e infraestruturas aéreas críticas.

Fadok (2001) mostra que a teoria do conflito de Boyd e a teoria do ataque estratégico de Warden representam um deslocamento fundamental na evolução das ideias do poder aéreo estratégico, da ênfase na guerra econômica para a ênfase na guerra de controle. Dessa forma, a derrota do adversário pela paralisia estratégica atacando seus centros vitais seria essencial para uma vitória rápida e decisiva e não destruição por meio da aniquilação.

Segundo Fadok (2001), o Marechal Lord Trenchard da Royal Air Force (RAF) acreditava na paralisia estratégica. Argumenta que os ataques paralisantes aos "centros vitais" inimigos oferecem "o melhor objetivo pelo qual alcançar a vitória, porque conseguem "efeito infinitamente maior" e "geralmente exigem um custo muito menor do atacante" do que os ataques contra a superfície e às forças aéreas que a defendem". Para Fadok (2001), Mitchell compartilhava visão de paralisia estratégica semelhante. Segundo Fadok, Mitchell afirmou que o maior valor do bombardeio aéreo está em "golpear os grandes centros nervosos de um inimigo no início mesmo da guerra, de modo a paralisá-los o máximo possível".

Na guerra cibernética, tem-se uma situação semelhante. O objetivo é atingir os centros vitais do inimigo explorando as vulnerabilidades de seus sistemas e deixá-lo incapacitado de contra-atacar. A guerra cibernética explora um novo campo de batalha, que não implica necessariamente em baixas civis, desta forma pode ser utilizada como um recurso intermediário entre a diplomacia e o confronto.

Para Clausewitz (1984), "A guerra é a continuação da política por outros meios". Na guerra cibernética, tem-se uma nova perspectiva, o ciberespaço, consequentemente um novo meio para continuar a guerra antes de partir para o conflito armado.

Levy (1999) mostra que o ciberespaço é o suporte do desenvolvimento da inteligência coletiva porque possui um aspecto participativo, socializante, descompartimentalizante e emancipador que favorece a mutação técnica. Desta forma, a inteligência coletiva que favorece a cibercultura é ao mesmo tempo um veneno para aqueles que dela não participam. Portanto, o reconhecimento do ciberespaço como novo campo de produção de conhecimento e técnicas cibernéticas é fundamental para o preparo e adaptação ao novo cenário de guerra, mutante, imprevisível e rico em inovações tecnológicas.

Segundo Douhet (1988), não existem guerras iguais, sempre mudam, e é preciso preparar a defesa nacional para essas mudanças:

> […]na organização da defesa nacional, é necessário mudar completamente a linha da política, porque a forma de qualquer possível guerra futura será inteiramente diferente da forma das guerras anteriores.

2.1 Guerra irregular, guerra assimétrica, guerra de 4ª geração e guerra cibernética

Heydte (1990, p.37) define que a guerra irregular é normalmente conceituada como o conflito armado, no qual as partes não constituem grandes unidades, mas pequenos grupos de ação, e cujo desfecho não é decidido em poucas e grandes batalhas, mas sim concretizado por meio de um número muito grande de pequenas operações individuais, roubos, atos de terrorismo e sabotagem, bombardeios e incursões. Desta forma, a guerra irregular poderia ser entendida como a "guerra das sombras".

Para Visacro (2009, p.12) a guerra irregular é todo conflito conduzido por uma força que não dispõe de organização militar formal e sobretudo, de legitimidade jurídica institucional, ou seja, é a guerra travada por uma força não regular. Visacro (2009, p.31) mostra a abrangência dispersa do conceito de guerra irregular como uma guerra de caráter informal, dinâmico, flexível e mutável do combate. Nesse sentido, aponta uma série de termos e definições de uso comum, como "pequena guerra" (*kleinkrieg*), "guerra de partisans" (*partisan warfare*), "guerra não convencional" (*unconventional warfare*), "guerra irregular" (*irregular warfare*) e "conflito de baixa intensidade" (CBI). Com o intuito e dar-lhe uma conotação atual, Visacro (2009, p.31) explica que a maioria dos autores tem empregado a expressão "conflito assimétrico" na definição de guerra irregular.

Carr (2009, p.194) explica que dada à facilidade com que qualquer indivíduo pode adquirir as ferramentas necessárias para realizar um ataque cibernético anonimamente, os ataques cibernéticos fornecem aos inimigos de um Estado uma ferramenta ideal para realizar uma guerra assimétrica. Carr (2009, p.194) complementa explicando que Estados e terroristas estão cada vez mais se voltando para ataques cibernéticos para fazer guerra contra seus inimigos.

Heydte (1990, p.39) afirma que a guerra é uma forma de fazer política porque ela é sempre uma luta pelo poder. Este é uma influência ampliada o bastante para induzir outros a se submeterem, voluntariamente ou mediante à compulsão, à vontade de quem exerce esta influência (Heydte, 1990, p.39). Nesse sentido a guerra convencional se caracteriza pelo emprego da força militar na resolução de um conflito entre Estados (Heydte 1990, p.41).

No que tange à guerra irregular, Heydte (1990, p.42) acredita que ela pode acontecer como guerra civil, na qual grupos lutam pelo poder no âmbito de um país. Já na arena

internacional, a guerra irregular pode ocorrer como uma forma de conflito armado entre um certo número de nações. Para o autor a guerra irregular também pode anteceder à guerra convencional, funcionando tanto para desgastar um oponente antes da irrupção de hostilidades convencionais como para negar ao adversário posições vantajosas.

Nesse contexto, Heydte (1990) volta-se para a estratégia, explicando que se trata da arte da correta demonstração de poder, que pretende provocar uma determinada reação psicológica no adversário para alcançar um objetivo político. Complementa dizendo que a estratégia militar não é necessariamente uma estratégia de guerra, a arte real da estratégia militar consiste em alcançar o objetivo político procurado sem recorrer à guerra e sim por meio de uma exclusiva demonstração do poder militar.

Dessa forma, no contexto da estratégia militar como da estratégia da guerra, Heydte (1990, p.70) explica que a ameaça da guerra irregular ou a sua efetiva condução deve levar o adversário a ser induzido a se comportar do modo como quem o ameaça deseja, sob pena de ver desencadeada a guerra irregular.

Para Heydte (1990, p.77), a luta pela motivação no âmbito do arsenal psicológico desempenha um papel importante na guerra convencional e na guerra irregular essa luta é decisiva. O guerrilheiro nada sabe sobre a sistemática de suprimentos, de posições preparadas, de recompletamento. Nessa situação, em meio ao perigo que o persegue, ele se agarra à ideia pela qual luta.

Heydte (1990, p.103) explica que na guerra irregular, todos os habitantes de um Estado são combatentes potenciais. Em uma guerra convencional, soldados combatem soldados. Na guerra irregular, ao contrário, grupos confrontam-se uns aos outros que são fundamentalmente contrários aos seus objetivos estratégicos.

A guerra irregular é, em primeiro lugar, o combate de soldados isolados ou em pequenos grupos. Heydte (1990, p.106) esclarece que a guerra irregular é concretizada por meio da multiplicação de atos isolados de violência, estes atos, na condição ideal são distribuídos por todo o território do Estado contra quem a guerra irregular é conduzida. Observa-se que a guerra irregular não possui frente nem campos de batalhas limitados, sua frente está em toda parte e o terreno de batalha está constantemente se modificando.

Enquanto na guerra convencional as unidades ocupam uma faixa do terreno e fazem movimentos para frente ou para a retaguarda, os guerrilheiros não ocupam uma área, eles a "contaminam". A contaminação significa limitar a liberdade de ação do inimigo na extensão mais ampla possível da área, por meio de um número crescente de ações de guerra irregular

como: atos de sabotagem em escalada, especialmente contra itinerários de transporte, ataques a instalações de passagem obrigatória, veículos isolados em deslocamento, pequenas colunas de suprimento e mediante o terror contra a população civil (Heydte, 1990, p.107).

Ressalta-se a dificuldade em determinar o começo de uma guerra irregular por causa da natureza de subversão violenta que ela busca ocultar, ou seja, a existência de um estado de guerra. O Estado, por razões políticas, buscará minimizar o cenário de guerra, tentando evidenciar uma situação de normalidade e continuidade da existência do estado de paz e levará algum tempo para reconhecer um cenário de conflito (Heydte, 1990, p.116).

Visacro (2009, p.39) explica que a primeira geração da guerra moderna está compreendida entre o término da Guerra dos Trinta Anos, em 1648 e a era napoleônica, ou seja, são as guerras pré-industriais. Para o autor, essas guerras foram caracterizadas pelo combate linear, por formações cerradas, ordem unida e batalhas campais que se assemelhavam a paradas e desfiles militares, com toques de clarins e estandartes desfraldados. Visacro (2009, p.39) explana que o valor combativo de uma tropa podia ser medido pelo modo como desfilava ou como se portava em forma. Visacro explica que para os soldados de primeira geração, a disciplina reduzia-se à rígida obediência às ordens emanadas dos escalões superiores e podia ser expressa por gestos e saudações formais. No período da primeira geração de guerras não se cogitava em Poder Aeroespacial porque não ainda era uma época pré-industrial.

Visacro (2009, p.40) explica que a Revolução Industrial, em meados do século XIX, deu origem à segunda geração das guerras. Aponta que foi durante a Primeira Guerra Mundial (1914-1918) que a guerra de segunda geração atingiu seu ápice, sendo caracterizada pela ascendência do sistema de apoio de fogo sobre a manobra. O autor descreve que ocorreu uma defasagem entre a tecnologia e a tática, prevalecendo a "guerra de atrito", e a defesa como forma de guerra mais forte além de uma sensível perda de mobilidade tática. Visacro (2009) complementa detalhando que a batalha permaneceu linear, seguindo padrões formais de planejamento e métodos rígidos de execução, com o propósito de concentrar o máximo poder relativo de combate e cercar sobre o inimigo para destruí-lo.

Nesse período da 2ª geração das guerras, Doueht ficou impressionado pelos sangrentos combates da Primeira Guerra Mundial e defendia que somente o avião poderia sobrepor-se à extensa guerra de atrito provocada pelos exércitos equipados com armas modernas, ou seja, a supremacia aérea significaria a vitória (Brasil, 2012a, 21). A fórmula de vitória preconizada por Douhet pode ser assim descrita: obtenção da supremacia aérea,

neutralização dos centros vitais estratégicos do inimigo e manutenção da defensiva na superfície enquanto fosse construída a ofensiva pelo ar (Brasil, 2012a, 21).

Mitchell preconizava que a força aérea deveria conduzir operações aéreas independentes, como o bombardeio estratégico, preocupando-se com objetivos próprios e não somente com ações de apoio (Brasil, 2012a, p.23). Tais convicções viriam a servir de suporte doutrinário para a Força Aérea norte-americana. Para Mitchell, a primeira missão do Poder Aeroespacial deveria ser a destruição da força aérea inimiga e, em seguida, viria o bombardeio aos centros vitais (Brasil, 2012a, p.24). Dado o caráter de "destruir forças militares do inimigo" como principal objetivo de batalha, seu modelo e expressão preponderante no campo militar assim como verbo de combate sendo "destruir", as ideias de Mitchell podem ser categorizadas como pertencentes à 2ª geração das guerras.

Visacro (2009, p.41) explica que a guerra de terceira geração representou um renascimento da tática e um retomo à mobilidade. O autor mostra que nesse tipo de guerra, a liberdade de ação, iniciativa, flexibilidade de raciocínio, discernimento tático, senso de oportunidade e capacidade de decisão tornaram-se atributos mais importantes que a disciplina formal e o rígido ordenamento das forças que caracterizavam as duas gerações anteriores. Visacro (2009, p.42) complementa que as unidades dessa geração de guerra eram capazes de operar em profundidade com rapidez e independência, como unidades blindadas, de paraquedistas ou de assalto aéreo.

No contexto dos tipos de guerras, as ideias defendidas por Trenchard se encaixam na guerra de 3ª geração porque acreditava que o avião era uma arma ofensiva estratégica, que poderia atingir, pela destruição da indústria do inimigo, o moral de trabalhadores de fábricas e, por extensão, da população como um todo (Brasil, 2012a, p.24). Entretanto, ao contrário de Douhet, Trenchard não era adepto da ideia de que uma campanha aérea poderia, sozinha, trazer a vitória na guerra. Logo, Trechard defendia um modelo de "guerra relâmpago" em que o campo de batalha é não linear e o objetivo da batalha consiste e causar o colapso das forças inimigas da retaguarda para frente caracterizando o enquadramento de suas ideias na guerra de 3ª geração.

Após uma análise detalhada sobre a Batalha da Inglaterra, primeira grande campanha conduzida apenas com o emprego do Poder Aeroespacial, que resultou em um fracasso alemão, Seversky apontou erros que deveriam ser evitados pelos planejadores militares, a saber: não neutralizar o Poder Aeroespacial antagonista antes de efetuar bombardeios estratégicos; escolher erradamente os objetivos vitais a atingir; e empregar o Poder

Aeroespacial de forma descontinuada. Essas descobertas apontam que Seversky tinha princípios alinhados à guerra de 3ª geração (Brasil, 2012a, p.24).

Após a Primeira Guerra Mundial, os autores Basil H. Liddell Hart e J. F. C. Fuller, desenvolveram um conceito que ficou conhecido como "paralisia estratégica", (Brasil, 2012a, p.27). Esse conceito, baseado no princípio da economia de forças, estabelece que se deve aplicar o mínimo de esforço para produzir o máximo de efeito contra o inimigo, pela ação em três esferas da guerra: física, moral e mental. A "paralisia estratégica" buscaria o desarme físico do inimigo (em vez de sua destruição), o que o deixaria mentalmente desnorteado e o conduziria a um colapso moral. Estes conceitos direcionam para uma "guerra relâmpago", modelo característico da guerra de 3ª geração (Brasil, 2012a, p.27).

Visacro (2009, p.43) explica que a guerra de 4ª geração é decidida nos níveis operacional, estratégico, mental e moral, ao invés dos níveis tático e físico. O autor caracteriza a guerra de 4ª geração como a guerra do futuro em que "não serão grandes mudanças em como o inimigo combate, mas quem estará lutando e para quê". Ele destaca que na guerra de 4ª geração, o mundo estará com suas culturas em conflito, com significativa participação de atores não estatais, apontando algumas características dessa guerra (Visacro, 2011, p.53).

> [...] os atores não estatais usam diferentes ferramentas não se restringindo ao que reconhecemos como sendo forças militares.
> [...] no seu fundamento se encontra uma crise universal da legitimidade do Estado
> [...] em todo o mundo, os militares se encontram combatendo oponentes não estatais tais como a Al Qaeda, o Hamas, o Hezbollah e as Forças Armadas Revolucionárias da Colômbia.

Crimes transfronteiriços, terrorismo internacional, fluxos migratórios, pressão demográfica, urbanização incontida, fortalecimento de identidades étnicas, globalização e questões ambientais são apenas alguns dos componentes desse intrincado mosaico da guerra de 4ª geração, esclarece Visacro (2011, p.54). As quatro gerações da guerra moderna são resumidas no Quadro 1.

Quadro 1 - Quadro comparativo: as quatro gerações da guerra moderna

	GUERRA MODERNA			
	1ª Geração	**2ª Geração**	**3ª Geração**	**4ª Geração**
Contexto histórico	Pré-industrial	Industrial		Pós-industrial
Protagonistas	Atores estatais			Atores estatais e não estatais
Campo de batalha	Linear		Não linear	Não contíguo Indefinido Difuso
Modelo	Guerra metódica (guerra científica)		"Guerra relâmpago"	"Guerra Irrestrita"
Objetivo da batalha	Subjugar o exército oponente	Destruir as Forças militares do inimigo	Provocar o colapso das Forças inimigas da retaguarda para frente	Auferir resultados psicológicos Afetar a opinião pública
Natureza do objetivo	*Física*: terreno e unidades de linha do inimigo		*Física*: sistemas de apoio logístico e de comando e controle. *Psicológica*: decisores militares.	*Psicológica*: decisores políticos e opinião pública
Expressão preponderante	Campo militar			Campo psicossocial
Relação fogo-manobra	Ascendência da manobra sobre o poder de fogo	Ascendência do poder de fogo sobre a manobra	Equilíbrio entre o poder destrutivo e a capacidade de manobra	Irrelevante, pois o que conta é o efeito psicológico da ação
Verbo que tipifica o combate	Marchar Manobrar	Destruir	Avançar	Influenciar
Indicadores mensuráveis da vitória	Estandartes, trens e bocas de fogo aprisionadas	Terreno conquistado e "contagem de corpos" (*body counts*)	Quilômetros percorridos por dia dentro do território inimigo	Espaço na mídia e aceitação popular
Comando e controle	Ações centralizadas (planejamento e execução)		Ações descentralizadas	Ações independentes
Atributos decisivos	Ordem e disciplina		Senso de oportunidade e iniciativa	
Exemplos	Guerras Napoleônicas	1ª Guerra Mundial Campanha aliada durante a 2ª Guerra Mundial Operações de busca e destruição realizadas pelos EUA no Vietnã	2ª Guerra Mundial (*Blitzkrieg* alemã) Campanhas israelenses em 1956, 1967 e 1973	- Atentados da Al Qaeda em Nova York, Washington, Madri e Londres. - Combates travados entre as Forças de Defesa de Israel e o Hezbollah, no Líbano, no verão de 2006.
Personagens e entidades	George Washington Frederico, o Grande Napoleão Bonaparte	Carl Von Clausewitz Ferdinand Foch Ludendorff W. Westmoreland	J. F. C. Fuller Liddell Hart Heinz Guderian Erwin Rommel	Al Qaeda Hezbollah Hamas FARC

Fonte: Visacro (2011, p.54)

Visacro (2011, p.54) indica a tecnologia da informação como a precursora dos riscos cibernéticos modernos para um Estado. Para ele, a tecnologia da informação, que permite o fácil estabelecimento de conexões entre redes globais de cooperação, aliada à busca por formas alternativas de financiamento tem aproximado facções extremistas e organizações criminosas ligadas, sobretudo, ao tráfico internacional de drogas e de armas e à lavagem de dinheiro. Portanto, tornou-se necessário reavaliar os preceitos de segurança e defesa, indo muito além da simples capacitação de Forças convencionais para a contrainsurgência.

No âmbito da tecnologia da informação, Carr (2009, p. 2) define a guerra cibernética como "... a arte e a ciência de lutar sem lutar; de derrotar um oponente sem derramar seu sangue". Segundo o autor, a Comissão Europeia recomenda, como medidas de segurança, um foco maior em áreas-chave para combater futuras ameaças no ciberespaço. Essas medidas incluem:

> *Preparação e prevenção:* Promover a cooperação de informações e a transferência de boas práticas políticas entre os Estados membros por meio de um Fórum Europeu que Estabelece uma Parceria Público-Privada Europeia para a Resiliência, que ajudará as empresas a compartilhar experiências e informações com autoridades públicas.
> *Detecção e resposta:* Apoiar o desenvolvimento de um sistema europeu de compartilhamento e alerta de informações.
> *Mitigação e recuperação:* Estimular uma cooperação mais forte entre os Estados membros por meio de planos de contingência nacionais e multinacionais e exercícios regulares para resposta em larga escala a incidentes de segurança de rede e recuperação de desastres.
> *Cooperação internacional:* Conduzir um debate em toda a Europa para definir as prioridades da UE para a resiliência e estabilidade a longo prazo da Internet, com o objetivo de propor princípios e diretrizes a serem promovidos internacionalmente.
> *Estabelecer critérios para a infraestrutura crítica européia no setor de tecnologias da informação e comunicação (TIC):* Os critérios e abordagens atualmente variam entre os Estados membros.

O ciberespaço pode ser definido como um meio virtual, muito menos tangível que o solo, a água, o ar ou mesmo o espaço e o espectro de Radiofrequência-RF. Uma maneira de entender o ciberespaço em geral e os ataques cibernéticos em particular, é vê-lo como constituído por três camadas: a camada física, uma camada sintática acima do físico e uma camada semântica no topo (Libicki, 2009, p.12).

Segundo Libicki (2009, p.12), todos os sistemas de informação assentam em uma camada física que consiste em caixas e (às vezes) fios. Explica que é possível atacar um sistema de informação por meios cinéticos, basta apenas acrescentar que um computador não pode ser enganado destruindo seus componentes (embora possa ser por meio da substituição de um componente por outro).

Libicki (2009, p.12) explica que o nível sintático contém as instruções que os designers e os usuários fornecem à máquina e os protocolos por meio dos quais as máquinas interagem entre si - reconhecimento de dispositivo, enquadramento de pacotes, endereçamento, roteamento, formatação de documentos, manipulação de banco de dados, etc. Esse é o nível no qual o *hacking* tende a ocorrer, pois pessoas externas procuram reivindicar sua própria autoridade sobre a de designers e usuários (Libicki, 2009, p.12).

Libicki (2009, p.12) acredita que a camada superior, a camada semântica, representa as informações que a máquina contém - a razão pela qual os computadores existem em

primeiro lugar. Algumas informações, como tabelas de pesquisa de endereços ou códigos de controle da impressora, destinam-se à manipulação do sistema. Nesta camada, explica Libicki (2009, p.12), muitos truques de hackers inserem instruções sob o disfarce de conteúdo; os exemplos incluem anexos que contêm vírus, endereços excessivamente longos que criam estouros de buffer enviando os bits extras para o fluxo de processamento e páginas da Web com código incorporado.

A guerra cibernética tem objetivos externos e internos. Libicki (2009, p.117) destaca que o objetivo externo é a razão da guerra cibernética em primeiro lugar. Para o autor, o objetivo interno se refere a gerenciar o próprio combate (pará-lo, limitar seu escopo) e evitar a escalada para a violência. Observa-se que um objetivo que a guerra cibernética não pode ter é desarmar e muito menos destruir o inimigo.

Na ausência de combate físico, a guerra cibernética não pode levar à ocupação de territórios, e como a guerra cibernética não pode desarmar guerreiros cibernéticos, estaria em vantagem, quem conseguisse saturar a capacidade de resposta do inimigo (Libicki, 2009, p.118).

A narrativa até agora sugere as muitas ambiguidades que acompanham o conflito no ciberespaço, Libicki (2009, p.121) exemplifica essas ambiguidades: dúvidas sobre a capacidade de descobrir quem fez o que (ocultação de evidências), efeitos de armas (tanto prospectivas quanto retrospectivas), tempo de recuperação, capacidade de continuar linhas de ataque semelhantes, falhas em cascata (ou a falta delas), capacidade de contornar danos ou ações de terceiros.

Resultados altamente assimétricos são possíveis: um estado faminto pode mobilizar pessoas inteligentes o suficiente para causar sérios danos a um estado mais rico e de alta tecnologia, mas que depende mais de suas informações. Agressões semelhantes no espaço real levariam à derrota esmagadora dos menores pelos maiores (Libicki, 2009, p.121).

Singer e Friedman (2014, p.148) explicam que uma “avaliação de ameaças” é o processo de ponderar os riscos que qualquer entidade enfrenta, seja uma nação, uma empresa ou mesmo um indivíduo. Para os autores, uma avaliação adequada das ameaças, consideram-se essencialmente três fatores básicos:

> A viabilidade dos adversários serem capazes de identificar e explorar suas vulnerabilidades, o efeito que aconteceria se eles pudessem tirar proveito dessas vulnerabilidades, e, finalmente, a probabilidade de que eles, de fato, estejam dispostos a fazê-lo.

Ao realizar uma avaliação de riscos, a tendência natural e de sua superestimação. Singer e Friedman (2014, p.148) afirmam que esta superestimação provoca o que eles descrevem como "ameaça de inflação". Trata-se do não conhecimento dos riscos exatos, assunção do pior caso e apesar de parecer sensato, pode perder muito tempo e energia preocupando-se com riscos cibernéticos que não são reais.

A natureza das vulnerabilidades no ciberespaço torna sua avaliação difícil. Singer e Friedman (2014, p.150) explicam que o próprio termo “dia zero”[4] ilustra o problema no ciberespaço, as vulnerabilidades mais frequentemente visadas são aquelas que ninguém, exceto o atacante, conhece.

Hoje, a guerra cibernética se coloca no horizonte dos novos conflitos entre os Estados. Deve ser estudada e detalhada a fundo, pois sua desconsideração pode implicar em grandes desvantagens em uma guerra no futuro.

A China tem buscado consolidar sua posição de poder no Leste Asiático. Sua modernização militar demonstra sua ascensão de poder na região ameaçando o poder dos Estados Unidos. De acordo com Dornelles Jr. (2014), a modernização do Exército de Libertação do Povo (ELP) mudou sensivelmente a distribuição de poder no Leste Asiático em favor da China. Para Dornelles:

> O ELP é capaz de degradar seriamente a capacidade de combate das forças estadunidenses em uma guerra marítima (convencional), por meio de operações de cunho assimétrico, apoiadas em suas capacidades aeronavais, missilísticas e informacionais.

Dentre as várias tecnologias demonstradas por Dornelles Jr.(2014), a China faria operações de Antiacesso (A2) e Negação de Área (AD) precedidas por ataques cibernéticos:

> [...]essas três dimensões das operações de A2/AD seriam precedidas por ataques ao sistema de C4ISR das forças estadunidenses localizadas no teatro de operações. Inicialmente, a rede de computadores inimiga seria atacada pelo ELP por meio de guerra cibernética, isto é, ataques de vírus, poluição de informação, coleta de informações etc. Essa etapa seria coordenada com ataques aos principais nós móveis da cadeia de comando, controle e comunicação das forças estadunidenses, ou seja, tais ataques seriam dirigidos contra os satélites inimigos, bem como seus porta-aviões e suas aeronaves de AWACS.

De acordo com este estudo as ações cibernéticas seriam essenciais para a tomada do poder na região do Leste Asiático pela China. Clarke e Knake (2015, p.2) esclarecem que os EUA possuem um Comando Cibernético, uma organização militar com a missão de utilizar

[4] vulnerabilidade nova, Zero-day attack ou ataque de dia zero é o termo usado para descrever uma vulnerabilidade de segurança desconhecida em um software.

a Tecnologia da Informação como arma. Nações como Rússia, China dentre outras possuem um comando militar semelhante.

O ataque à instalação nuclear da Síria e a atividade cibernética dos Estados Unidos que precedeu a invasão do Iraque são exemplos do uso militar de *hacking*[5] como ferramenta para auxiliar em um tipo de guerra convencional, em que o uso do espaço cibernético precedeu um bombardeio e uma destruição de tanques, respectivamente.

Em 2007 ocorreu a Noite de Bronze em Tallin, capital da Estônia. A remoção da estátua do Exército Vermelho russo que combateu nazistas na Segunda Guerra Mundial provocou alvoroço entre os que apoiavam a derrubada do monumento e os que não apoiavam. Segundo Milhazes (2007), os primeiros eram naturais da Estônia, cerca de 67%, afirmavam que o Exército Vermelho não havia libertado dos nazistas em 1945 e sim imposto uma nova ditadura. Do outro lado, cerca de 31% da população, eram russos, ucranianos e bielorrussos que defendiam a permanência da estátua do Monumento ao Combatente Libertador e consideravam um sacrilégio sua remoção. O fato é que o monumento foi desmontado e reconstruído em um cemitério militar. Após a desmontagem do monumento o conflito mudou para o ciberespaço.

De acordo Clarke e Knake (2015, p.16), a Estônia é um país altamente conectado, competindo com Coréia do Sul, e bem à frente dos Estados Unidos na utilização de aplicações de Internet e na penetração da banda larga na vida cotidiana. Isso fez com que se tornasse um alvo perfeito para um ataque cibernético. Imediatamente após o conflito da Noite de Bronze, os servidores que hospedavam as páginas mais utilizadas na Estônia foram inundados por pedidos de acesso. Dessa forma os estonianos não podiam acessar seus bancos on-line, os sites de seus jornais ou serviços eletrônicos do governo.

Clarke e Knake (2015) mostram que a Estônia passou a sofrer um Ataque Distribuído de Negação de Serviço (DDoS), o maior já visto até o momento. Os serviços de segurança russos haviam encorajado a mídia nacional a insuflar o sentimento patriótico contra a Estônia. Não é exagero imaginar que eles também tenham solicitado a grupos do crime organizado que "hackeassem" os sistemas estonianos. As autoridades russas sempre negaram os ataques cibernéticos, no entanto, nada fizeram para colaborar nas investigações da origem dos ataques quando foram solicitados, mesmo que tudo indicava que vinham de território russo.

Outro fato importante relatado por Clarke e Knake (2015, p.20) se refere ao conflito na Geórgia, na disputa pelos territórios de Ossétia do Sul e Abkházia. Ossétia do Sul e

[5] Penetração em um sistema computacional por meio da exploração de suas vulnerabilidades

Abkházia eram territórios pertencentes a Geórgia, mas que a partir de 2008 fugiram de seu controle. A partir de então, teve início uma série ataques entre estes territórios, apoiados pela Rússia e a Geórgia. No mesmo momento que o exército russo avançava, avançava também a força cibernética. O objetivo era impedir que os georgianos percebessem o que estava acontecendo, então eles realizaram ataque de DDoS em meios de comunicação e sites do governo da Geórgia. Os acessos a sites como CNN e BBC também foram bloqueados. Diante dos ataques, o sistema bancário paralisou, assim como de cartões de crédito e de telefonia móvel. A França mediou um acordo de paz em que a Ossétia do Sul e a Abkházia foram reconhecidas como estados independentes. Uma força de segurança internacional ocuparia o vácuo de segurança, o que não aconteceu, e os estados declarados independentes convidaram os russos a ficar.

Segundo Clarke e Knake (2015, p.22), nos episódios da Estônia e Geórgia, na verdade, os russos demonstraram bastante moderação no uso de armas cibernéticas e guardaram as melhores armas para um conflito que envolvesse a OTAN e os Estados Unidos.

A Coreia do Norte não tem investido no desenvolvimento de infraestrutura interna de Internet, mas tem investido esforços para prejudicar a infraestrutura de outros países. De acordo com Clarke e Knake (2015, p.27):

> A *Lab 110*, (...) é apenas uma das quatro unidades de guerra cibernética da Coreia do Norte. A unidade Conjunta de Guerra Cibernética do *Korean People's Army* (KPA), Unidade 121, tem mais de seiscentos *hackers*. O Departamento Secreto para Guerra Psicológica e Cibernética Inimiga, Unidade 204, possui cem *hackers* e é especializada em elementos cibernéticos para guerra de informação. O Departamento Central de Investigação do Partido, Unidade 35, é a unidade cibernética menor, mas altamente capaz, com funções de segurança interna e capacidade ofensiva externa cibernética. A Unidade 121 é a maior e mais bem treinada (...) é especializada em desabilitar as redes de comunicação, comando e controle militares da Coreia do Sul.

Vários países já se envolveram em conflitos cibernéticos e muitos vêm se preparando para este novo campo de batalha. As armas cibernéticas utilizadas até agora foram relativamente primitivas, com algumas exceções, levando a supor que as armas sofisticadas estão sendo guardadas para um conflito mais oportuno. A guerra cibernética é real e os Estados Unidos e outras nações poderiam devastar uma nação em uma guerra cibernética.

Para mapear os diversos tipos de ataques recorrentes e constantes pode-se modelar cenários de ataques cibernéticos identificando causas, relacionamentos e propondo soluções. Segundo Cheung et al. (2003), na modelagem de ataques cibernéticos existem definições básicas que são fundamentais no entendimento destes cenários. A primeira é a vulnerabilidade, definida como a condição em um sistema que pode violar explícita ou

implicitamente a política de segurança do sistema. A segunda é o *exploit* ou "façanha", definida como exploração de um único passo (atômico) de uma única vulnerabilidade. A terceira é o *Attack step* ou passo de ataque, definido como uma exploração ou outra atividade realizada por um adversário como parte de uma campanha em direção ao objetivo deste adversário. A quarta é *Composite Attack* ou Ataque Composto, definido como uma coleção de *Attack step* para atingir um determinado objetivo. Os autores deixam claro que o objetivo da modelagem de ataques não é fornecer detalhes de como cada ataque pode ser realizado, mas sim enfatizar como os ataques podem ser detectados e relatados.

Cheung et al. (2003) mostram que na modelagem é preciso identificar como um Ataque Composto em um cenário de ataque pode ser decomposto em diversos ataques menores de forma a ter subobjetivos compondo um macro objetivo. Outro fator importante na modelagem de cenário é a detecção dos ataques, a partir da observação de certos exemplos ou certos estados dos sistemas ou até mesmo por meio de inferências. E por fim é fundamental estabelecer relacionamento entre os ataques, sejam eles temporais (que precisam de uma sequência de execução no tempo para atingir o efeito esperado) ou ataques de pré-requisitos, que habilitam uma vulnerabilidade para que possa ocorrer outro de maiores proporções.

A guerra cibernética é um assunto global porque, virtualmente, no momento em que servidores e computadores no mundo todo estão passíveis de serem invadidos, rapidamente vários países são envolvidos. Betz e Stevens (2012, p.4) mostram, como uma primeira característica, que em termos gerais, o ciberespaço permite obscurecer a identidade e a localização de atores, por causa da sua arquitetura física e protocolos de software que permitem o uso fácil de *proxies* relativamente difíceis de penetrar ou revelar.

Uma segunda característica evidenciada pelos autores é que o ciberespaço aumenta radicalmente a velocidade, volume e alcance das comunicações, não apenas de Estados, mas também de cidadãos que querem se comunicar, quase que instantaneamente e com uma segurança razoável usando uma variedade de mídias de textos a vídeos. A terceira característica é a capacidade de expansão do ciberespaço, as barreiras de acesso diminuem a medida em que dispositivos com capacidade de conexão à Internet se disseminam.

Considerando as três características, verifica-se que a internet é análoga um campo de batalha aumentado exponencialmente. Pode ser uma plataforma para alcançar os objetivos de qualquer ator que a manipule com mais eficiência. De acordo com Singer e Brooking (2018, p.261) a batalha na internet é contínua, o campo de batalha é contíguo e a informação

que produz é contagiosa porque o que mais importa online é a atenção e engajamento dos internautas.

É por meio das redes informáticas que são cometidos crimes de natureza cibernética. Gomes (2000) explica que algumas irregularidades são feitas contra o computador e outras são feitas “através” da máquina. É mais tarde que surge o cibercrime. No Brasil, o Projeto de Lei 89/2003, conhecido como Lei Azeredo, tem como um de seus principais pilares obrigar os provedores de internet a manterem um arquivo com as informações de acesso de seus usuários por até três anos. Isso visa proteger as empresas que conquistam o direito de quebrar o sigilo telefônico de hackers e acabam esbarrando em questões burocráticas dos provedores, que hoje apagam esses logs de acesso quando querem - por vezes, antes que os trâmites judiciais deem um parecer, seja ele favorável ou não.

Como aponta Ferreira (2011), assim como criminosos usam armas e/ou explosivos para cometer crimes, sistemas ou computadores também são ferramentas utilizadas por criminosos. O Google Threat Analysis Group (TAG) anunciou que pesquisadores da área de segurança de dados estavam sendo alvos de ataques por um grupo da Coreia do Norte. Operadores de usinas nucleares ucranianas também denunciaram um grande ataque cibernético russo em seu site, enquanto o Kremlin apontou "sabotagem" na explosão de um arsenal militar na Crimeia. A estatal ucraniana disse que o ataque cibernético contra o Energoatom "veio do território russo" e foi "o ataque mais poderoso desde o início da invasão".

Na guerra da informação, um evento só carrega poder se as pessoas também acreditarem que ele aconteceu. Singer e Brooking (2018, p.262) explicam que a natureza desse processo significa que um evento fabricado pode ter poder real, enquanto um evento comprovadamente verdadeiro pode se tornar irrelevante. A política assumiu elementos de guerra de informação, enquanto o conflito violento é cada vez mais influenciado pela opinião *online*.

Singer e Brooking (2018, p.262) explicam que aqueles que deliberadamente facilitam os esforços do inimigo, seja fornecendo um megafone para grupos terroristas ou espalhando desinformação conscientemente, especialmente de ofensivas de governos estrangeiros, devem ser vistos pelo que são. Eles não estão mais apenas lutando por sua marca pessoal ou por seu partido político, mas sim ajudando e incentivando inimigos que buscam prejudicar toda a sociedade.

Segundo Vasconcelos (2022) o WikiLeaks é uma organização de divulgação de documentos e informações fundada em 2006 por Julian Assange. Essa organização ganhou

destaque por expor informações confidenciais e sigilosas de governos, corporações e outras entidades. O WikiLeaks opera uma plataforma online onde pessoas com acesso a documentos sensíveis podem vazar e divulgar esses documentos de forma anônima.

De acordo com Vasconcelos (2022) o WikiLeaks se tornou amplamente conhecido por vazar uma série de documentos importantes e sensíveis, contendo uma grande quantidade de documentos classificados do governo dos Estados Unidos, incluindo comunicações diplomáticas e relatórios militares.

Zendron (2023) explica que só no Brasil, no ano de 2022, mais de 100 bilhões de tentativas de ataques cibernéticos foram contabilizadas, tornando o país o segundo mais atingido na América Latina. A maioria dos crimes cibernéticos foi motivada financeiramente e compreendia o uso de *ransomware* ou scripts maliciosos, revelando que este é um dos ataques mais comuns. Os investimentos em cibersegurança aumentaram no Brasil depois da pandemia, mas ainda estão aquém do necessário (ZENDRON, 2023):

> Depois da pandemia, o cenário de investimentos nacional em segurança da informação até começou a mudar, visto que muitas empresas tiveram que passar por massivos processos de digitalização. Porém, as ações atualmente correspondem a apenas 10% dos investimentos totais em tecnologia. Em países da América do Norte ou da Europa, as empresas costumam destinar entre 25% e 30% do orçamento de tecnologia para práticas e ferramentas de cibersegurança.

No contexto da Lei Geral de Proteção de Dados (LGPD), independentemente de as empresas terem ou não instalados nas máquinas os melhores pacotes antivírus do mercado, elas são alvos em potencial, pois os hackers estão sempre criando novas estratégias para cometer crimes cibernéticos (DCIBER, 2023). A violação de dados resulta em dois prejuízos graves: primeiro porque, as informações confidenciais são vendidas na *dark web* ou a terceiros. Em segundo lugar, a Lei Geral de Proteção de Dados (LGPD) prevê sanções para vazamento de dados. A norma visa que as empresas adotem métodos eficazes para garantir a segurança dos dados. Dependendo do caso, um vazamento pode ser considerado uma infração e a empresa terá que pagar uma multa de 2% de sua receita, a qual pode chegar ao teto de R$ 50 milhões para quem não definir protocolos claros para a proteção de dados pessoais de consumidores e funcionários.

É nesse ambiente de cibersegurança que a aviação opera. A aviação depende muito da tecnologia de rede, que é usada para aumentar a segurança e a eficiência do transporte aéreo. No entanto, a interconectividade dos sistemas e a dependência da tecnologia criaram

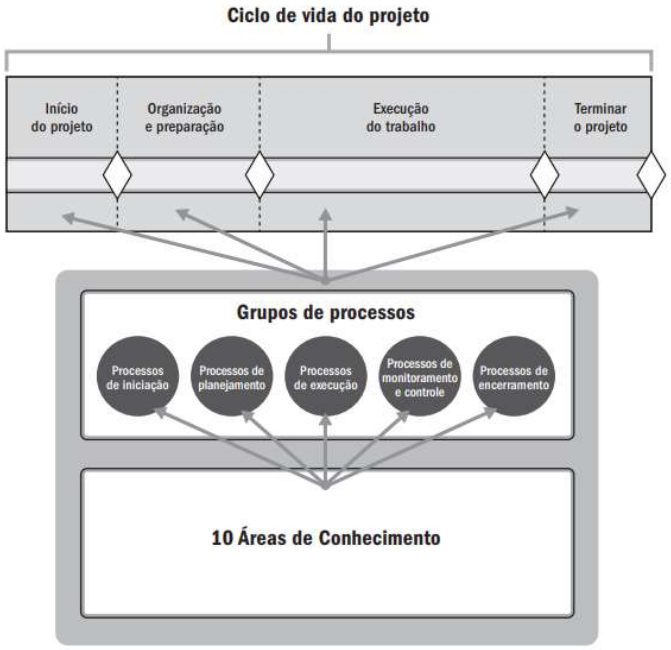
condições ideais para o surgimento de novos riscos. A indústria da aviação usa uma vasta gama de sistemas de computadores interconectados, desde sistemas de navegação aeronáutica, sistemas de comunicação e controle de aeronaves, sistemas terrestres de aeroportos, sistemas de informação de voo, segurança de inspeção e muitos outros sistemas usados todos os dias e para todas as atividades relacionadas à aviação. A tendência da indústria da aviação é cada vez mais a digitalização. A digitalização introduz novos perigos, pois as interações homem-sistema tornam os riscos mais difíceis de prever.

Uma das maneiras de tentar manter uma segurança em rede, é a tecnologia Blockchain, a qual permite que um grupo coletivo de participantes selecionados compartilhe dados. Com *blockchain*, dados de transações de várias fontes podem ser coletados e compartilhados. Os dados são divididos em blocos compartilhados ligados entre si por identificadores únicos na forma de hashes criptográficos. Blockchain fornece integridade de dados com uma única fonte, eliminando a duplicação de dados e aumentando a segurança. Em um sistema blockchain, a fraude e adulteração de dados são evitadas porque os dados não podem ser alterados sem o consentimento das partes. Um registro de blockchain pode ser compartilhado, mas não modificado. Se alguém tentar modificar os dados, todos os participantes serão alertados e saberão quem tentou.

2.2 Modelo de Avaliação de Riscos segundo o PMBOK

O PMBOK (*Project Management Body of Knowledge* ou Corpo de Conhecimento em Gerenciamento de Projetos) é composto de cinco grupos de processos principais de acordo com o PMI (2017, p.18): Processos de Iniciação, Planejamento, Execução, Monitoramento e Controle e Encerramento. Além desses processos, existem dez áreas de conhecimento de projeto: Integração, Escopo, Cronograma, Custos, Qualidade, Recursos, Comunicação, Riscos, Aquisições e Partes Interessadas ou *stackholders* que podem ser representados por meio da Figura 3.

Figura 3 - Inter-relação dos componentes-chave do Guia PMBOK em projetos



Fonte: PMI (2017, p.18)

Murcha (2011, p.373) explica que o Gerenciamento dos Riscos de Projeto corresponde a uma das dez áreas de conhecimento do PMBOK e seus processos abrangem os grupos de Planejamento e Monitoramento e Controle conforme representado na Tabela 2.

Quadro 2 - Gerenciamento de Riscos nos grupos de processos PMBOK

O processo de gerenciamento dos riscos	Realizado durante
Planejar o gerenciamento dos riscos	Grupo de processos de planejamento
Identificar os riscos	Grupo de processos de planejamento
Realizar a análise qualitativa dos riscos	Grupo de processos de planejamento
Realizar a análise quantitativa dos riscos	Grupo de processos de planejamento
Planejar as respostas aos riscos	Grupo de processos de planejamento
Monitorar e controlar os riscos	Grupo de processos de monitoramento e controle

Fonte: Mulcahy (2011, p.373)

Vargas (2009, p.27) mostra que o custo de promover mudanças em um projeto é pequeno nas fases iniciais, crescendo exponencialmente com o progresso do projeto até chegar ao seu custo total, podendo até mesmo superá-lo. Verifica-se, portanto, que é importante realizar um Gerenciamento de Riscos adequado desde a origem do projeto para

evitar custos elevados de mudanças e manter monitoramento e controle a fim de evitar que os risco mitigados voltem aumentar seu grau de probabilidade e/ou impacto.

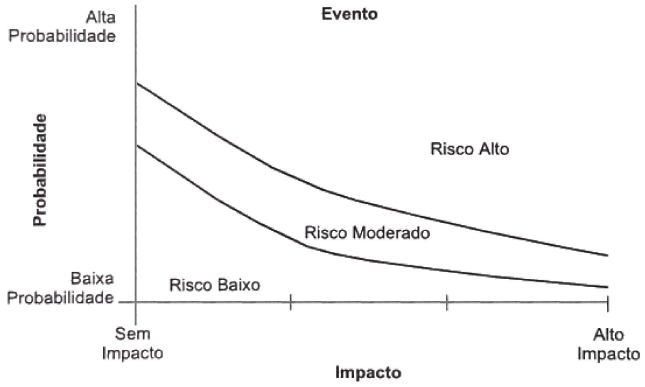
Segunda Varella (2005, p.191), o Gerenciamento de Riscos pode ser definido como um processo metódico de definição, análise e resposta aos riscos do projeto cujo objetivo é maximizar os eventos positivos, ou seja, as oportunidades, e reduzir os eventos negativos. Conforme o PMI (2017, p.395), o Guia PMBOK define os principais processos da Gerência de Riscos que são:

> - Planejar o Gerenciamento dos Riscos - O processo de definição de como conduzir as atividades de gerenciamento dos riscos de um projeto.
> - Identificar os Riscos - É o processo de identificação dos riscos individuais do projeto, bem como fontes de risco geral do projeto, e de documentar suas características.
> - Realizar a Análise Qualitativa dos Riscos - O processo de priorização de riscos individuais do projeto para análise ou ação posterior, através da avaliação de sua probabilidade de ocorrência e impacto, assim como outras características.
> - Realizar a análise quantitativa dos riscos - O processo de analisar numericamente o efeito combinado dos riscos individuais identificados no projeto e outras fontes de incerteza nos objetivos gerais do projeto.
> - Planejar as Respostas aos Riscos - O processo de desenvolver alternativas, selecionar estratégias e acordar ações para lidar com a exposição geral de riscos, e também tratar os riscos individuais do projeto.
> - Implementar Respostas a Riscos - O processo de implementar planos acordados de resposta aos riscos.
> - Monitorar os Riscos - O processo de monitorar a implementação de planos acordados de resposta aos riscos, acompanhar riscos identificados, identificar e analisar novos riscos, e avaliar a eficácia do processo de risco ao longo do projeto.

Varella (2005, p.193) mostra que um risco apresenta duas perspectivas para análise: a probabilidade e o impacto. A probabilidade é a sua possibilidade de acontecer. O impacto é a consequência sobre o objetivo do projeto, caso a eventualidade ou as premissas de risco venham a materializar-se.

Para Varella (2005, p.193), as motivações dos riscos são os pontos mais relevantes sob a perspectiva gerencial. Devem ser estudadas, analisadas e compreendidas para que possam ser implementadas ações apropriadas de gerenciamento de risco. O autor mostra a análise conjugada da probabilidade e do impacto dos riscos, que permite qualificá-los em níveis de importância ou gravidade para o projeto como ser verificado no gráfico 1.

Gráfico 1 - Probabilidade x impacto do risco



Fonte: Varella (2005, p.194)

Vargas (2009) explica por meio de mapas mentais cada um dos processos do PMBOK relacionado ao Gerenciamento de Riscos.

Planejar o gerenciamento dos riscos: é o processo de definir como conduzir as atividades de gerenciamento de risco de um projeto, representado pela figura 4.

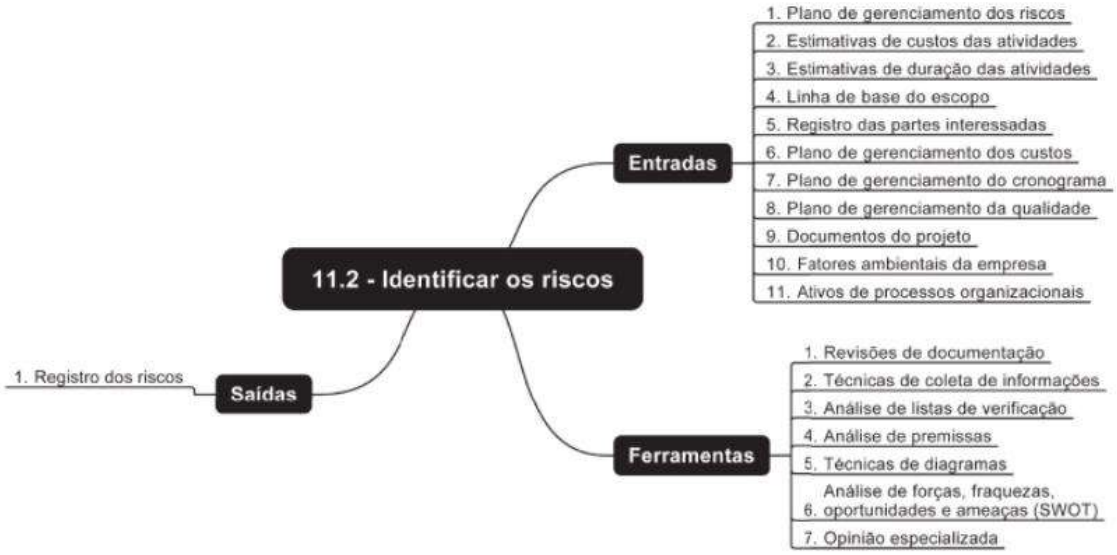
Figura 4 - Mapa mental do processo planejar o gerenciamento de riscos

Fonte: Vargas (2009, p.90)

Em um mundo cada vez mais conectado e dependente da tecnologia, a importância desse processo de planejamento não pode ser subestimada. Ao antecipar potenciais vulnerabilidades, ameaças e suas possíveis consequências, as organizações podem desenvolver estratégias proativas para mitigar, transferir ou aceitar esses riscos.

O próximo processo é identificar os riscos: neste processo ocorre a determinação dos riscos que podem afetar o projeto e de documentação e suas características, representado pela figura 5.

Figura 5 - Mapa mental do processo identificar os riscos



Fonte: Vargas (2009, p.91)

Identificar os riscos cibernéticos não se limita apenas a ameaças externas, mas também inclui fatores internos, como vulnerabilidades no sistema e comportamentos dos funcionários. Ao ter uma visão clara e abrangente dos riscos, as organizações podem direcionar recursos e esforços de segurança de maneira mais eficaz, implementar medidas de proteção apropriadas e garantir a resiliência contra ameaças digitais em um ambiente cada vez mais complexo e interconectado.

O próximo processo trata de realizar análise qualitativa dos riscos: nesta fase ocorre a priorização de riscos para análise ou ação adicional por meio da avaliação e combinação de sua probabilidade de ocorrência e impacto, representado pela figura 6.

Figura 6 - Mapa mental do processo realizar análise qualitativa dos riscos

Fonte: Vargas (2009, p.91)

A análise qualitativa avalia a natureza e a gravidade dos riscos de maneira holística. Isso permite identificar não apenas as ameaças potenciais, mas também entender melhor suas origens, características e possíveis impactos. Além disso, a análise qualitativa leva em consideração fatores subjetivos, como a reputação da empresa e o nível de confiança dos clientes, que podem ser afetados por incidentes cibernéticos.

O próximo passo é realizar análise quantitativa dos riscos: significa analisar numericamente o efeito dos riscos identificados nos objetivos gerais do projeto, representado pela figura 7.

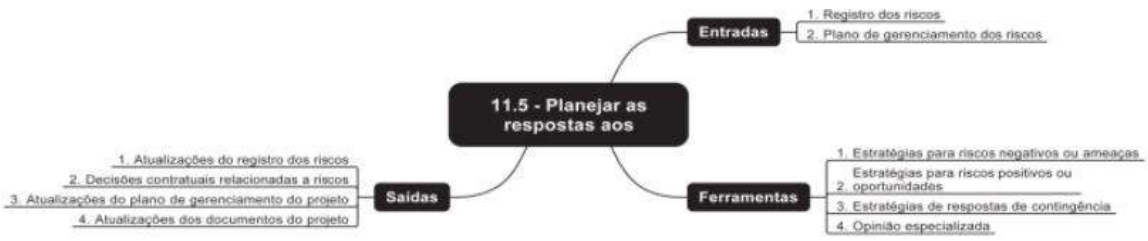
Figura 7 - Mapa mental do processo realizar análise quantitativa dos riscos

Fonte: Vargas (2009, p.92)

A análise quantitativa fornece uma base objetiva para avaliar a probabilidade de ocorrência de incidentes cibernéticos e os potenciais impactos financeiros associados a esses eventos. Ao atribuir valores monetários aos riscos, as organizações podem comparar e priorizar ameaças de acordo com seu potencial de dano, permitindo a alocação eficiente de orçamento e recursos para mitigação, transferência ou aceitação de riscos.

O próximo processo trata de planejar respostas aos riscos: é o processo de desenvolvimento de opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto, representado pela figura 8.

Figura 8 - Mapa mental do processo planejar respostas aos riscos



Fonte: Vargas (2009, p.92)

Ao antecipar possíveis cenários de incidentes cibernéticos e desenvolver estratégias de resposta apropriadas, a FAB pode minimizar o impacto de ameaças digitais, preservar a integridade dos sistemas e proteger a confidencialidade dos dados. Além disso, o planejamento de respostas aos riscos cibernéticos permite a coordenação eficaz das equipes de resposta, a comunicação adequada com partes interessadas e a documentação das ações a serem tomadas em caso de violação de segurança.

O processo seguinte trata de monitorar e controlar os riscos: nesse processo ocorre a implementação do plano de respostas aos riscos, acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação de novos riscos e avaliação da eficácia do processo de riscos durante todo o projeto, representado pela figura 9.

Figura 9 - Mapa mental do processo monitorar e controlar os riscos

Fonte: Vargas (2009, p.92)

Monitorar e controlar os riscos cibernéticos significa estar constantemente vigilante para identificar possíveis vulnerabilidades, ataques cibernéticos e ameaças em evolução. Além disso, a capacidade de responder de maneira eficaz a incidentes cibernéticos é essencial para minimizar os danos e preservar a confiança dos clientes e parceiros.

2.3 Modelo de Avaliação de Riscos segundo o PRINCE2

O PRINCE2 (Projetos em Ambiente Controlado) é um método de gerenciamento de projetos estruturado com base na experiência obtidas de milhares de projetos e contribuição de inúmeros acadêmicos, treinadores, consultores, patrocinadores de projetos e gerentes de projetos (OGC, 2011, p.3).

Para que se possa compreender melhor este método, faz-se necessária a definição de Gerenciamento de Projetos, (OGC, 2011, p.4):

> Gerenciamento de projetos é o planejamento, delegação, monitoramento e controle de todos os aspectos do projeto e a motivação dos envolvidos para atingir os objetivos do projeto conforme as metas para desempenho no que diz respeito a prazo, custo, qualidade, escopo, benefícios e riscos.

O modelo de Gerenciamento de Projetos PRINCE2 é composto de sete temas que descrevem os aspectos de gerenciamento que devem ser monitorados ao longo do ciclo de vida do projeto. Para Ribeiro (2011, p.15) os temas do PRINCE2 podem ser descritos da seguinte forma:

> ● *Business Case* - Refere-se ao porquê do projeto. Por que iniciar o projeto? Quais benefícios serão realizados?
> ● *Organization* - Foco numa estrutura temporária, com papéis e res-ponsabilidades definidos, para o gerenciamento do projeto. Quem faz parte do time do projeto? Quais são seus papéis e responsabi-lidades?
> ● *Quality*- Foco no entendimento, por todos os envolvidos, dos atributos de qualidade dos produtos a serem desenvolvidos pelo projeto. O que o projeto entregará?
> ● *Plans* - Foco no planejamento, na comunicação e no controle para desenvolver e entregar os produtos do projeto conforme os critérios de qualidade. Como o produto do projeto será desenvolvido e entregue? Quanto custará? Quem fará?
> ● *Risk* - Gerenciamento das incertezas do projeto. O que fazer se... acontecer?
> ● *Change* - Gerenciamento e análise de impacto das mudanças do pro-jeto. Qual o impacto (prazo, custo, qualidade, riscos etc.) de implemen-tar esta mudança no projeto?
> ● *Progress* - Monitoração do desempenho do projeto, pontos de tomada de decisão, escalonamento de problemas, viabilidade de seguir com o projeto etc. Onde o projeto está agora? Onde o projeto quer e deve chegar? O projeto chegou onde queria?

Pode-se entender que os temas PRINCE2 se equiparam às áreas de conhecimento do PMBOK.

Os processos do PRINCE2 são sete e são descritos por Ribeiro (2011, p.16) da seguinte forma:

> ● *Starting up a Project* - Este processo visa assegurar se o projeto é viável para ser iniciado.
> ● *Directing a Project* - Este processo, de responsabilidade do *Project Board* (Comitê de Direção do Projeto), visa assegurar condições propí-cias para um bom direcionamento do projeto.
> ● *Initiating a Project* - Este processo visa assegurar o entendimento dos objetivos, escopo, qualidade e quaisquer outras informações que con-solidem uma base para iniciar o projeto.
> ● *Manage a Stage Boundary* - Este processo visa assegurar ao *Project Board* informações suficientes sobre o desempenho do projeto e, com isto, decisões sobre continuidade, interrupção, cancelamento e/ou en-cerramento do projeto podem ser tomadas.
> ● *Controlling a Stage* - Este processo contempla atividades de controle e monitoramento dos estágios do projeto.
> ● *Managing Product Delivery* - Este processo visa garantir que os produ-tos do projeto sejam desenvolvidos e entregues conforme planejado e dentro dos padrões de qualidade preestabelecidos.

- *Closing a Project* -Este processo visa garantir o encerramento contro-lado do projeto.

Os dois processos do PRINCE2 que lidam com os riscos são *Initiating a Project* para a definição da Estratégia de Gerenciamento de Riscos e *Controlling a Stage* que trata do monitoramento e controle dos riscos dentre outras atividades conforme o manual de gerenciamento de projetos do PRINCE2.

O processo *Initiating a Project* é responsável por estabelecer sólidos fundamentos para o projeto por meio da criação das Estratégias de Gerenciamento de Risco, Qualidade, Configuração, e Comunicação, estabelecimento dos Controles do Projeto, criação do Plano de Projeto, detalhamento do Business Case e montagem da documentação para Iniciação do Projeto, (OGC, 2011, p. 157).

A Estratégia de Gerenciamento de Riscos descreve as metas de aplicação do gerenciamento de riscos, o procedimento que será adotado, os papéis e responsabilidades, as tolerâncias a riscos, a sequência das atividades do gerenciamento de riscos, as ferramentas e técnicas que serão utilizadas e os requisitos de relatórios (OGC, 2011, p.159).

Ribeiro (2011, p.93) mapeia o processo e define a estratégia de gerenciamento de riscos em suas entradas e saídas, representado pela figura 10.

Figura 10 - Entradas e saídas do processo definir estratégia de gerenciamento de riscos

Fonte: Ribeiro (2011, p.93)

As ações para cada uma das entradas e saídas do processo definir estratégia de gerenciamento de riscos são (OGC, 2011, p.159):

> - *Project Brief* : Revisar o Sumário do Projeto para saber a necessidade de se aplicar ao projeto estratégias, padrões ou práticas da gerência corporativa ou do programa relativos ao gerenciamento de riscos.
> - *Lessons Log:* Solicitar lições de projetos anteriores similares a gerência corporativa ou do programa e organizações externas relativas ao gerenciamento de riscos
> - *Daily Log:* Revisar no Diário do Projeto para quaisquer *issues* e riscos relativos ao gerenciamento de riscos.
> - *Registro de Riscos*: Criar o Registro de Riscos em conformidade com a Estratégia de Gerenciamento de Riscos e alimentá-lo com os riscos do Diário do Projeto.
> - *Parte da documentação de Iniciação do Projeto*: Solicitar a aprovação do Comitê Diretor do Projeto para a Estratégia de Gerenciamento de Riscos.

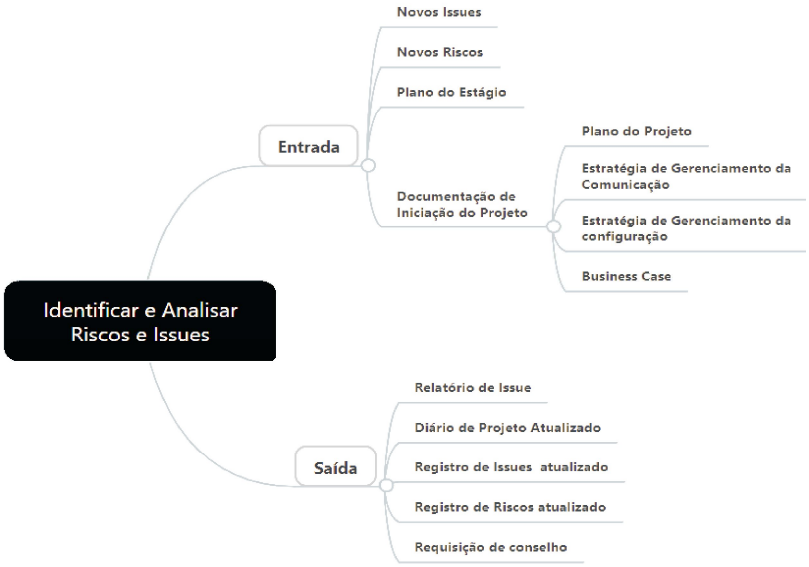
A definição da estratégia de gerenciamento de riscos estabelece o direcionamento e as prioridades para lidar com riscos cibernéticos, alinhando-se com os objetivos e valores da organização. Uma estratégia bem elaborada proporciona uma visão clara das ameaças, vulnerabilidades e recursos necessários para mitigar ou aceitar riscos de maneira informada.

O processo *Controlling a Stage* do PRINCE2 descreve o trabalho do gerente de projeto no gerenciamento diário. O propósito deste processo é atribuir o trabalho a ser feito, monitorar esse trabalho, lidar com *issues*[6], relatar o progresso ao Comitê Diretor do Projeto e tomar ações corretivas para que o estágio do projeto seja mantido dentro da tolerância. Desta forma tem-se três subprocessos relacionados a riscos: Identificar e analisar *issues* e riscos, Escalar *issues* e riscos e Tomar ação corretiva (OGC, 2011, p.177).

O subprocesso identificar e analisar *issues* e riscos pode ser descrito por Ribeiro (2011, p.108) pela atividade de estar atento, durante todo o ciclo de vida dos estágios do projeto, quanto a potenciais ameaças e questões que podem afetar os resultados do projeto porque os *issues* e riscos podem chegar de qualquer maneira e a qualquer momento. O mapa mental da figura 11 representa as entradas e saídas deste processo.

[6] Evento relevante que ocorreu, não foi planejado e requer ação de gerenciamento. Pode ser uma preocupação, consulta, requisição de mudança, sugestão ou não conformidade que apareça durante o projeto (OGC, 2011, p.325).

Figura 11 - Entradas e saídas do processo Identificar e Analisar Riscos e Issues



Fonte: Ribeiro (2011, p.93)

As ações para as entradas e saídas do processo Identificar e Analisar Riscos e *Issues,* são (OGC, 2011, p.189):

> - Verificar os requisitos do procedimento de gerenciamento de riscos na Estratégia de Gerenciamento de riscos;
> - Incluir o risco no Registro de Riscos assim que for capturado;
> - Identificar o evento do risco e descrever sua causa e efeito;
> - Avaliar o risco em relação ao Plano de Estágio, Plano de Projeto e Business Case e planejar a resposta para o risco selecionado;
> - Relatar o *status* do risco em conformidade com a Estratégia de Gerenciamento de Riscos e verificar na Estratégia de Gerenciamento da Comunicação se existe alguma parte externa que precisa ser informada sobre ele.

O subprocesso Escalonar Riscos e *issues* é necessário porque um estágio não deve ultrapassar as tolerâncias acordadas com o Comitê Diretor do Projeto. Conforme entendimento de Ribeiro (2011, p.108), o Gerente de projeto tem poder para tomar decisões sobre ações que não excedam os limites de tolerância estabelecidos para o estágio. Riscos e *issues* que porventura causem grandes impactos no estágio, que fogem dos limites do Gerente do Projeto, devem ser imediatamente escalonados para o Comitê Diretor do Projeto. O mapa mental da figura 12 representa as entradas e saídas deste processo:

Figura 12 - Entradas e saídas do processo Escalonar Riscos e Issues

Fonte: Ribeiro (2011, p.109)

As ações para as entradas e saídas do processo Escalonar Riscos e Issues são (OGC, 2011, p.190):

> - Examinar o Plano de Estágio para definir a extensão do desvio e os produtos não acabados e extrapolar o que aconteceria se o desvio continuasse;
> - Examinar no Plano de Projeto o status do projeto e o efeito geral de algum desvio (usando a linha de base atual do Documento de Iniciação do Projeto);
> - Determinar as opções de recuperação e avaliá-las em relação ao Business Case;
> - Avaliar o impacto das opções de recuperação em relação ao Plano de Estágio para o estágio atual;
> - Colocar a situação, as opções e a recomendação para uma linha de ação para o Comitê Diretor do Projeto em um Relatório de Exceção. O Comitê decidirá sobre a linha adequada de ação (que poderá aceitar de alguma forma a recomendação do Gerente do Projeto). Isso poderá incluir: Solicitar mais informações ou mais tempo para considerar sua resposta. Aprovar, deferir ou rejeitar uma solicitação de mudança. Fazer concessão para uma não-conformidade, deferi-la ou rejeitá-la. Aumentar as tolerâncias com previsão de serem excedidas. Instruir o Gerente de Projeto para preparar um Plano de Exceção, declarando que será aceito. Instruir o Gerente de Projeto para encerrar o Projeto prematuramente.

A escalada dessas ameaças para níveis de gestão adequados garante que a alta administração esteja ciente dos riscos críticos e possa tomar decisões estratégicas informadas para mitigá-los. Além disso, o processo de escalonamento facilita a comunicação eficaz entre as equipes de segurança cibernética e a liderança da organização, garantindo que todos compreendam a importância de lidar com riscos e *issues* de maneira oportuna.

O subprocesso Tomar ação corretiva tem como objetivo definir e implantar ações corretivas para corrigir ou amenizar os desvios ocorridos no projeto. Ribeiro (2011, p.109)

mostra que as ações corretivas de estágio devem ser implementadas pelo Gerente de Projetos sem a autorização do Comitê Diretor, desde que não exceda as tolerâncias atribuídas ao Gerente de Projeto. O mapa mental da figura 13 representa as entradas e saídas deste processo:

Figura 13 - Entradas e saídas do processo Ações Corretivas

Fonte: Ribeiro (2011, p.110)

As ações para as entradas e saídas do processo Ações Corretivas são (OGC, 2011, p.190):

- Coletar informações relevantes sobre o desvio (dos Registro de Itens de Configuração, Registro de *Issue*, Registro de Riscos, Relatório de *Issue*, Relatório de Exceção, conselho do Comitê Diretor do Projeto, Diário do Projeto);
- Identificar os modos possíveis de tratar o desvio e selecionar a opção mais apropriada;
- Ativar a ação corretiva, autorizando um Pacote de Trabalho;
- Atualizar os Registros de Configuração dos produtos afetados;
- Atualizar o Relatório de Issue (se necessário) para mostrar o status da ação corretiva;
- Atualizar o Registro de Issue com as mudanças resultantes da ação corretiva (ou se for tratado informalmente, atualizar o Diário do Projeto com os detalhes e o status da ação corretiva);
- Atualizar o Registro de Riscos com as mudanças resultantes da ação corretiva;

- Atualizar o Plano de Estágio para o estágio atual.

Essas ações corretivas visam não apenas mitigar as ameaças cibernéticas identificadas, mas também remediar os danos já causados por incidentes. Ao agir prontamente, a FAB pode minimizar o impacto financeiro e a perda de dados, recuperar sistemas e informações críticas e, o mais importante, aprender com os incidentes passados para fortalecer sua postura de segurança cibernética.

2.4 Modelo de Avaliação de Riscos segundo as Três Linhas de Defesa

As nações têm forças armadas, diplomatas e patrulhas de fronteira para proteger seus cidadãos. Geralmente uma organização não depende apenas de uma única linha de defesa para se proteger. Em vez disso, uma abordagem em camadas é a mais eficaz e eficiente, e o gerenciamento de riscos cibernéticos não é exceção.

Lam (2017, p.157) explica que as estruturas de defesa internas e externas podem ser vistas como uma pirâmide, cuja base são as "linhas de frente", que impedem os ataques mais óbvios. O próximo nível supervisiona essa base ampla e captura ameaças mais evasivas e, no topo, um quadro altamente refinado gerencia e monitora os níveis mais baixos enquanto combate as ameaças que penetraram nas outras linhas, esta estrutura piramidal pode ser visualizada na figura 14.

Figura 14 - Visão piramidal das Três Linhas de Defesa

Fonte: Elaborada pelo autor.

Sendo assim, pode-se perceber a dependência entre cada linha de defesa onde a primeira sustenta a segunda e assim sucessivamente.

Lam (2017, p.158) mostra que na década de 1990, o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO[7]) produziu a orientação amplamente adotada para o controle interno dos relatórios financeiros. E em 2001, a comissão voltou sua atenção para o gerenciamento de riscos corporativos e produziu seu primeiro quadro de ERM (Enterprise Risk Management) alguns anos depois. Em 2004, um sistema de defesa tripla para empresas foi lançado pelo COSO:

1. Unidades de negócios e operação.
2. Funções de risco e conformidade
3. Auditoria interna

Desde sua introdução, esse modelo foi adotado não apenas pelas comunidades financeira e de auditoria, mas também por reguladores governamentais como o *Federal Reserve* (Banco Central Norte-Americano) e o Escritório da Controladoria da Moeda (OCC). Lam (2017, p.158) mostra que o OCC codifica os papéis e responsabilidades de cada uma das três linhas de defesa na versão final de suas Diretrizes que estabelecem padrões elevados para grandes bancos nacionais, associações de poupança federal e agências federais.

Segundo o IIA (2012) citado pelo TCU (2019):

> [...] as três linhas devem existir de alguma forma, separadas e claramente identificadas, em todas as organizações, não importando o tamanho ou a complexidade do negócio, pois isso assegura a efetividade do gerenciamento de riscos.

Entende-se que o elevado nível de autonomia da auditoria interna não está presente nas outras linhas de defesa, nem mesmo na segunda linha de defesa, (TCU, 2019).

A função primordial da auditoria interna é fornecer avaliações autônomas sobre a efetividade do gerenciamento de riscos e dos controles internos, incluindo a maneira como a primeira e a segunda linhas de defesa atingem os objetivos de gerenciamento de riscos e controle (TCU, 2019).

O modelo das três linhas de defesa foi aplicado na Europa por meio dos órgãos ECIIA (*European Confederation of Institutes of Internal Auditing*) e FERMA (*Federation of European Risk Management Associations*) como instrumento para controle e gerenciamento

[7] é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa

do risco. O modelo define áreas, papéis e profissionais discriminando obrigações distintas e seus limites, proporcionando entendimento em como as tarefas dos gestores se inserem na estrutura geral de riscos e controles da organização.

Maali e Schwartz (2016) mostraram que o escopo impactado pelas três linhas de defesa dentro de uma organização compreende as políticas, os padrões regulatórios e *frameworks* utilizados, os controles e os riscos propriamente ditos, conforme pode ser observado na Figura 15.

Figura 15 - O escopo impactado pelas três linhas de defesa

Fonte: Maali e Schwartz (2016, p.3)

Veltsos (2017) explica que a segurança cibernética deve ser tratada como uma disciplina de risco por meio das três linhas de defesa. Dessa forma, é explorado como cada linha de defesa pode lidar com os ataques cibernéticos de forma a suportar um nível de segurança cibernética desejável em uma organização.

2.4.1 A Primeira Linha de Defesa

Para Lam (2017, p.158), a primeira linha de defesa são as unidades operacionais ou de negócios que conduzem os negócios da empresa no dia-a-dia. Essas unidades incluem não apenas unidades geradoras de lucro, como equipes de vendas, equipes de atendimento ao cliente e unidades de fabricação, mas também funções de back-office, como recursos humanos, TI, além de inúmeras outras unidades operacionais, grandes e pequenas.

Como primeira linha de defesa, Lam (2017, p.159) explica que as unidades comerciais e operacionais são os proprietários finais de seu próprio risco, responsáveis por medi-lo e gerenciá-lo no dia-a-dia.

No caso da FAB, a primeira linha de defesa trata-se de todos dos órgãos responsáveis pela atividade operacional da Força Aérea Brasileira. Cada unidade é responsável em lidar

com o risco cibernético em primeira instância e a seguir escalar o reporte e/ou tratamento para o ETIR responsável até CTIR.FAB.

Veltsos (2017) explica que a primeira linha de defesa engloba o departamento de segurança da informação da organização, assim como as várias unidades de negócios que possuem riscos cibernéticos. O objetivo é que essas unidades reconheçam as vulnerabilidades de seus ativos e a necessidade de gerenciamento dos riscos cibernéticos. Veltsos (2017) aponta que é necessário executar vários controles e isso significa lidar com eventos de risco, atualizar indicadores de riscos chave (KRIs) e implantar e gerenciar controles que afetam pessoas, processos e tecnologia.

Segundo Kogan e Quaresma (2018), a primeira linha de defesa é responsável por implementar e operacionalizar os controles para mitigar os riscos cibernéticos. Cada unidade de negócio tem riscos operacionais inerentes e é responsável por manter controles internos eficientes e implementar ações corretivas para resolver deficiências em processos.

Culp e Thompson (2016) mostraram que a primeira linha de defesa se resume em três itens chave: Eventos de Risco (detecção de malware[8], etc), Indicadores de Risco Chave (KRI) e Controles da Linha de Frente. Para Telem (2016), a primeira linha de defesa é responsável pelo conteúdo do risco e visa implementar ações para gerenciar e tratar os riscos, bem como avaliar situações emergentes. Maali e Schwartz (2016) mostram que a primeira linha de defesa está ligada diretamente a gerência sênior e possui dois processos principais: controle do gerenciamento e medidas de controles internos.

Observa-se uma semelhança e complementaridade em como os autores tratam a primeira linha de defesa. Basicamente, está ligada à área operacional onde é preciso implementar controles tanto dos processos como do gerenciamento desses processos assim como as ações relacionadas a gerenciamento de riscos.

2.4.2 A Segunda Linha de Defesa

Lam (2017, p.159) explica que a segunda linha de defesa consiste nas funções de risco e conformidade. A função de risco estabelece processos e procedimentos para garantir que a organização opere dentro de seu nível de tolerância ao risco, monitora o perfil de risco geral da empresa e recomenda ações quando o risco estiver fora dos níveis de tolerância estabelecidos pelo conselho e pela administração. A função de conformidade tem um foco

[8] *software* malicioso que se instala sozinho e/ou causa danos, realizando operações indesejadas nos computadores atingidos.

mais restrito, monitorando as operações para garantir que a empresa esteja cumprindo os requisitos estatutários e regulamentares.

No nível mais maduro, a função de risco supervisionará ativamente os vários riscos envolvidos, incluindo estratégicos, financeiros, de crédito, de mercado, reputacionais, operacionais, dente outros. Da mesma forma, a conformidade se envolverá em diferentes áreas, dependendo do setor, mas pode incluir proteção ao cliente, segurança e privacidade de dados, segurança ambiental e outras áreas regulamentadas (LAM, 2017, p.159).

O escopo e a complexidade da segunda linha de defesa variam dependendo de vários fatores, como o tamanho da empresa e o setor em que atua. As empresas menores podem relegar responsabilidades de segunda linha às funções financeiras ou operacionais. Nas empresas maiores - particularmente aquelas em setores fortemente regulamentados - essas funções podem ser chefiadas por um diretor de risco (CRO) e diretores de conformidade (COOs) que se reportam à gerência sênior ou diretamente ao CEO (LAM, 2017, p.159).

Kogan e Quaresma (2018) mostram que a segunda linha de defesa é responsável por definir as diretrizes e monitorar o cumprimento pela primeira linha de defesa. Na gestão de riscos cibernéticos, a proposição é a existência de uma função de segurança da informação corporativa independente. A segunda linha de defesa inclui funções de gerenciamento de risco e conformidade, e ambas devem trabalhar em conjunto com a área de negócios para garantir que a 1ª linha de defesa tenha identificado, avaliado e reportado corretamente os riscos do seu negócio.

Veltsos (2017) identifica a segunda linha de defesa como o gerenciamento do risco, mas pode incluir também conformidade, controle legal, de qualidade e financeiro. Para o autor, a segunda linha analisa estruturas de controle de segurança cibernética, define riscos-chave (KRIs) e métricas, cria avaliações de risco, testa e revisa a conformidade rastreando as ações da primeira linha de defesa e analisa o impacto dessas ações para determinar sua eficácia na mitigação de riscos cibernéticos. Em resumo, essa função monitora como a administração está lidando com os riscos cibernéticos, determinando a extensão em que os riscos são ativamente monitorados e gerenciados.

Para Culp e Thompson (2016), na segunda linha de defesa que está definida a política de segurança cibernética, os padrões de gerenciamento de ameaças e vulnerabilidades, definições dos indicadores de KRIs, e de ferramentas e processos de gerenciamento de segurança cibernética. Também é nesta linha que ocorrem definições de métricas-chave ligadas à garantia de controle de segurança cibernética e testes de conformidade. Para que

essas garantias sejam alcançadas é preciso realizar um rastreamento da análise de risco e de ações. Desta forma, a segunda linha exerce um papel supervisor, analisando as saídas, problemas nos controles, perfis de segurança e proporciona o desafio da mudança para a primeira linha e revisão dos controles adotados.

De acordo com Telem (2016), a segunda linha de defesa está diretamente ligada aos padrões da organização e responsável pelas políticas e processos para gerenciamento de riscos. Telem (2016) mostra que as funções principais nessa linha são definir, orientar e coordenar ações a fim de identificar tendências, sinergias e oportunidades de mudança dentro da organização.

Para Maali e Schwartz (2016), a segunda linha de defesa pode ser resumida nos seguintes processos:

- Gerenciamento do Risco: inclui a avaliação de riscos e como eles se encaixam no risco que organização é capaz de assumir;

- Compliance: responsável por suprir a primeira linha com ferramentas para fazer negócios em conformidade com a lei e regulamentos aplicáveis, monitorando a conformidade e fornecendo supervisão e relatórios para a gerência sênior e para o conselho;

- Funções de supervisão: podem ser aplicáveis a áreas como qualidade, regulamentação, financeiro, recursos humanos ou tecnologia da informação (segurança cibernética).

Pode-se concluir que a segunda linha de defesa está diretamente ligada às definições de políticas de segurança pela organização, ao cumprimento das normas e regulamentos, às atividades de supervisão, ao cumprimento da primeira linha assim como sua melhoria contínua.

2.4.3 A Terceira Linha de Defesa

A terceira linha de defesa na estrutura do COSO é a auditoria interna, a qual fornece garantia independente da segunda linha de defesa, bem como da primeira linha de defesa (LAM, 2017, p.160). O autor explica que à medida que a auditoria interna analisa os controles e os procedimentos de gerenciamento de riscos, identifica problemas e relata suas descobertas ao comitê de auditoria do conselho e à alta administração. Em função de suas responsabilidades distintas e posicionamento independente, a auditoria interna é capaz de fornecer garantia confiável sobre a eficácia dos processos gerais de governança, gerenciamento de riscos e controle interno da organização (LAM, 2017, p.160).

Lam (2017, p.160) esclarece que é um mal-entendido comum combinar a terceira linha de defesa com as funções das outras duas porque, a princípio, o auditor seria a melhor pessoa para ajudar a estabelecer controles de primeira linha ou executar as atividades de gerenciamento de risco cibernéticos da segunda linha. Mas, dado o papel da auditoria interna como à prova de falhas e a supervisão da primeira e da segunda linhas de defesa, a combinação de suas funções com as outras duas pode comprometer a objetividade da auditoria interna e limitar sua eficácia (LAM, 2017, p.160).

Para Kogan e Quaresma (2018), a terceira linha de defesa necessita de profissionais preparados tecnicamente para realizar avaliações independentes que permeiam o ciclo completo de gestão de riscos cibernéticos revendo de modo minucioso e eficiente as incumbências das duas primeiras linhas de defesa e colaborando para seu aperfeiçoamento.

Veltsos (2017) explica que pode também englobar informações de auditores externos e / ou reguladores. Essa linha de defesa representa uma avaliação independente, garantindo que a estrutura de controle interno da organização seja apropriada para lidar com os riscos que a organização enfrenta uma vez que o processo geral de governança de riscos cibernéticos é avaliado. Com mesmo efeito da segunda linha, pode implicar em mudanças nos controles das linhas anteriores.

Segundo Telem (2016) a terceira linha de defesa é responsável pelo monitoramento do conteúdo e do processo do risco fornecendo uma supervisão sobre estes dois aspectos. O objetivo dessa linha é garantir que os processos de gerenciamento de riscos sejam adequados e apropriados.

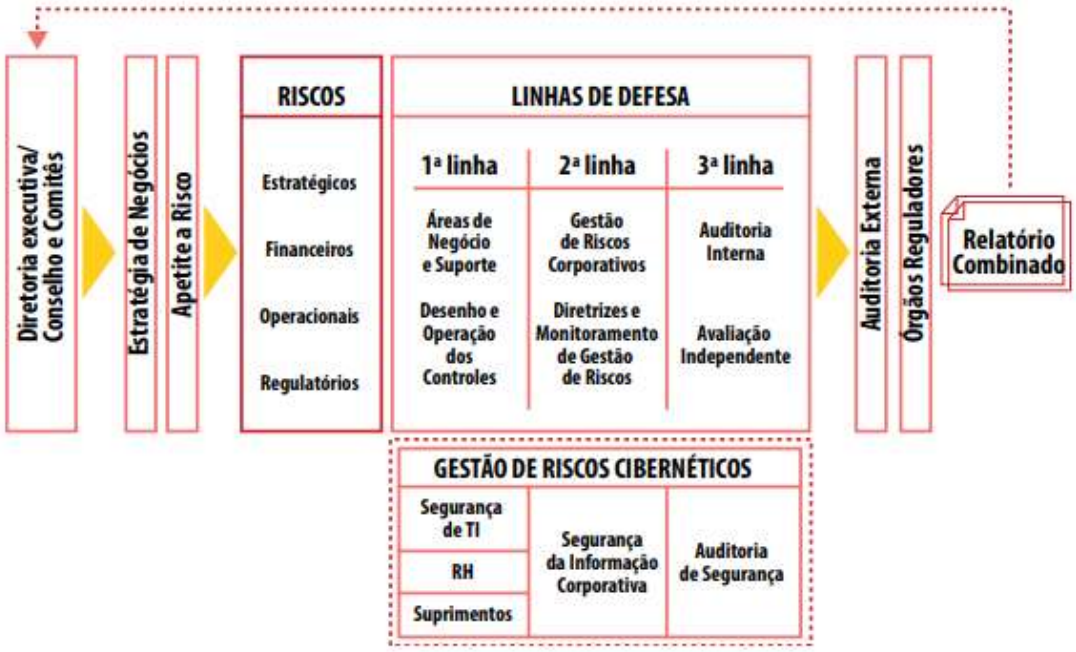
Para Maali e Schwartz (2016) a terceira linha de defesa fornece a “garantia independente”. A auditoria interna é responsável por analisar se os riscos de uma empresa estão sendo gerenciados por meio da avaliação de sua estrutura de controle.

Portanto, é evidente que auditoria interna se figura como o principal processo da terceira linha de defesa em que se busca uma garantia independente para os processos de gestão dos riscos cibernéticos. Complementarmente, alguns autores admitem auditorias externas nesta linha também.

2.4.4 Representações esquemáticas do Modelo das Três Linhas de Defesa

Kogan e Quaresma (2018) sistematizam suas linhas de defesa no modelo da figura 16.

Figura 16 - Modelo de gestão de riscos cibernéticos alinhado às 3 linhas de defesa



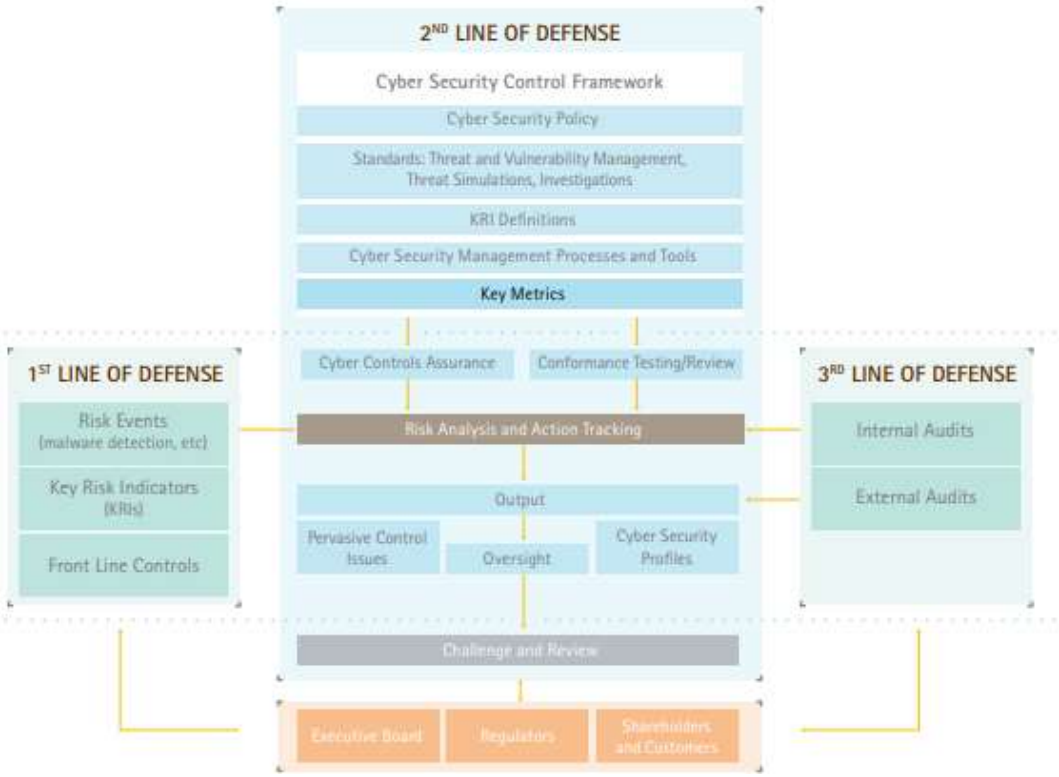
Fonte: Kogan e Quaresma (2018, p.6)

Observa-se que a gestão dos riscos cibernéticos engloba, segurança de TI, RH e Suprimentos para primeira linha de defesa, enquanto a segunda linha engloba a segurança da informação corporativa e a terceira linha a auditoria de segurança.

Veltsos (2017) não definiu um modelo esquemático específico de gestão de riscos alinhados às três linhas de defesa. No entanto, este autor deixa claro que a abordagem das Três Linhas de Defesa é a melhor maneira de uma organização rastrear e atuar sobre seus riscos cibernéticos com uma estratégia coordenada, em nível de organização, e que produz medições ao longo do caminho para avaliar o impacto dessas ações.

Culp e Thompson (2016) resumem suas análises sobre as três linhas de defesa, conforme a figura 17.

Figura 17 - *Framework* para alinhamento operacional de riscos com segurança cibernética



Fonte: *Chartis Research, based on analysis of the risk strategies of several global financial institutions, December 2015* apud CULP e THOMPSON (2016).

Observa-se na figura 17 que esse mapeamento define na primeira linha de defesa os eventos de riscos como detecção *malware*, indicadores de riscos-chave e controles de linha de frente. A segunda linha abrange todo arcabouço de controle de segurança (políticas, padrões, definições e gerenciamento de processos). E a terceira linha de defesa seria a auditoria interna e externa.

Telem (2016) traz um modelo em que classifica as três linhas de defesa em termos de responsabilidade sobre o conteúdo dos riscos ou sobre o processo dos riscos, conforme figura 18.

Na figura 18 pode-se observar que a primeira linha de defesa se preocupa com o gerenciamento dos riscos e implementação das ações de tratamento dos riscos cibernéticos. Essas ações devem estar de acordo com o processo de gerenciamento de riscos definidos na segunda linha de defesa. Esta por sua vez, estabelece as políticas e processos de gerenciamento de riscos fornecendo o rumo a ser seguido. Por fim, a terceira linha está diretamente ligada à gerência sênior do órgão e fornece a garantia de que o processo de gerenciamento de riscos está adequado e apropriado.

Figura 18 - *Framework* das três linhas de defesa

Fonte: Telem (2016, p.2)

Na Figura 19 pode-se observar o modelo de três linhas de defesa proposto por Maali e Schwartz (2016):

Figura 19 - As três linhas de defesa

Fonte: Maali e Schwartz (2016, p.4)

No modelo descrito na figura 19 pode-se notar que a primeira linha de defesa utiliza-se de medidas de controles internos para realizar o controle do gerenciamento de riscos. A segunda linha estabelece o gerenciamento de risco propriamente dito, os controles financeiros, segurança, qualidade, aspectos legais e *compliance*. A terceira linha volta-se exclusivamente para a auditoria interna.

Pode-se notar que as diferentes abordagens do modelo de três linhas de defesa mostrados apontam que a combinação das três linhas de defesa ajuda a garantir uma abordagem holística e eficaz na identificação, mitigação e gerenciamento de riscos cibernéticos, fortalecendo a resiliência da organização e a proteção dos ativos digitais em um ambiente em constante evolução de ameaças cibernéticas.

3 Revisão Documental: Defesa cibernética, gerenciamento de riscos cibernéticos, segurança da Informação e qualidade na Força Aérea Brasileira

Neste capítulo é apresentada a estruturação da defesa cibernética, do PMBOK, do PRINCE2, da governança da segurança da informação e da garantia governamental da qualidade na Força Aérea Brasileira no que tange ao tratamento incidentes cibernéticos e avaliação dos riscos cibernéticos.

A governança cibernética refere-se ao conjunto de políticas, procedimentos, processos e controles utilizados por uma organização para garantir a segurança, integridade, confidencialidade e disponibilidade de seus ativos de informação, especialmente no contexto de ambientes digitais e sistemas computacionais, ITGI (2007, p.12). Em outras palavras, é a maneira como uma organização planeja, implementa, monitora e aprimora suas estratégias e práticas relacionadas à segurança cibernética.

A governança cibernética abrange diversos aspectos, incluindo a gestão de riscos cibernéticos, conformidade com regulamentações, resposta a incidentes, proteção de dados e privacidade, além do desenvolvimento e implementação de políticas de segurança, explica ITGI (2007, p.07). Ela envolve a colaboração entre diferentes partes interessadas, como a alta administração, profissionais de segurança da informação, equipes de TI, fornecedores e outros stakeholders, com o objetivo de criar um ambiente seguro e resiliente contra ameaças cibernéticas.

Pode-se alinhavar uma abordagem *top-down* para compreender o contexto da segurança cibernética na Força Aérea Brasileira. No ponto mais alto tem-se o Gabinete de Segurança institucional, que possui entre outras funções a coordenação das atividades relativas à inteligência federal e segurança da informação conforme previsto na Instrução Normativa GSI/PR nº 1 (BRASIL, 2008, p. 2) e atualizada pela Instrução Normativa GSI/PR nº 1, de 2020.

Segundo a Instrução Normativa GSI/PR nº 1, (BRASIL, 2008, p. 2), a Segurança da Informação e Comunicações pode ser definida como o conjunto de ações que objetivam viabilizar e assegurar a disponibilidade[9], a integridade[10], a confidencialidade[11] e a

[9]propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade, (Brasil, 2008, p. 2).

[10] propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, Brasil (2008, p. 2).

[11] propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados, (Brasil, 2008, p. 2).

autenticidade[12] das informações. Essa Instrução Normativa disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

Dessa forma, o Ministério da Defesa, assim como os demais órgãos e entidades da Administração Pública Federal, direta e indireta foram orientados quanto à condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas.

O Ministério da Defesa criou a Portaria Normativa 3.389 de 21 de dezembro de 2012, a qual dispõe sobre a Política Cibernética de Defesa. Os objetivos definidos na Política Cibernética de Defesa são:

> A. assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional;
> B. capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD;
> C. colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
> D. desenvolver e manter atualizada a doutrina de emprego do St Ciber;
> E. implementar medidas que contribuam para a Gestão da SIC no âmbito do MD;
> F. adequar as estruturas de C, T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber;
> G. definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber;
> H. cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e
> I. contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD (Brasil, 2012c, p.15).

A defesa cibernética concentra-se nas ações e medidas específicas adotadas para proteger sistemas, redes e dados contra ameaças cibernéticas. Isso inclui a implementação de tecnologias de segurança, monitoramento proativo, resposta a incidentes e a aplicação de políticas que visam mitigar ou neutralizar ataques digitais. A defesa cibernética é uma parte essencial da governança cibernética, contribuindo para a segurança geral dos ambientes digitais de uma organização.

[12] propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade, (Brasil, 2008, p. 2).

Dentro do contexto deste trabalho, foi realizado um recorte de como está estruturada a Política de Defesa dentro da Força Aérea uma vez que uma das diretrizes traçadas é conceber e implantar o Sistema Militar de Defesa Cibernética (SMDC), contando com a participação de militares das Forças Armadas e civis (BRASIL, 2012b, p.17).

3.1 Defesa cibernética na Força Aérea Brasileira

O Centro de Defesa Cibernética (CDCiber) foi criado pela Portaria Normativa nº 666 de 4 de agosto de 2010 e está vinculado ao Ministério da Defesa por meio do Exército Brasileiro. Conforme a portaria nº 3.028-MD, de 14 de novembro de 2012, cabe ao CDCiber, a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa.

O CDCiber integra o Sistema Militar de Defesa Cibernética (SMDC), que atua em cinco áreas de competência: Doutrina, Operações, Inteligência, Ciência e Tecnologia e Capacitação de Recursos Humanos.

O Sistema Militar de Defesa Cibernética pode ser definido como:

> um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional (Brasil, 2014, p.25).

A eficácia das ações de Defesa Cibernética depende, principalmente, da atuação colaborativa da sociedade brasileira, incluindo, o Ministério da Defesa, a comunidade acadêmica, os setores público e privado e a base industrial de defesa, (Brasil, 2014, p.25).

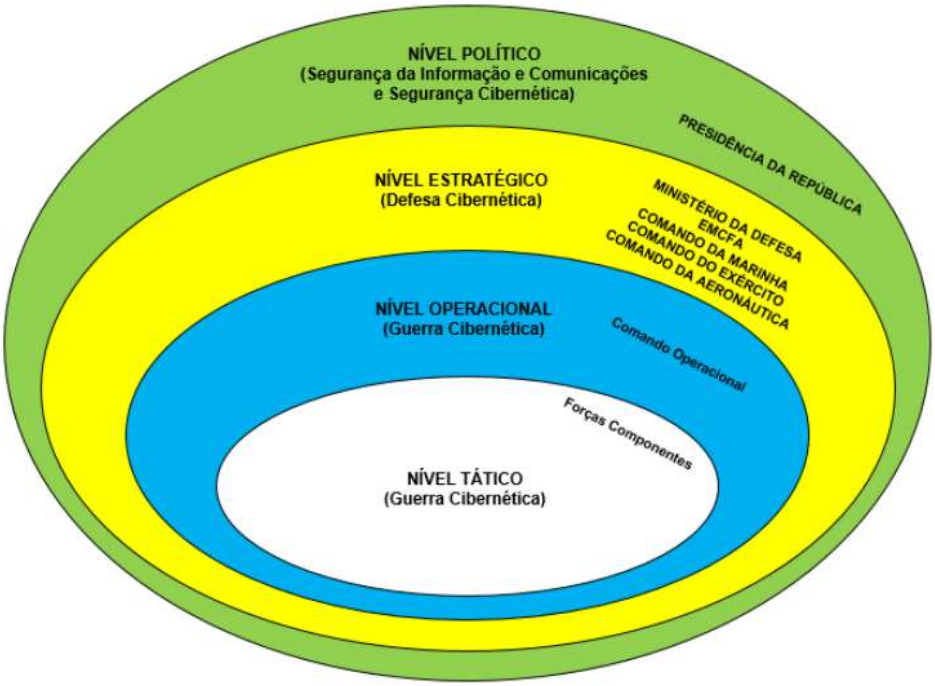
O CDCiber atuou de forma conjunta, coordenando atividades com diversos órgãos como o Serviço de Repressão a Crimes Cibernéticos (SRCC) da Polícia Federal, Agência Nacional de Telecomunicações (Anatel), Agência Brasileira de Inteligência (Abin), Serviço Federal de Processamento de Dados (SERPRO), CTIR.FAB, CTIR.MB, CTIR.EB. Vianna (2014, p.10) explica que o CDCiber atuou nos seguintes eventos:

- Rio +20 em 2012 - Conferência das Nações Unidas sobre Desenvolvimento Sustentável.
- JMJ 2013 - XXVIII Jornada Mundial da Juventude.
- Copa das Confederações FIFA de 2013.
- Copa do Mundo FIFA de 2014.

- Jogos Olímpicos de Verão de 2016

No contexto do SMDC, os níveis de decisão podem ser representados pela figura 20.

Figura 20 – Níveis de decisão



Fonte: (Brasil, 2014)

- Nível político - abrange as ações de SIC e Segurança Cibernética, cujos principais atores são a Presidência da República e o Comitê Gestor da Internet no Brasil;
- Nível estratégico - abrange as ações de Defesa Cibernética, a cargo do EMCFA, por intermédio do Centro de Defesa Cibernética, bem como dos Comandos das FA, por intermédio de seus respectivos órgãos de Defesa Cibernética, além de Centros de Tratamento de Incidentes de Redes (CTIR), da APF, de outras instituições parceiras e do Destacamento Conjunto de Defesa Cibernética, quando constituído;
- Nível Operacional - abrange as ações de Guerra Cibernética, a cargo dos Comandos Operacionais e de seus Estados-Maiores, quando ativados; e
- Nível Tático - abrange as ações de Guerra Cibernética, a cargo das Forças Componentes com seus elementos de Guerra Cibernética e o Destacamento Conjunto de Guerra Cibernética, quando ativados, (Brasil, 2014).

Segundo Sakude (2015), o Laboratório de Comando e Controle (LAB-C²) do ITA tem a missão de apoiar a Força Aérea Brasileira e o Ministério da Defesa na experimentação e desenvolvimento de novas tecnologias na área de Comando e Controle.

Sakude (2015) explica a diferença entre Tarefas Básica e Ações de Força Aérea:

> Na doutrina encontramos a definição das Tarefas Básicas e Ações de Força Aérea. Tarefas Básicas e as Ações de Força Aérea dizem respeito aos efeitos que podem ser produzidos com os Meios de Força Aérea. Enquanto as Tarefas Básicas definem os propósitos mais abrangentes de uma campanha ou operação militar, mormente estratégicos e operacionais, as Ações de Força Aérea descrevem atos específicos a serem executados no nível tático para a consecução daqueles propósitos. O somatório dos efeitos causados pelas Tarefas e pelas Ações contribui para a consecução dos objetivos da campanha ou operação militar e para o alcance do estado final desejado.

Sabe-se que a informação é um fator primordial na guerra moderna, porque influencia diretamente o processo de decisão das forças em conflito. Além disso, Sakude (2015) explica que as várias fontes de notícias que circulam durante a guerra podem induzir o senso comum a uma opinião favorável ou contrário aos propósitos da operação militar. Nesta conjuntura, também deve ser considerado o controle do ambiente cibernético, apoiado por um Sistema de Comunicações e Tecnologia da Informação para Comando e Controle, que são indispensáveis para troca de informações entre todos os escalões da cadeia de comando.

No entendimento Sakude (2015) do Laboratório de Comando e Controle (LAB-C²) do ITA o domínio do ambiente cibernético é muito importante porque ele pode influenciar direta ou indiretamente as lideranças, as forças militares e as infraestruturas críticas do inimigo inclusive até o ponto de poupar a confrontação militar direta:

> Controlar a informação, portanto, significa ter habilidade para coletar, processar, armazenar, disseminar e proteger dados e conhecimentos e, paralelamente, negar ao adversário a possibilidade de fazer o mesmo.

Portanto, pode-se registrar que a Tarefa Básica de Exploração da Informação da Doutrina descrita na DCA 1-1 é uma das atividades essenciais de Força Aérea.

Vianna (2014, p.9) mostra que o Simulador de Operações de Guerra Cibernética - SIMOC, do Exército Brasileiro, possibilitou a simulação de cenários práticos de guerra cibernética e proveu funções nas quais o instrutor podia examinar e acompanhar o exercício dos alunos, bem como adaptar condições e premissas durante o treinamento.

O SIMOC para o Exército Brasileiro permitiu ao CDCiber realizar suas simulações e treinamentos. Decatron (2020) explica que o simulador foi fundamentado em técnicas de virtualização, o que não limitava o EB a uma rede física, mas permitia criar redes virtuais e

adicionar elementos físicos, opcionalmente. Decatron (2020) explica ainda que o SIMOC permitia a memorização dos cenários e ações de treinamento bem-sucedidos, além disso, a aplicação foi desenvolvida utilizando a linguagem Java, tecnologia de virtualização VMware e interface do usuário com técnicas de drag & draw para criação das redes.

Vianna (2014, p.9) apresenta, na figura 21, um exemplo de rede criada utilizando o SIMOC:

Figura 21 - Exemplo de exercício de treinamento

Fonte: Vianna (2014)

Com uso do SIMOC foi possível a atuação do CDCiber em diversos eventos e treinamentos permitindo extrair alguns pontos importantes, conforme Vianna (2012, p.22):

- A disparidade entre proteção e ataque é muito expressiva.
- Para diminuir o hiato (gap) entre os dois aspectos é essencial:
- garantir a proatividade por meio da atividade de
- Inteligência e da gestão de riscos;
- realizar a Segurança e a Defesa de modo eminentemente colaborativo (“intra” e “extra” institucional);
- ter alto grau de maturidade em gestão de segurança da informação;
- Doutrina baseada nas melhores práticas e em Lições
- Aprendidas e exercida com agilidade e simplicidade.

Essa ferramenta permite que profissionais simulem cenários de ataques cibernéticos em um ambiente controlado e seguro, proporcionando a oportunidade de adquirir habilidades práticas, testar protocolos de resposta a incidentes e aprimorar a capacidade de identificar e mitigar ameaças em tempo real. Além disso, os simuladores de operações cibernéticas ajudam as organizações a avaliar a eficácia de suas estratégias de segurança e a identificar vulnerabilidades antes que sejam exploradas por invasores reais.

O arcabouço documental da Força Aérea Brasileira relacionado a segurança da informação e gestão de riscos pode ser representado pelo quadro 3:

Quadro 3 – Legislações FAB de segurança da informação

TIPO	ASSUNTO
DCA14-7	POLÍTICA DO COMANDO DA AERONÁUTICA PARA TECNOLOGIA DA INFORMAÇÃO
DCA14-8	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA
ICA 7-1	GESTÃO DE CONTINUIDADE DOS SERVIÇOS NOS ELOS ESPECIALIZADOS DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA
ICA 7-5	USO DA REDE MUNDIAL DE COMPUTADORES - INTERNET - NO COMANDO DA AERONÁUTICA
ICA 7-6	GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO NOS ELOS DE SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO DE "NÍVEL 2"
ICA 7-42	GERENCIAMENTO DE INCIDENTES DE SEGURANÇA EM REDES DE COMPUTADORES NO COMANDO DA AERONÁUTICA
DCA 7-3	POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO DO DECEA
DCA 7-4	GERÊNCIA DE CONFIGURAÇÃO DE TECNOLOGIA DA INFORMAÇÃO NO ÂMBITO DO DECEA
MCA 7-1	GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO
ICA 7-19	PRECEITOS DE SEGURANÇA DA INFORMAÇÃO PARA O DECEA
ICA 7-21	REDES SEM FIO WI-FI DO DECEA
ICA 7-23	PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DO DECEA
ICA 7-24	PROCESSO DE GESTÃO DE MUDANÇAS DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO DO DECEA
ICA 7-26	GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO NO DECEA
ICA 7-27	PROCESSO DE GESTÃO DE VULNERABILIDADES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO DO DECEA
ICA 7-28	PROCESSO DE GESTÃO DE LOG DO DECEA
ICA 7-29	PROCESSO DE GESTÃO DE CÓPIAS DE SEGURANÇA DA INFORMAÇÃO DO DECEA
ICA 7-30	PROCESSO DE CONTROLE DE ACESSO À REDE INTERNA E EXTERNA DO DECEA
ICA 7-31	CLASSIFICAÇÃO DOS SISTEMAS DE INFORMAÇÃO DO SISCEAB

ICA 7-32	REQUISITOS TÉCNICOS PARA AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS SEGUROS DE TECNOLOGIA DA INFORMAÇÃO DO DECEA
ICA 7-35	MODELO DE ESTAÇÃO SEGURA DO DECEA
ICA 7-36	GESTÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO NO ÂMBITO DO DECEA
ICA 7-37	GESTÃO DE CONTROLE DE ACESSO, IDENTIDADE E CRIPTOGRAFIA DE TECNOLOGIA DA INFORMACAO NO AMBITO DO DECEA

Fonte: Elaborado pelo autor

O arcabouço de documentos da FAB sobre segurança cibernética define as políticas, diretrizes e procedimentos que visam proteger a integridade dos sistemas e informações críticas da instituição. Esses documentos proporcionam um guia estruturado para a gestão de riscos cibernéticos, estabelecendo normas de segurança e boas práticas que ajudam a garantir a resiliência dos sistemas em um ambiente digital complexo e em constante evolução. Além disso, eles promovem a conscientização sobre a importância da segurança cibernética entre os servidores da FAB e contribuem para a manutenção da confiabilidade e da segurança das operações aéreas e estratégicas da instituição.

3.1.1 As três linhas de defesa na Força Aérea Brasileira: Tratamento de Incidentes cibernéticos na FAB e Auditoria Interna

O tratamento de incidentes na Força Aérea Brasileira está organizado em Elos que se estruturaram conforme os seguintes atos normativos:

- Norma Complementar 05/IN01/DSIC/2009:

Criação de equipes de tratamento e respostas a incidentes em redes de computadores.

- Norma Complementar 08/IN01/DSIC/2010

Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública.

- NSCA 7-13 / 2013

Segurança da Informação e Defesa Cibernética nas organizações do comando da aeronáutica.

- ICA 7-42 / 2016

Gerenciamento de Incidentes de Segurança de Redes de Computadores no Comando da Aeronáutica.

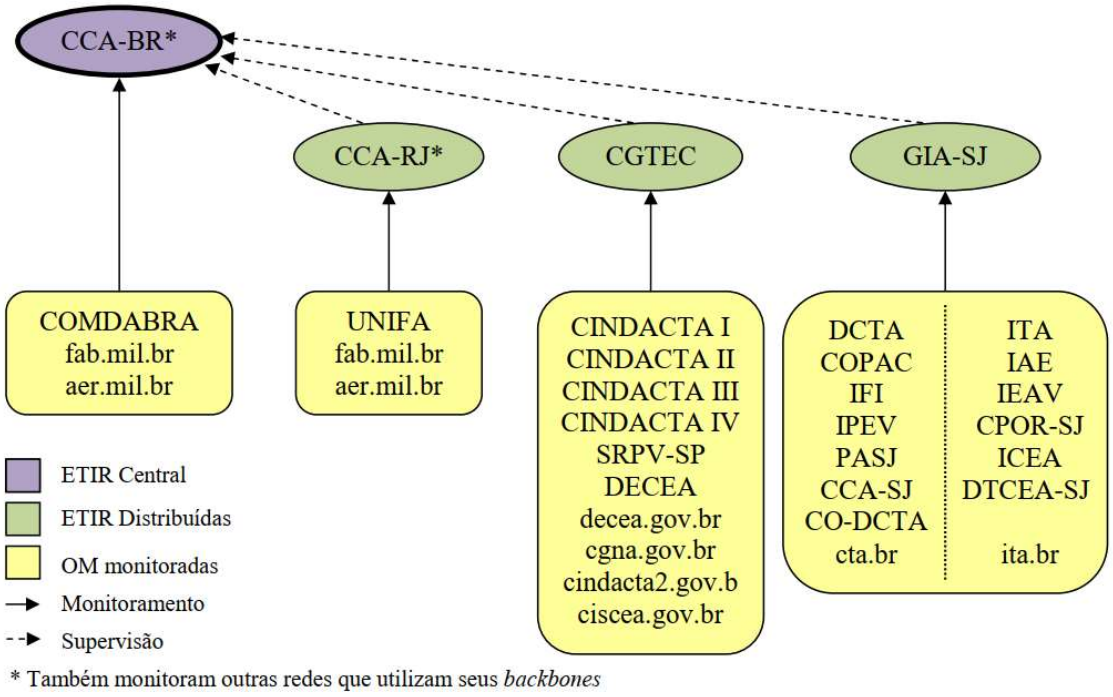
A ICA 7 – 42 tem por finalidade orientar as organizações do COMAER quanto ao Gerenciamento de Incidentes de Segurança em Redes de Computadores no COMAER, realizado pelo Centro de Tratamento de Incidentes de Rede da Força Aérea Brasileira (CTIR.FAB), por meio das Equipes de Tratamento de Incidentes de Segurança em Redes Computacionais (ETIR) (Brasil, 2016a, p. 6).

O CTIR.FAB tem como missão facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, receber e/ou notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, a fim de contribuir para a segurança da informação no COMAER (Brasil, 2021).

O Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Força Aérea Brasileira (CTIR.FAB) é uma das seções da Subdivisão de Segurança da Informação (SDSI) do CCA-BR, que, por sua vez, é subordinado à Diretoria de Tecnologia da Informação da Aeronáutica (DTI), Órgão Central do Sistema de Tecnologia da Informação do COMAER.

Para que todas suas atividades sejam cumpridas o CTIR.FAB opera por meio da Equipe Central de Tratamento e Resposta a Incidentes de segurança em Redes de Computadores (ETIR Central) e de ETIR distribuídas organizados conforme diagrama da figura 22.

Figura 22 - Modo de operação do CTIR.FAB no COMAER



Fonte: (Brasil, 2016a, p.25)

Observa-se a atuação da rede de ETIR em todo o COMAER inclusive nas unidades que utilizam sistemas críticos de Defesa Aérea e Controle do Tráfego Aéreo.

O CTIR.FAB deve reportar -se ao Chefe do CCA-BR, que se relacionará no âmbito do COMAER e se reportará ao GSIC (Comitê de Segurança da Informação e Comunicações). O CTIR.FAB relacionar-se-á externamente com o Centro de Tratamento e Resposta de Incidentes em Redes Computacionais (CTIR Gov) e outras equipes similares, no que couber (Brasil ,2016a, p. 12).

A responsabilidade por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes distribuídas cabe ao CTIR.FAB, além de ser a única responsável, perante toda a organização, pela comunicação com o CTIR Gov e agentes externos ao COMAER (Brasil, 2016a, p. 12).

Outra atividade importante do CTIR.FAB consiste em monitorar e analisar tecnicamente os incidentes de segurança no STI, permitindo a criação de métricas e/ou alertas além de comunicar o tratamento de incidentes às áreas envolvidas.

O CTIR.FAB também auxilia o Órgão Central do STI na geração de indicadores do processo. Tendo em vista o impacto que os incidentes de segurança da informação podem

provocar, o CTIR.FAB implementa mecanismos que permitem a avaliação dos danos ocasionados por incidentes de segurança nos Elos do STI.

Buscando o *compliance*[13] com as normas do setor e procurando orientar os elos distribuído e regionais, o CTIR.FAB regulamenta os procedimentos a serem adotados quando sistemas de software e hardware que sejam comprovadamente inseguros sejam identificados e orienta as ETIR por meio dos normativos técnicos necessários para o tratamento de incidentes no âmbito do COMAER (Brasil, 2016a, p. 12).

As ETIR atuam na linha de frente aplicando as ações de tratamento a incidentes, e são responsáveis por implementar as estratégias e medidas de segurança da informação contidas nas legislações ligadas a este assunto em suas respectivas áreas de responsabilidade, em alinhamento às orientações recebidas do CTIR.FAB.

As ETIR também são responsáveis por monitorar os incidentes de segurança e comunicar ao CTIR.FAB, no menor prazo possível além de analisar e identificar sistemas de software e hardware que sejam comprovadamente inseguros de forma que não sejam utilizados nas infraestruturas de TI do COMAER (Brasil, 2016a, p. 13).

A estrutura adotada é denominada CTIR.FAB, sendo operada por uma ETIR Central e uma rede de ETIR Distribuídas, ativadas de acordo com os planos do STI.

O processo de tratamento de incidentes no CTIR.FAB é baseado no modelo do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) tendo como abrangência toda a estrutura de redes de computadores do COMAER e seus usuários.

Sabe-se que a ETIR Central é parte integrante da estrutura orgânica do CCA-BR.

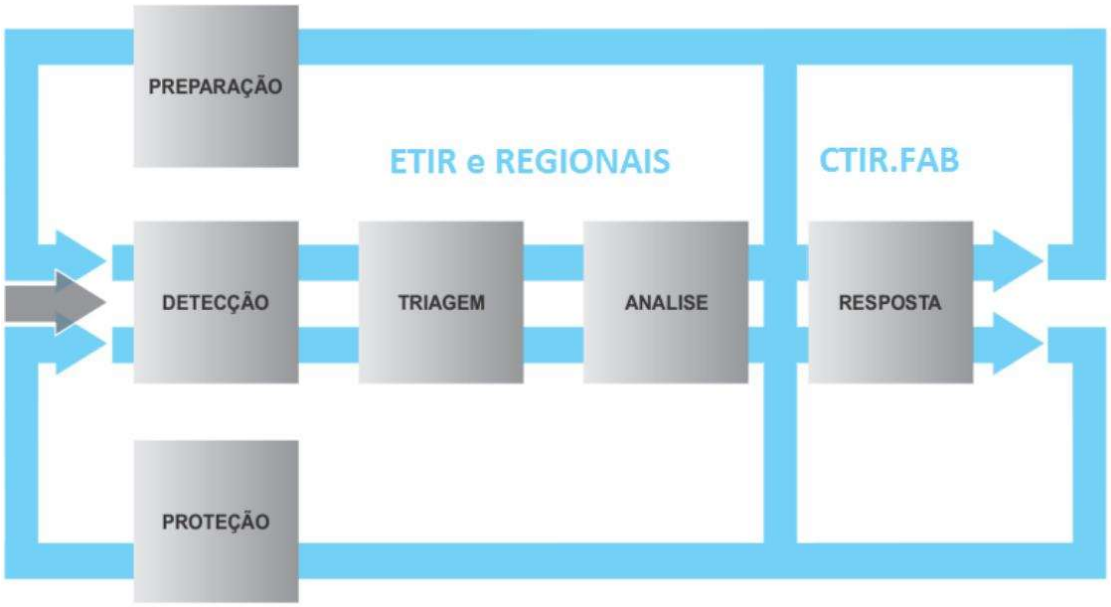
Para iniciar-se a discussão sobre o processo de tratamento de incidentes cibernéticos na FAB é fundamental compreender a definição de incidente. Consiste em um evento adverso, confirmado ou sob suspeita relacionado à segurança dos sistemas de computação ou das redes de computadores (CERT.br, 2021).

O Tratamento de Incidentes é o processo de identificar, prevenir e mitigar os incidentes de segurança.

O macroprocesso de gerenciamento de incidentes de segurança no COMAER é baseado nos processos definidos pelo CERT.br. e pode representado pela figura 23.

[13] É estar em conformidade com leis e regulamentos (Siteware, 2017).

Figura 23 – Processo de tratamento de incidentes do CTIR.FAB



Fonte: (Brasil, 2016a, p.19)

Detecção do Incidente Cibernético: Esse processo tem início quando a ETIR recebe uma notificação de um evento suspeito. A informação pode vir de algum Elo do STI, de alguma outra ETIR externa ao COMAER ou gerada por soluções de monitoramento.

Triagem: A triagem de eventos compreende as atividades de categorização e distribuição de incidentes entre os membros da equipe. O incidente recebido deverá ser categorizado, priorizado, correlacionado e complementado, de modo a subsidiar uma posterior análise.

Análise: Essa atividade consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados ou potenciais e propor estratégias de contenção e recuperação.

Resposta: Nessa etapa, as ações necessárias para o tratamento do incidente são comunicadas às partes envolvidas. Também podem ser enviadas notificações para os envolvidos em possíveis ações maliciosas.

Preparação: Nesta etapa, são implementados os mecanismos computacionais e organizacionais para que os incidentes cibernéticos possam ser detectados.

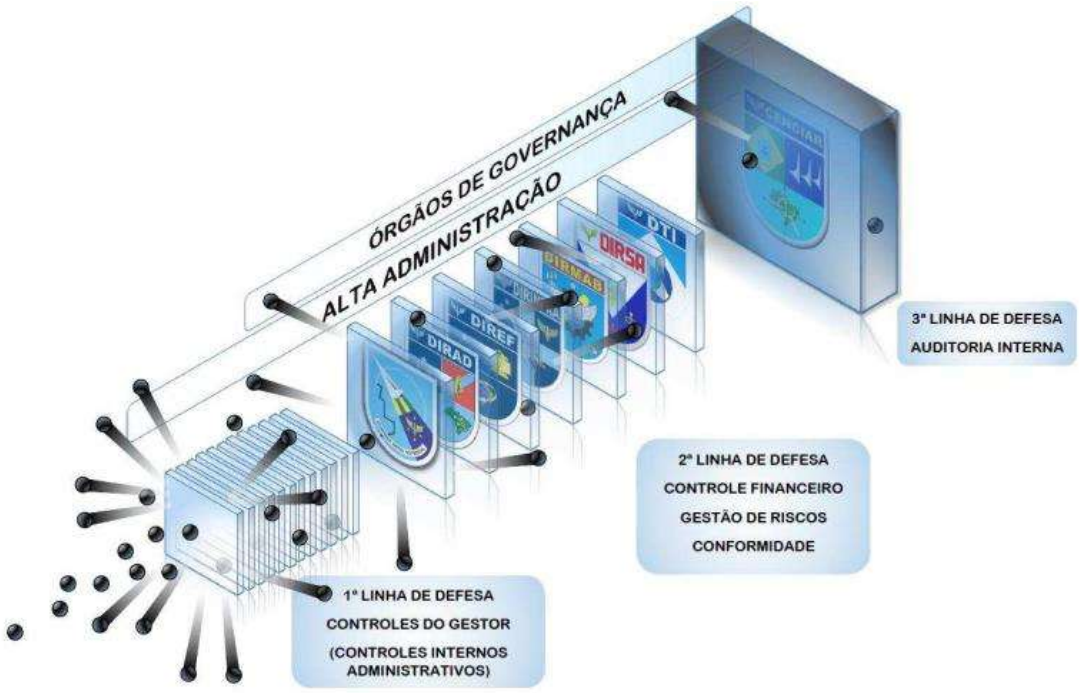
Proteção: Consiste na implementação de mecanismos de hardware e software para proteção dos sistemas, computadores, servidores e redes no COMAER.

A Auditoria Interna da Força Aérea Brasileira é exercida pelo Centro de Controle Interno da Aeronáutica (CENCIAR) por meio do Sistema de Controles Internos da

Aeronáutica (SISCONIAER) conforme estabelecido na NSCA 179-1/2019 (Brasil, 2019a, p.5).

Na figura 24, está demonstrado o modelo de três linhas de defesa segundo a visão do Sistema de Controles Internos da Aeronáutica e pode-se observar a posição clara do CENCIAR como o órgão responsável pela Terceira Linha de Defesa.

Figura 24 – Linhas de Defesa



Fonte: (Brasil, 2019a, p.19)

O CENCIAR não atua como partícipe da gestão (cogestão), mas dessa se dissocia, a fim de preservar sua independência e sua isenção na avaliação do órgão executor. A Auditoria Interna Governamental é uma atividade independente e objetiva de avaliação e de consultoria, destinada a agregar valor e contribuir para aprimorar as operações e os controles internos de uma organização. A Auditoria Interna Governamental auxilia a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar a eficácia dos processos de gestão de riscos, controle e governança.

A auditoria interna, principal atividade da terceira linha de defesa, é constituída, no âmbito do COMAER, pelo Centro de Controle Interno da Aeronáutica (CENCIAR), Unidade de Auditoria Interna Governamental, sendo responsável por avaliar a operacionalização dos controles internos da gestão implementados pela primeira linha de defesa (executada por

todos os níveis de gestão dentro da organização) e supervisionados pela segunda linha de defesa (Brasil, 2019a, p.5).

Ao CENCIAR, como Órgão Central do SISCONIAER, compete orientar os Órgãos Executivos quanto à implementação, manutenção, monitoramento e revisão dos controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos e seus possíveis impactos na consecução dos objetivos estabelecidos (Brasil, 2019a, p.13).

O CENCIAR também orienta a avaliação de riscos, atividades de controles internos, informação, comunicação e monitoramento além da integração, ao processo de gestão, de adequados controles internos da gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, complexidade, estrutura e missão da OM.

Por fim, outra orientação do CENCIAR consiste na necessidade de implementação de controles internos de modo contínuo, como uma série de ações entremeadas nas atividades da organização, inerentes à prática rotineira de gestão e à supervisão e monitoramento dos controles internos implementados.

3.2 Os modelos PMBOK e PRINCE2 na Força Aérea Brasileira

O gerenciamento de riscos de uma forma geral, assim como o gerenciamento de riscos cibernéticos na Força Aérea Brasileira está regulamentado por meio das seguintes legislações: DCA 16-2 no âmbito do EMAER de 31/08/2022, DCA 7-3 de 16/04/2022 e ICA 7-26 de 24/05/2013 no âmbito do DECEA, ICA 16-1 de 02/04/2019 no âmbito do COMGEP, ICA 12-30 no âmbito da SEFA de 16/07/2018, ICA 16-3 de 11/05/2021 no âmbito do COMPREP e ICA 80-13 de 23/01/2018 no âmbito do DCTA. Essas legislações detalham os aspectos do gerenciamento de riscos conforme modelo PMBOK e PRINCE2, os quais podem ser observados a seguir.

Quanto à definição da estratégia de risco cibernético e ao planejamento de risco cibernético, o EMAER mostra como deve ocorrer a definição de uma estratégia organizada e interativa para conduzir o gerenciamento de riscos e a sua materialização em um Plano (Brasil, 2017, p.17). Nessa fase inicial são identificadas as variáveis principais do projeto ou da atividade (escopo, custo, prazo e qualidade) e suas principais metas, requisitos, recursos, restrições e óbices (Brasil, 2017, p.18). Nesta fase estratégica, o estabelecimento do contexto envolve o entendimento da organização, dos objetivos e do ambiente interno e externo com a finalidade de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização de atingir seus objetivos (Brasil, 2022b, p.22).

Para o DECEA essa primeira fase trata-se da definição do contexto:

> definir o contexto interno e externo, os critérios utilizados para análise, avaliação, tratamento e aceitação dos riscos e o mapeamento dos ativos de informação do escopo definido (Brasil, 2013b, p.10).

O COMGEP descreve que no contexto externo, podem-se incluir os seguintes ambientes: cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico e natural, quer seja internacional, nacional, regional ou local. Deve ser dada especial atenção ao relacionamento da Organização com as partes interessadas externas (Brasil, 2019b, p.10). No contexto interno, devem-se avaliar quais os fatores podem influenciar na gestão de riscos, por exemplo, a cultura organizacional, os processos, a estrutura e a estratégia da organização. Além disso é necessário conhecer como estão estruturados os sistemas de informação, os fluxos de informação e os processos de tomada de decisão da Organização (Brasil, 2019b, p.10).

No âmbito da SEFA, a gestão de riscos deve ser considerada em todos os projetos, processos e atividades da Organização. Deve-se considerar o investimento na gestão de riscos sob a forma de treinamento, capacitação e gestão do conhecimento. Para uma maior efetividade do processo de gestão de riscos, devem-se estabelecer mecanismos efetivos de comunicação e reporte internos e externos. É indispensável que sejam definidas a responsabilização e a propriedade dos riscos por meio da formalização da autoridade e competência apropriadas. Isso visa garantir que o processo seja implementado e mantido adequadamente (Brasil, 2018b, p.14).

Para o COMPREP, o planejamento inicial deve-se basear em uma análise SWOT sobre cada macroprocesso da respectiva cadeia de valores, para a identificação de forças e fraquezas, bem como para analisar e registrar as possíveis influências do ambiente externo quanto a oportunidades e ameaças. O cruzamento dos quadrantes de fraquezas com ameaças, é inicialmente o foco da Gestão de Riscos da Organização. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas e as fontes de risco, suas consequências positivas ou negativas, expressas em termos de impactos tangíveis ou intangíveis (Brasil, 2018c, p.28).

Para o DCTA, a estrutura para a gestão de riscos cibernéticos é entendida como o conjunto (ou arranjo) de práticas, processos, sistemas, recursos (humanos e materiais) e cultura que, atuando no sistema de gestão da organização, possibilitam que os riscos sejam gerenciados (Brasil, 2018a, p.15).

Logo após a fase de planejamento e estratégia de gerenciamento de riscos cibernéticos inicia-se a fase de identificação dos riscos. Para o EMAER, no processo de identificação dos riscos é obtida uma lista abrangente de eventos que possam afetar a realização dos objetivos do projeto ou da atividade, incluindo suas causas e consequências, reações em cadeia provocadas por efeitos específicos e resultantes cumulativos e em cascata (Brasil, 2017, p.19). O principal propósito dessa fase é identificar a possibilidade do surgimento de acontecimentos ou situações que, eventualmente, podem interferir ou obstar, de alguma maneira, o alcance dos objetivos organizacionais (Brasil, 2022b, p. 25).

Para o DECEA, o processo de identificação de riscos cibernéticos corresponde ao processo de análise e avaliação de riscos, que valora ativos, ameaças e vulnerabilidades (Brasil, 2013b, p.12). A identificação dos riscos cibernéticos determina os eventos que podem causar perdas potenciais para a instituição (Brasil, 2013b, p.12)

O COMGEP trata o processo de identificação dos riscos cibernéticos da mesma forma que o EMAER enfatizando que deve seguir as etapas do gerenciamento de riscos previsto na DCA 16-2 (Brasil, 2019b, p.10).

Na SEFA, a identificação dos riscos cibernéticos refere-se à correta caracterização das fontes de risco, áreas de impacto, eventos, suas causas e consequências, em todos os níveis da OM (Brasil, 2018b, p.17). O resultado dessa etapa é uma lista de eventos (registro de riscos) que poderão impactar o alcance dos objetivos, os projetos ou atividades da instituição. Para auxiliar essa atividade, convém o uso de ferramentas e técnicas de identificação de riscos, como: *brainstorming*[14]; *brainwritting*[15]; análise *bow tie*; opiniões de especialistas; análise SWOT; entrevistas estruturadas e outras (Brasil, 2018b, p.17).

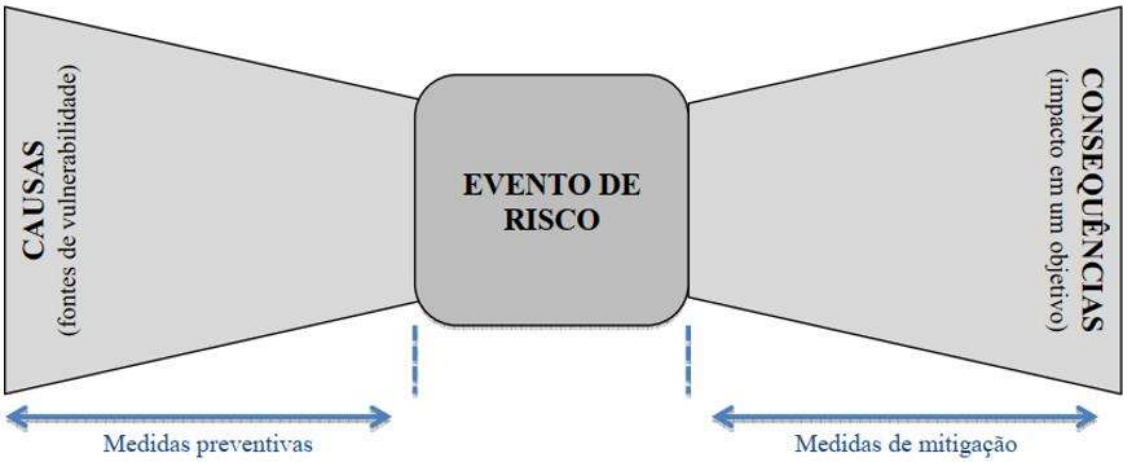
O COMPREP destaca a análise *bow tie*[16] na identificação dos riscos cibernéticos representada pela figura 25:

[14] Brainstorming é uma técnica utilizada para propor soluções a um problema específico. Consiste em uma reunião também chamada de tempestade de ideias, na qual os participantes devem ter liberdade de expor suas sugestões e debater sobre as contribuições dos colegas Neipatel (2021).

[15] técnica que envolve um grupo na geração de ideias de modo escrito e compartilhado, Baltazar (2019).

[16] A metodologia BOW TIE ou GRAVATA-BORBOLETA é uma maneira esquemática e simples de descrever e analisar os caminhos de um risco, desde as suas causas até as suas consequências, Carvalho (2015).

Figura 25 – Causa, Risco e Consequências



Fonte: (Brasil, 2018c)

No DCTA, a identificação de riscos é focada em obter uma lista abrangente de eventos que possam afetar a realização dos objetivos organizacionais, de projetos ou de atividade (Brasil, 2018a, p.21).

Após a Identificação dos Riscos, o próximo processo é a Avaliação de Riscos. No âmbito do EMAER é descrita como o processo de comparar os resultados da análise dos riscos com os critérios para determinar se ele é aceitável, tolerável ou inaceitável. O resultado da avaliação é a classificação dos níveis de riscos em faixas, por meio do agrupamento de níveis adjacentes, de maneira consistente com os critérios de riscos definidos para o projeto ou para a atividade (Brasil, 2017, p.22).

O EMAER prevê uma análise preliminar qualitativa nas fases iniciais do projeto ou da atividade, que evoluirá para quantitativa quando mais dados e conhecimentos forem obtidos. A análise qualitativa é definida no EMAER pela estimativa do risco e compreende dois aspectos: a probabilidade da ocorrência de cada risco e sua consequência, impacto no projeto ou na atividade (Brasil, 2017, p.21).

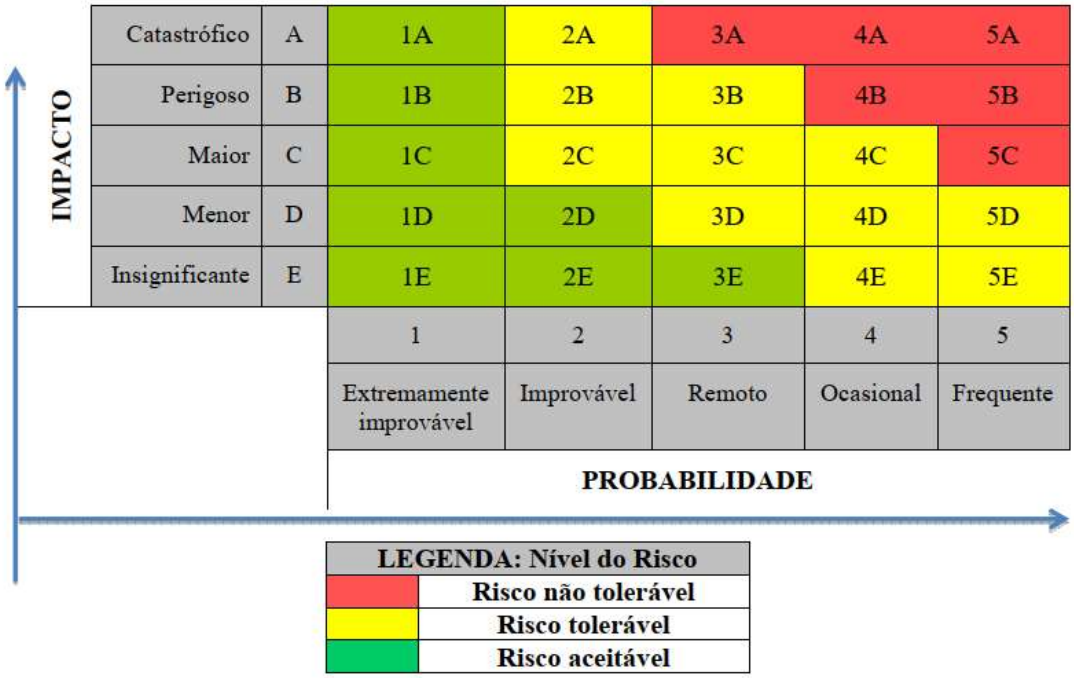
No DECEA, a Avaliação de Risco visa produzir os dados que auxiliam na decisão sobre quais riscos serão tratados e quais formas de tratamento são empregadas. A etapa de avaliação de riscos tem por objetivo comparar os níveis de riscos identificados na fase anterior com os critérios de avaliação e aceitação e obter uma lista de riscos ordenados por prioridade (Brasil, 2013b, p.29). Para o DECEA, a análise qualitativa é realizada por meio da estimativa dos riscos que determina a probabilidade de ocorrência e os impactos desses eventos e se localiza dentro do processo analisar e avaliar (Brasil, 2013b, p.12). A análise quantitativa dos riscos ocorre como o efeito combinado dos riscos individuais identificados

no projeto. Pode ser inferida pelas consequências ou prejuízos para a Organização, advindas de um cenário de incidentes, resultado da exploração da vulnerabilidade existente (Brasil, 2013b, p.12)

No âmbito do COMGEP, o processo de avaliação de riscos é baseado no levantamento do contexto em que a Organização está inserida, além de depender de outros fatores que são variáveis no tempo (Brasil, 2019b, p.12). Para o COMGEP, a estimativa de riscos (análise qualitativa) deve seguir processo idêntico ao mapeado pelo EMAER e adicionalmente utilizar o modelo de classificação percentual variando os valores de 0% a 100% para probabilidade de ocorrência e impacto do risco ocorrer (Brasil, 2019b, p.28). Quanto à análise quantitativa o COMGEP desencoraja, pois exige obtenção de dados com precisão. Caso seja necessária para os riscos de maior severidade, deve-se ter em mente que poderão ser utilizadas algumas técnicas como: análise de histórico das ocorrências, simulação de Monte Carlo ou análise de sensibilidade (Brasil, 2019b, p.25).

Na alçada do COMPREP, a avaliação de riscos envolve a identificação das fontes de risco, dos eventos e de sua probabilidade de ocorrência, de suas causas e suas consequências potenciais, das áreas de impacto, das circunstâncias envolvidas, inclusive aquelas relativas a cenários alternativos (Brasil, 2018c, p.28). A avaliação de riscos é feita por meio de análises quantitativas e qualitativas ou da combinação de ambas e, ainda, quanto à sua condição de inerentes (risco bruto, sem considerar qualquer controle) e residuais (considerando os controles identificados e avaliados quanto ao desenho e a sua execução) (Brasil, 2018c, p.29). O nível do risco é apurado de acordo com a seguinte matriz, a qual define os níveis de exposição ao risco do COMPREP, conforme quadro 4.

Quadro 4 – Matriz de riscos do COMPREP



Fonte: (Brasil, 2018c, p.31)

Para a SEFA, a avaliação de riscos consiste na comparação dos resultados da análise dos riscos com os critérios de riscos para determinar se o risco é aceitável, tolerável ou inaceitável (Brasil, 2018b, p.10). No contexto da SEFA, os riscos são qualitativamente estimados por meio análise sob o aspecto de probabilidade e do impacto no caso da ocorrência do evento e segue os preceitos da DCA 16-2 do EMAER (Brasil, 2018b, p.17). Não foi possível constatar o uso de técnicas quantitativas para avaliação do risco pela SEFA.

No DCTA, a avaliação de riscos também consiste na comparação entre os resultados da análise de riscos e os critérios de riscos. A definição dos parâmetros de comparação deve levar em consideração a tolerância ao risco da OM para o objeto da gestão de risco em particular e deve ser definida no Plano de Gerenciamento de Riscos (Brasil, 2018a, p.23). Este Plano deve conter, ao menos, duas classificações para os riscos, a saber:

> a) riscos aceitáveis - categoria de riscos cujo nível foi considerado passível de ser objeto das estratégias de tratamento de aceitação, mitigação ou transferência; e
> b) riscos inaceitáveis - categoria de riscos cujo nível não encontra tratamento compatível com o nível de decisão atual, devendo ser levado à consideração da Alta Direção para decisão de encaminhar ou não para a instância superior.

No âmbito do DCTA a estimativa dos riscos é feita pela análise qualitativa e compreende a análise dos riscos que determina a natureza do risco e o seu nível. O grau de detalhe da análise dos riscos depende da aplicação em particular, da disponibilidade de dados

confiáveis e das necessidades de tomada de decisões da organização (Brasil, 2018a, p.22). Esse detalhamento deve constar do Plano de Gerenciamento de Riscos, devendo conter ao menos:

a) tipologia do risco;

b) probabilidade de ocorrência do risco;

c) impacto da ocorrência do risco; e

d) nível do risco.

Para a categoria ou tipologia do risco, devem ser considerados, entre outros, os seguintes tipos (Brasil, 2018a, p.22):

> a) riscos operacionais - eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. No caso de projetos, este tipo de risco geralmente está associado às próprias áreas de conhecimento do gerenciamento de projetos: um cronograma malfeito; um orçamento com valor base muito aquém do esperado, um escopo sem foco definido etc.
> b) riscos de imagem/reputação do órgão - eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão;
> c) riscos legais - eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;
> d) riscos financeiros/orçamentários - eventos que podem comprometer a capacidade do órgão, entidade ou Projeto de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;
> e) riscos tecnológicos - eventos que podem comprometer o atingimento de objetivos da Organização, do Projeto ou Atividade em curto, médio ou longo prazo, em consequência das decisões de investimento na estrutura de sistemas, materiais e tecnologias. Envolvem eventos críticos de curta duração com amplas consequências, tais como: falhas em sistemas cibernéticos, falhas catastróficas em sistemas devido à baixa maturidade de tecnologias etc.;
> f) risco ambiental - eventos associados a agravos ao meio ambiente, tais como vazamentos ou derramamentos de produtos danosos, contaminação de sistemas naturais por lançamento ou deposição de resíduos químicos, incêndios, explosões etc.;
> g) riscos associados a agentes adversos - eventos desencadeados deliberadamente por opositores ou inimigos inteligentes, tais como sabotagem, ataques cibernéticos, terrorismo, violência política, espionagem, fraudes etc.;
> h) riscos associados a pessoas - eventos decorrentes de perda de talento, fraudes, denúncias infundadas, conflitos trabalhistas, conflitos interpessoais e psicossociais etc.; e
> i) riscos da cadeia de suprimento - eventos ligados a dificuldades de fornecedores e parceiros diversos em se manterem competitivos no mercado.

Não foi possível constatar uso de técnicas quantitativas para avaliação de risco cibernético pelo DCTA.

Para o EMAER, o Planejamento de Respostas aos Riscos é o processo de desenvolver as opções e ações para realçar as oportunidades e reduzir as ameaças aos objetivos do projeto (Brasil, 2017, p.22).

No âmbito do DECEA, os riscos considerados aplicáveis são inseridos no Plano de Tratamento de Riscos. Já os controles de segurança da informação para tratar os riscos devem ser implementados de acordo com o processo de Gestão de Mudanças dependendo da ação de tratamento escolhida (Brasil, 2013b, p.14). Não foi possível localizar estratégia de contingenciamento de riscos da segurança da informação a partir da ICA 7-26 do DECEA.

No COMGEP, o tratamento dos riscos transcorre por meio dos planos de respostas aos riscos que contêm informações sobre como realizar contingência (mitigar ou aceitar os riscos), ações específicas para efetivar a estratégia de contingência, orçamento, cronograma, evento de disparo da execução do plano, responsável pela execução e data da decisão. As respostas aos riscos também devem ter os Riscos Residuais (após execução do Plano de Resposta), Riscos Secundários (gerados pelas respostas aos riscos) e a Aprovação do Plano de Resposta (Brasil, 2019b, p.12).

Na SEFA, as respostas aos riscos são definidas pela estratégia a ser adotada para responder ao evento de risco (aceitar, mitigar/reduzir, transferir ou evitar). Neste plano, basicamente adotaram-se as duas primeiras (aceitar ou reduzir) conforme o nível do risco sob análise, ou seja, se o nível do risco estiver dentro da tolerância ao risco, a estratégia a adotar poderia ser aceitar. Do contrário, adotaria medidas de controle de modo a minimizar a probabilidade e/ou o impacto até que o nível do risco estivesse dentro do apetite a risco, (Brasil, 2018b, p.17). Não foi possível localizar estratégia de contingenciamento de riscos com análise da ICA 12-30 da SEFA.

No COMPREP, as respostas são definidas de forma idêntica à SEFA resumidas na figura 26 (Brasil, 2018c, p.32).

Figura 26 –Respostas aos riscos do COMPREP

Fonte: (Brasil, 2018c, p.32)

No DCTA as respostas aos riscos consistem em desenvolver as opções e ações para realçar as oportunidades e reduzir as ameaças. Essas ações podem envolver a remoção da fonte do risco, a alteração da probabilidade de ocorrência, alteração do impacto das consequências (Brasil, 2018a, p.24).

De uma forma geral os riscos de oportunidades são tratados pelo EMAER, DECEA, COMGEP, SEFA, COMPREP e DCTA como opções a serem exploradas (Brasil, 2017, p.22). No entanto, não é evidenciado como esses riscos de oportunidades podem ser maximizados para suas ocorrências se concretizarem.

No que tange à Implementação de Respostas aos Riscos, a FAB possui Respostas implementadas de acordo com o nível de tolerância da organização, o que significa ações para responder aos eventos em função do nível de risco e da tolerância ao risco de cada OM (Brasil, 2018c, p.33).

O EMAER define a Comunicação dos Riscos como "todas as comunicações e dados necessários para o gerenciamento do risco endereçados aos decisores e participantes relevantes afetos ao projeto ou atividade" (Brasil, 2017, p.07).

No DECEA, a comunicação dos riscos é feita por meio da identificação das partes interessadas e posteriormente realizada a efetiva comunicação associada (Brasil, 2013b, p.15).

No COMGEP, a organização deve estabelecer mecanismos de comunicação interna e reporte, a fim de que componentes-chave da estrutura da gestão de riscos, e quaisquer alterações subsequentes, sejam comunicados. Tais mecanismos devem garantir que as informações pertinentes, derivadas da aplicação da gestão de riscos, estejam acessíveis nos níveis e nos momentos apropriados (Brasil, 2019b, p.10).

No âmbito da SEFA, a comunicação dos riscos para uma maior efetividade do processo de gestão de riscos, deve estabelecer mecanismos efetivos de comunicação e reporte internos e externos (Brasil, 2018b, p.14).

No COMPREP, as informações pertinentes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades com os dados produzidos internamente e também com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão (Brasil, 2018c, p.26).

No DCTA, a gestão de riscos deve estabelecer mecanismos de comunicação e reporte internos e externos, de forma eficaz e rastreável (Brasil, 2018a, p.15).

Todos os grandes comandos avaliados apresentam papéis e responsabilidades bem definidos, elementos essenciais para um bom gerenciamento dos riscos. Todavia, não apresentam de forma explícita previsão orçamentária exclusivamente à gestão de riscos.

Quanto ao monitoramento e controle dos riscos o EMAER define como sendo o processo de acompanhamento da evolução do cenário de riscos afetos ao projeto ou à atividade (Brasil, 2017, p.22).

No DECEA, o monitoramento e controle é visto como a retroalimentação necessária para corrigir e aperfeiçoar o próprio processo. Assim, este subprocesso permite detectar possíveis falhas nos resultados, monitorar os riscos, os controles de segurança da informação e verificar a eficácia do processo de Gestão de Riscos (Brasil, 2013b, p.16).

Para o COMGEP, o monitoramento e controle compreende: identificar, analisar, e planejar-se para riscos novos; monitorar os riscos identificados; analisar novamente os riscos existentes de acordo com as mudanças de contexto; monitorar condições para ativar o Plano de Contingência; e monitorar os riscos residuais (Brasil, 2019b, p.12).

Na SEFA, o monitoramento do gerenciamento dos riscos na OM pode ocorrer por meio da inclusão desse assunto no processo de auditoria interna, anualmente (Brasil, 2018b, p.18).

No COMPREP, o monitoramento e o controle dos riscos têm o objetivo de avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes. Buscam assegurar que funcionem como previsto e que sejam alterados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos (Brasil, 2018c, p.26).

Para o DCTA, o acompanhamento das ações para o tratamento de riscos é realizado comparando a execução definida no Plano de Enfrentamento com a execução efetivamente realizada fornecida pelos relatórios de situação de tratamento e se materializa através de um relatório de status e tendência do tratamento (Brasil, 2018a, p.27).

3.3 Política do Comando da Aeronáutica para Segurança da Informação

Sabe-se que a DCA 14-8 estabelece a Política de Segurança da Informação do Comando da Aeronáutica. Os objetivos e as diretrizes desta política têm por finalidade orientar o planejamento e a execução das ações relacionadas com a Segurança da Informação no âmbito do Comando da Aeronáutica (Brasil, 2013c, p. 7).

Atualmente, a era digital tornou o conteúdo informacional de uma organização seu principal ativo. A informação possui um valor agregado elevado e está sob constante risco (Brasil, 2013c, p. 5). Portanto, a Segurança da Informação e do Conhecimento tornaram-se essenciais para o cumprimento da missão institucional do Comando da Aeronáutica.

A DCA 14-8 - Política de Segurança da Informação do Comando da Aeronáutica foi concebida por meio dos pilares de que a informação é um recurso vital para o Comando da Aeronáutica (Brasil, 2013c, p. 10):

> A Segurança da Informação no COMAER compreende um conjunto de objetivos, diretrizes, normativas gerenciais e técnicas, e demais controles destinados a garantir a confidencialidade, a disponibilidade, a integridade, a irretratabilidade e a autenticidade da informação em todo o seu ciclo de vida, disponibilizada ou em trânsito em ambiente digital

Neste contexto a preocupação com as ameaças e vulnerabilidades de ativos digitais tem sido crescente no Comando da Aeronáutica uma vez que a informatização de processos tem se tornado uma realidade nos últimos anos.

Observa-se que o sucesso das ações de segurança da informação depende diretamente da qualificação de recursos humanos, conscientização do público interno, qualidade das soluções adotadas, e à proteção das informações contra ameaças internas e externas. Há também a necessidade da gestão de riscos dos ativos de informação, conforme documentação normativa coerente com a política prevista na DCA 14-8 e a exploração de novas tecnologias respeitando as diretivas traçadas nesta política (Brasil, 2013c, p. 10).

São traçados cinco objetivos para que o Comando da Aeronáutica possa estabelecer a segurança da informação de forma plena nas suas organizações (Brasil, 2013c, p. 13). O primeiro objetivo visa subsidiar normativamente os elos do Comando da Aeronáutica de forma a garantir os requisitos de confidencialidade, integridade, disponibilidade, autenticidade dos ativos físicos e ativos de informação (Brasil, 2013c, p. 13).

O segundo objetivo visa à capacitação do capital humano dentro do Comando da Aeronáutica de forma a desenvolver as competências técnico-científicas necessárias para condução das atividades relacionadas a segurança da informação (Brasil, 2013c, p. 13). O terceiro objetivo visa ações necessárias ao desenvolvimento, à implementação e ao gerenciamento da segurança dos serviços e dos ativos físicos, dos ativos de informação com vistas à operacionalidade da Força (Brasil, 2013c, p. 13).

O quarto objetivo visa garantir o uso das melhores práticas da segurança da informação por meio do intercâmbio científico-tecnológico entre o COMAER e os órgãos da Administração Pública, da iniciativa privada e demais Forças singulares (Brasil, 2013c, p.

13). O quinto e último objetivo visa garantir a interoperabilidade entre soluções direcionadas para a segurança da informação, no âmbito do COMAER, e deste com as demais Forças singulares e órgãos da Administração Pública (Brasil, 2013c, p. 13).

Existem ainda diversas diretrizes estratégicas traçadas no âmbito do COMAER para que os objetivos sejam alcançados, (Brasil, 2013c, p. 15):

> Estabelecimento de Certificados Digitais;
> Sistema de Inteligência deve possuir requisitos de segurança: recursos criptográficos, de modo a assegurar a autenticidade, a confidencialidade, a integridade e o não repúdio;
> O Sistema de Tecnologia da Informação - STI deve possuir normativas técnicas no gerenciamento do ciclo de vida de sistemas de informação uso de certificados digitais assim como possuir normativas gerenciais que promovam as atividades de gerenciamento de riscos em todas as OM do COMAER;
> O STI deve possuir normativas gerenciais que propiciem a auditoria nos serviços e nos ativos físicos, ativos de informação e ativos de software disponíveis;
> O STI deve possuir programas educativos destinados à conscientização e à capacitação do capital humano, no contexto da Segurança da Informação;
> Sistema de Ensino deve fomentar o desenvolvimento de teses e trabalhos científicos em instituições de ensino superior do País, de interesse do COMAER, os quais estejam voltados para o tema Segurança da Informação;
> Sistema de Ensino deve ter programas dos cursos de formação, de adaptação, de aperfeiçoamento militar e de especialização do COMAER, conteúdos didáticos que visem a disseminar o tema Segurança da Informação;
> O STI deve prever auditorias periódicas nos seus diversos Elos com o intuito de aferir o nível de segurança quanto à utilização, ao armazenamento e ao controle dos serviços e dos ativos físicos, de informação e de software.
> O STI deve conceber, implementar e manter um grupo técnico-especializado - dedicado ao tratamento, controle, monitoramento, análise forense e resposta a incidentes de segurança, no ambiente cibernético;
> Divulgação sobre o tema Segurança da Informação e uso seguro dos recursos computacionais;
> Os sistemas implantados no COMAER devem evitar o uso de sistemas criptográficos de origem estrangeira, devendo ser buscado o desenvolvimento e a adoção de padrões criptográficos conforme normas e demais instruções emitidas pelo Sistema de Inteligência;
> O STI deve fomentar a criação de um núcleo de excelência, no âmbito do COMAER, voltado para a pesquisa e o desenvolvimento de soluções no campo da criptologia;
> O STI deve acompanhar, em âmbitos nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à Segurança da Informação;
> Evolução doutrinária e tecnológica das atividades inerentes à Segurança da Informação;
> Comunicação entre o COMAER e as demais Forças singulares, de modo a facilitar o compartilhamento dos conhecimentos relativos à Segurança da Informação;
> Interoperabilidade - manter padrões de procedimentos e, quando aplicável, de equipamentos, nas soluções de segurança em sistemas de informação;
> O STI deve elaborar e implantar um Modelo de Gestão da Segurança da Informação (MGSI), a ser homologado por meio de publicação complementar a esta Política, contendo diretivas que regulem o gerenciamento sistêmico da segurança da informação no âmbito do COMAER.

As diversas diretrizes estratégicas de defesa cibernética da Força Aérea Brasileira desempenham um papel essencial na garantia da integridade, confidencialidade e disponibilidade dos sistemas e informações críticas da instituição. Elas proporcionam um

quadro estratégico que orienta as ações e investimentos em segurança cibernética, alinhando-as com os objetivos gerais de defesa e segurança do país.

3.4 Procedimentos para Segurança da Informação no Comando da Aeronáutica

No âmbito da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica NSCA 7-13 são definidos os Procedimentos de Segurança e as competências dos elos do Comando da Aeronáutica envolvidos. O primeiro procedimento de segurança da informação a se observar é o Controle de Acesso Físico, ou seja, as instalações que hospedam sistemas de TI devem ter seu acesso controlado e restrito aos indivíduos devidamente autorizados, a fim de garantir a integridade, a confidencialidade e a disponibilidade das informações. Em seguida, há que se observar o procedimento de Controle de Acesso Lógico aos sistemas de TI, que deve ser protegido por meio das medidas dedicadas de segurança, tais como senhas seguras ou, quando necessário, de dispositivos de segurança adicionais, tais como *smart cards*, *tokens* e interfaces com biometria (Brasil, 2013a, p. 19).

Outro procedimento de segurança diz respeito aos Programas Maliciosos. É preciso configurar e instalar nos servidores e nas estações de trabalho de TI, o software antivírus corporativo e outros utilitários de software indicados pelo Comando da Aeronáutica (Brasil, 2013a, p. 19).

O procedimento de segurança relacionado aos Serviços de Rede da INTRAER e da Internet disponibilizados pelas unidades do Comando da Aeronáutica disciplina que estes serviços somente deverão ser utilizados para apoio às atividades de interesse do Comando da Aeronáutica (Brasil, 2013a, p. 20).

A utilização de computadores portáteis será precedida de medidas que visem à orientação dos usuários dos equipamentos e, se necessário, do emprego de soluções de criptografia de dados. É vedado o uso de computador portátil para trato de assuntos sigilosos. Também é vedado o uso de computadores pessoais (particulares) na rede das organizações do Comando da Aeronáutica, salvo as exceções previamente autorizadas pelo Comandante da respectiva Organização Militar (Brasil, 2013a, p. 21).

As instalações físicas e os recursos de TI empregados no desenvolvimento, na realização dos testes e na geração das versões de produção dos sistemas de TI não devem ser os mesmos, estabelecendo-se o maior grau de segregação possível entre esses ambientes

(Brasil, 2013a, p. 21). Lima (2018, p.62) explica a importância da segregação entre ambientes de desenvolvimento, homologação e produção de sistemas de TI. Para o autor a segregação ambientes mantém as alterações de códigos não testados seguros evitando corromper os dados de produção e mantendo a restrição de acesso de cada perfil de acordo com o ambiente que trabalha.

Quanto a Inspeções de Sistemas, devem ser estabelecidos registros em mídia que permitam, posteriormente, a realização de inspeções em atividades de desenvolvimento, operação e manutenção de sistemas aplicativos (Brasil, 2013a, p. 21). Sommerville (2011, p.464) explica como devem ser realizadas as inspeções de programas/sistemas de TI.

> As inspeções de programa envolvem membros de equipe de diferentes origens fazendo uma revisão cuidadosa, linha por linha de código-fonte de programa. Eles procuram defeitos e problemas e os descrevem em uma reunião de inspeção. Os defeitos podem ser erros lógicos, anomalias no código que podem indicar uma condição errada ou recursos que foram omitidos do código. A equipe de revisão examina em detalhes os modelos de projeto ou o código de programa e destaca anomalias e problemas para que sejam reparados.

Há também, procedimentos de segurança relacionado a Colaboradores Terceirizados. Os dispositivos legais utilizados para a contratação de colaboradores terceirizados devem contemplar cláusulas que estabeleçam controles de segurança para os sistemas de TI envolvidos, principalmente as relativas ao estabelecimento de termo de confidencialidade entre as contratadas (Brasil, 2013a, p. 22). Todos os contratos em vigor, que envolvam direta ou indiretamente, acesso a dados sigilosos, deverão ser revisados pelo CIAER (Centro de Inteligência da Aeronáutica) a fim de assegurar que recursos críticos não estejam sendo acessados por pessoal terceirizado não credenciado (Brasil, 2013a, p.22).

No que diz respeito aos procedimentos de segurança relacionados a Monitoramento de Atividades, o CTIR.AER é o responsável pelo tratamento, controle, monitoramento, análise forense e resposta a incidentes de segurança, estando sob coordenação do Órgão Central do STI, que dará ciência imediata ao CIAER, ao respectivo Elo de Coordenação do STI e ao Comandante, Chefe ou Diretor da OM envolvida de incidentes de segurança da informação ocorridos. O CTIR.AER é operado pelo CCABR - Centro de Computação da Aeronáutica de Brasília (Brasil, 2013a, p. 23).

Quanto aos procedimentos de segurança relacionados a Incidentes de Segurança da Informação, devem ser reportados tão logo sejam observados pelo Elo do STI ao SAUTI, quando for o caso, ou diretamente ao CTIR.AER. O Órgão Central do STI, Diretoria de Tecnologia da Informação (DTI), define o processo de atendimento aos incidentes de Segurança da Informação e a prática forense computacional necessária na etapa de coleta de

evidências. Também é responsável por produzir e divulgar conhecimento baseado na análise dos relatórios referentes aos atendimentos a incidentes de Segurança da informação, objetivando eliminar a falha de segurança explorada ou minimizar a ocorrência dessas situações (Brasil, 2013a, p. 23).

O emprego de redes sem fio como solução técnica de TI para atender a atividades ou sistemas de interesse do COMAER só poderá ser efetivado com autorização do Órgão Central do STI, mesmo que estas atividades ou sistemas estejam isolados da INTRAER e que sua operação tenha caráter temporário.

Além disso, os critérios utilizados para emissão de autorização para uso de VoIP são estabelecidos em instrução específica emitida pelo Órgão Central de Telecomunicações, o DECEA (Brasil, 2013a, p. 24). Os critérios utilizados para emissão de autorização para uso de videoconferência também seão estabelecidos em instrução específica emitida pelo DECEA, Órgão Central de Telecomunicações do COMAER (Brasil, 2013a, p. 24).

3.5 Garantia Governamental da Qualidade para Segurança da Informação no Comando da Aeronáutica

O Comando da Aeronáutica tem a incumbência de assegurar a qualidade e a segurança dos sistemas e produtos empregados no cumprimento de seu propósito constitucional e de suas atribuições subsidiárias (Brasil, 2016b, p. 5).

Sistemas são conjuntos de elementos (humanos, materiais e procedimentais) que se inter-relacionam ou interagem para a consecução de determinadas funções ou o atingimento de determinados objetivos (Brasil, 2016b, p.5). Sommerville (2011, p.201) define este tipo de sistema como Sistema Sociotécnico que inclui um ou mais sistemas técnicos, mas, principalmente, também pessoas que entendem o propósito do software dentro do próprio sistema. Os sistemas sociotécnicos definiram que os processos operacionais e as pessoas (os operadores) são partes inerentes do sistema. Eles são regulados por políticas e regras organizacionais e podem ser afetados por restrições externas, como leis e políticas nacionais de regulação.

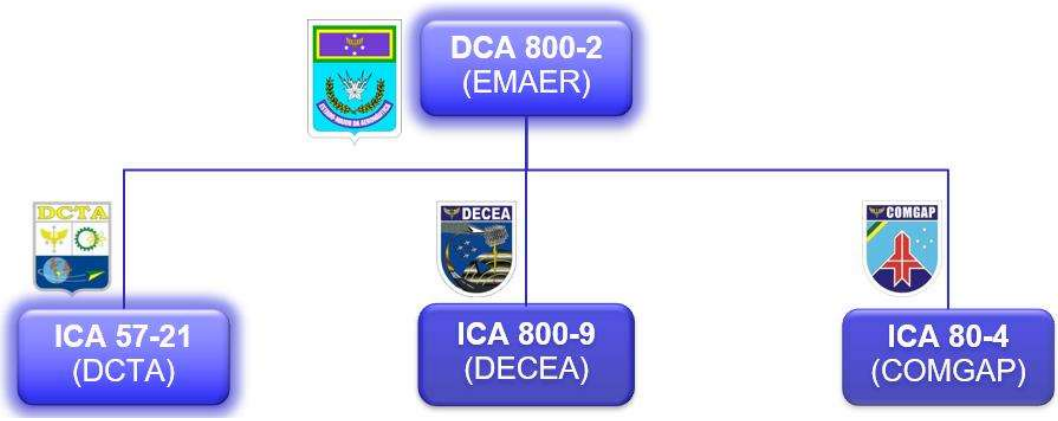
Nesse sentido, a Garantia da Qualidade e da Segurança são disciplinas que visam à gestão de pessoas, processos e produtos inter-relacionados a fim de garantir o atendimento a requisitos e manter a segurança operacional em níveis aceitáveis.

As responsabilidades das organizações certificadoras do COMAER podem ser descritas como (Brasil, 2016b, p.18):

> Regular as atividades relativas à garantia da qualidade e a segurança, cabendo-lhes estabelecer normas e procedimentos e baixar instruções afins em todo o ciclo de vida de produtos e sistemas.
> Garantir a independência e a imparcialidade das atividades de aprovação, certificação, aceitação e outras modalidades de verificação de cumprimento de requisitos por ela estabelecidas.
> Emitir certificados e demais documentos referentes às atividades de sua competência, inclusive para fins de exportação, quando requeridos.

A estrutura Normativa da Garantia Governamental da Qualidade e da Segurança de Sistema e Produtos no COMAER pode ser compreendida no modelo da figura 27.

Figura 27 - Estrutura Normativa da Qualidade e Segurança



Fonte: Elaborado pelo Autor

A DCA 800-2 dispõe sobre a Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER. A ICA 800-9 dispõe sobre "Garantia da Qualidade e da Segurança de Sistemas e Produtos no Âmbito do SISCEAB". A ICA 57-21 dispõe sobre "Regulamento de Aeronavegabilidade Militar - Procedimentos para Certificação de Produto Aeronáutico", no âmbito do Departamento de Ciência e Tecnologia Aeroespacial. A ICA 80-4 dispões sobre certificação de produtos aeronáuticos, bélicos e de infraestrutura e a garantia governamental da qualidade desses produtos, no âmbito do COMGAP.

Não se trata somente de buscar a excelência na operação de sistemas e equipamentos, na prestação de serviços ou na disponibilização de informações. A busca pela qualidade e segurança deve permear todas as fases do ciclo de vida dos produtos, sendo aspecto mandatório em cada programa de aquisição e desenvolvimento de sistemas.

4. Análise dos modelos Três Linhas de Defesa, PRINCE 2 e PMBOK

Neste capítulo é realizada uma análise acerca da convergência dos processos empregados na FAB e o preconizado nos modelos de Três Linhas de Defesa, PRINCE 2 e PMBOK tanto no tratamento de incidentes cibernéticos como na avaliação e gerenciamento dos riscos cibernéticos.

4.1 Análise do Modelo Três Linhas de Defesa

Os processos de Detecção, Triagem e Análise de incidentes cibernéticos caracterizam as funções básicas da atuação da Primeira Linha de Defesa pois detectam, categorizam, e analisam o ataque cibernético mostrando atuação diretamente na parte operacional da FAB que caracteriza a definição de Kogan e Quaresma (2018), que a primeira linha de defesa é responsável por implementar e operacionalizar os controles para mitigar os riscos cibernéticos.

De acordo Lam (2017, p.158), quando as organizações estão seguindo as práticas recomendadas como procedimento operacional padrão, essas unidades estão reduzindo o risco. Veltsos (2017) explica que a primeira linha de defesa engloba o departamento de segurança da informação da organização, assim como as várias unidades de negócios que possuem riscos cibernéticos. O objetivo é que essas unidades reconheçam as vulnerabilidades de seus ativos e a necessidade de gerenciamento dos riscos cibernéticos. A estrutura adotada, denominada CTIR.FAB, sendo operada por uma ETIR Central e uma rede de ETIR Distribuídas demostra que o COMAER apresenta uma Primeira Linha de Defesa sólida e com boa capilaridade dentro da organização pois atende todas as organizações da FAB por meio das ETIR distribuídas e as unidades que não usufruem de uma ETIR distribuída são atendidas diretamente pela ETIR Central.

Culp e Thompson (2016) mostraram que a primeira linha de defesa se resume em três itens chave: Eventos de Risco, Indicadores de Risco Chave (KRI) e Controles da Linha de Frente. Observa-se que os Eventos de Risco são atendidos na etapa de Detecção realizado pelas ETIR do Processo de tratamento de incidentes do CTIR.FAB. Os Indicadores de Risco Chave são contemplados na implementação de mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento pelas ETIR. E os Controles de Linha de frente são implementados pelas ETIR por meio das funções de monitoramento dos incidentes de segurança e comunicação ao CTIR.FAB.

Os procedimentos e normas relativos ao tratamento de incidentes cibernéticos no âmbito do COMAER descritos acima comprovam que FAB possui preocupação com as funções de risco cibernético e conformidade com a segurança da informação evidenciando atendimento a segunda linha de sefesa conforme descreve Lam (2017, p.159), uma vez que a segunda linha de defesa consiste nas funções de risco e conformidade.

De acordo com Telem (2016), a segunda linha de defesa está diretamente ligada aos padrões da organização e é responsável pelas políticas e processos para gerenciamento de riscos. O padrão de operacionalização do CTIR.FAB segue o padrão do CERT.br e está definido e estruturado normativa e operacionalmente obedecendo às legislações do GSIC, elo com o Governo Federal, e da Força Aérea Brasileira, portanto, em consonância com a segunda linha de defesa.

Kogan e Quaresma (2018) mostram que a segunda linha de defesa é responsável por definir as diretrizes e monitorar o cumprimento pela primeira linha de defesa. O CTIR.FAB estabelece os regulamentos e procedimentos a serem adotados quando sistemas de software e hardware que sejam comprovadamente inseguros sejam identificados e orienta as ETIR por meio dos normativos técnicos necessários para o tratamento de incidentes no âmbito do COMAER (Brasil, 2016a, p. 12). O CTIR.FAB monitora o cumprimento da Primeira Linha de defesa por meio do monitoramento e análise técnica dos incidentes de segurança no STI e reportando e/ou se comunicando com os elos quando necessário. Logo a estrutura do CTIR.FAB atende à segunda linha de defesa.

A auditoria interna realizada pelo CENCIAR nas unidades da FAB representa bem uma avaliação dos controles internos da organização conforme prevê Lam (2017, p.160), pois mostra que a terceira linha de defesa deve fornecer uma garantia independente da segunda linha, bem como da primeira linha.

Como sugestão, o CENCIAR poderia orientar a avaliação de riscos, atividades de controles internos, informação, comunicação e monitoramento de forma integrada aos processos de gestão da OM o que caracterizaria uma boa avaliação independente que permeando o ciclo completo de gestão de riscos cibernéticos e revendo de modo minucioso e eficiente as incumbências das duas primeiras linhas de defesa e colaborando para seu aperfeiçoamento, conforme explica Kogan e Quaresma (2018). Portanto, o CENCIAR pode colaborar com o papel correspondente à terceira linha de defesa na FAB em complemento às ações de monitoramento e controle feitas pelo CTIR.FAB.

A aplicação do modelo de Três Linhas de Defesa permite o acompanhamento do incidente cibernético. Observa-se que pelo prisma do Modelo de Três Linhas de Defesa o

processo de tratamento de incidentes cibernético melhora continuamente o processo de gestão dos riscos de segurança da informação previstos pelo PRINCE2 e PMBOK pois se torna um retro alimentador com exemplos reais para a organização aperfeiçoar seus processos.

Pode-se notar que quanto ao aspecto de atendimento às Três Linhas de Defesa, a FAB está bem estruturada e consegue alcançar os objetivos que este modelo preconiza, por meio da estruturação do CTIR.FAB com sua rede de ETIR atendendo bem à primeira e segunda linha de defesa e o CTIR.FAB junto com o CENCIAR cobrindo a terceira linha. Em síntese, a FAB atende ao modelo de três linhas de defesa (tabela 1).

Tabela 1 - Atendimento ao Modelo de Três Linhas de Defesa

Camadas	Previsto no Modelo	Executado na FAB
1ª Linha de Defesa	Controles de linha de frente	✓
2ª Linha de Defesa	Atendimento aos padrões e normas	✓
3ª Linha de Defesa	Auditoria Interna	✓

Fonte: Elaborado pelo autor.

A Força Aérea Brasileira demonstra seu compromisso com a segurança cibernética ao atender plenamente às três linhas de defesa. A primeira linha, representada pelos funcionários e proprietários de processos, é fortalecida por meio de políticas de segurança e conscientização, garantindo que todos os envolvidos estejam aptos a contribuir para a proteção dos ativos digitais. A segunda linha, composta por gestores de riscos e equipes de conformidade, trabalha para desenvolver e implementar políticas e diretrizes de segurança, monitorando continuamente a conformidade com padrões e regulamentos. Finalmente, a terceira linha, com auditoria interna e externa, assegura que as medidas de segurança sejam eficazes e a conformidade seja mantida. A FAB demonstra, assim, um compromisso sólido e abrangente com a segurança cibernética, garantindo a resiliência de seus sistemas e operações em um ambiente digital desafiador.

4.2 Análise dos Modelos PRINCE 2 e PMBOK

Os modelos PRINCE2 e PMBOK oferecem uma perspectiva de gestão de projetos em que a preocupação com o risco nasce com os projetos e os riscos são gerenciados e tratados durante todo o ciclo de vida do projeto.

Ao observar os processos do gerenciamento de riscos previsos no PMBOK (Planejar o gerenciamento dos riscos, identificar os riscos, realizar a análise qualitativa e quantitativa dos riscos, planejar as respostas aos riscos, monitorar e controlar os riscos) a FAB atende o gerenciamento de riscos cibernéticos por meio de sua rede de ETIR e CTIR.FAB. No entanto quando se trata do gerenciamento do riscos cibernéticos antes do projeto estar em execução, ou seja na fase de concepção e projeto do sistema de informação, apenas na análise quantitativa não ficaram claras as ações da SEFA e DCTA, os demais processos do PMBOK foram atendidos quanto ao gerenciamento dos riscos cibernéticos na fase de planejamento para criação de um sistema de informação.

No subprocesso de identificar e analisar *issues* e riscos cibernéticos pode-se verifica que ele desempenha um papel importante na gestão de segurança digital de uma organização. *Issues* são problemas ou incidentes que podem não ser ameaças imediatas, mas que merecem atenção, uma vez que podem evoluir para riscos significativos. Através da identificação e análise cuidadosa dessas questões, bem como dos riscos cibernéticos, as organizações podem tomar medidas preventivas e corretivas oportunas para mitigar potenciais ameaças.

Enquanto se observa na perspectiva do PRINCE2, alguns pontos precisam ser aprimorados. Primeiramente, seria importante os órgãos da FAB que não possuem, preverem as respostas do tipo *Fallback* em seus planos de gerenciamento de risco cibernético. Trata-se de um plano de ações de salvaguarda que pode ser realizado caso o risco vire um óbice. Essas operações ajudariam a minimizar o efeito da ameaça, conforme explica Turley (2022).

Posteriormente, seria importante a FAB aprimorar suas ações para aproveitar as oportunidades que advém com os riscos cibernéticos atuais. Mais especificamente: compartilhar, explorar, ampliar/melhorar/aumentar (AMA) ou rejeitar.

No compartilhamento de oportunidades duas partes dividem os ganhos (com limites previamente acordados) se esse o custo for inferior ao custo planejado e compartilham o prejuízo se o plano de custos for excedido (OGC, 2011, p.90). Esse modelo de compartilhamento de oportunidades de risco cibernético poderia ser estudado pela FAB para aprimorar o uso com as demais Forças e talvez com as agências de segurança.

No que se refere à exploração de oportunidades, significa aproveitar a oportunidade para garantir que será aproveitada e seu benefício gerado (OGC, 2011, p.90). Com base na revisão documental realizada não foi possível identificar indícios claros de que as oportunidades ligadas a riscos cibernéticos são exploradas. A exploração das oportunidades poderá ser aprimorada na FAB no âmbito do gerenciamento e tratamento dos riscos

cibernéticos e representa um potencial que pode alavancar a FAB na defesa cibernética no país.

Referente às ações de ampliar/melhorar/aumentar (AMA) as oportunidades nos riscos cibernéticos, são ações proativas para ampliar a probabilidade que um evento ocorra e ampliar o impacto de um evento se este vier a ocorrer (OGC, 2011, p.90). É importante que no processo de gerenciamento/tratamento riscos cibernéticos na FAB, mantenha a prática na qual quando uma oportunidade reconhecida for identificada, ela seja mapeada como boa prática e ampliada, melhorada e aumentada a fim de tornar os processos de gerenciamento/tratamento de riscos cibernéticos da FAB mais robustos, inovadores e perenes.

Rejeitar uma oportunidade relacionada a risco cibernético, significa uma decisão consciente e deliberada para não explorar ou ampliar uma oportunidade, concluindo que é mais econômico não tentar uma ação para responder à oportunidade, sendo que a oportunidade deve continuar a ser monitorada (OGC, 2011, p.90). Na FAB, tão importante quanto saber explorar a oportunidade certa na hora adequada, é saber rejeitar uma oportunidade que seja inviável naquele momento, no mínimo essa análise de rejeição de oportunidade permite que a alta direção tome uma decisão adequada.

Resumidamente, o quadro 5 representa o atendimento parcial da FAB quanto aos riscos cibernéticos seguindo o preconizado pelo PMBOK e PRINCE2.

Quadro 5 – Atendimento dos modelos PMBOK e PRINCE 2 na FAB

PRINCE2	PMBOK	EMAER	DECEA	COMGEP	SEFA	COMPREP	DCTA
1.Estratégia	1.Planejamento	✓	✓	✓	✓	✓	✓
2.Identificação do Risco	2.Identificação do Risco	✓	✓	✓	✓	✓	✓
3.Avaliação do Risco	3.Avaliação do Risco	✓	✓	✓	✓	✓	✓

3.1Estimativa do Risco (Probabilidade x Impacto x Proximidade)	3.1Análise qualitativa do Risco	✓	✓	✓	✓	✓	✓
3.2 Avaliação do risco geral do projeto	3.2 Realizar a análise quantitativa	✓	✓	✓	✗	✓	✗
4 Planejamento de respostas aos riscos	4 Planejamento de respostas aos riscos	✓	✓	✓	✓	✓	✓
4.1 Evitar	n/a	✓	✓	✓	✓	✓	✓
4.2 Reduzir	n/a	✓	✓	✓	✓	✓	✓
4.3 *Fallback* (contingência caso o risco se materialize)	n/a	✓	✗	✓	✗	✓	✓
4.4 Transferência	n/a	✓	✓	✓	✓	✓	✓
4.5 Aceitação	n/a	✓	✓	✓	✓	✓	✓
4.6 Compartilhar	n/a	✓	✓	✓	✓	✓	✓
4.7 Plano de Respostas a oportunidades	n/a	✓	✓	✓	✓	✓	✓
4.8 Compartilhar – compartilhar lucros e perdas com outra parte	n/a	✗	✗	✗	✗	✗	✗
4.9 Explorar	n/a	✗	✗	✗	✗	✗	✗
4.10 Ampliar/Melhorar/ Aumentar (AMA)	n/a	✗	✗	✗	✗	✗	✗

4.11 Rejeitar	n/a	✗	✗	✗	✗	✗	✗
5. Implementar as Respostas	n/a	✓	✓	✓	✓	✓	✓
6. Comunicar	n/a	✓	✓	✓	✓	✓	✓
7. Orçamento de Risco	n/a	✗	✗	✗	✗	✗	✗
8. Papéis e Responsabilidades	n/a	✓	✓	✓	✓	✓	✓
9. Monitoramento	Monitorar e avaliar	✓	✓	✓	✓	✓	✓

Fonte: Elaborado pelo autor

Pode-se deduzir do quadro 5, que a FAB demonstra sua abordagem sólida no atendimento de estruturas de gerenciamento de projetos, como o PRINCE2 e o PMBOK, no contexto da segurança cibernética. No entanto, há oportunidades de melhoria identificadas. A primeira delas é a necessidade de melhorar o compartilhamento de informações e riscos cibernéticos entre as partes interessadas, garantindo uma compreensão mais abrangente das ameaças e desafios enfrentados. Além disso, é importante aprimorar a avaliação do risco geral dos projetos, garantindo que os riscos cibernéticos sejam devidamente ponderados e considerados em todas as fases. A FAB também pode explorar e ampliar as oportunidades relacionadas aos riscos cibernéticos, identificando maneiras de fortalecer a segurança cibernética de maneira proativa. Ao mesmo tempo, é crucial que a organização saiba rejeitar oportunidades que possam estar associadas a riscos cibernéticos não gerenciáveis. Por fim, a provisão de orçamento para risco cibernético é fundamental, garantindo que recursos estejam disponíveis para mitigar e responder a ameaças digitais, de modo a proteger de forma eficaz os ativos e operações da FAB no ciberespaço.

O uso do modelo de Três Linhas de Defesa em conjunto com o PRINCE2 e PMBOK também irá contribuir em treinamentos da FAB sobre defesa cibernética além de contribuir na elaboração de documentos que inclua defesa cibernética e documentos de requisitos de riscos cibernéticos nas contrações de projetos de interesse do COMAER.

De uma forma geral, como visto anteriormente, a muitos dos processos do PRINCE2 e PMBOK são atendidos pela FAB. No entanto, existem alguns processos que precisam ser melhorados, principalmente os voltados para o PRINCE2.

5. Considerações Finais

Na Força Aérea Brasileira, os riscos cibernéticos estão presentes em todas as organizações e têm impacto direto nos projetos, desde sua concepção até na operação dos sistemas. A gestão destes riscos representa um desafio constante para a FAB. As diversas legislações que tratam o assunto dentro da FAB são consistentes, mas não são perfeitas. Nem sempre conseguem atingir o nível de segurança que o atual contexto de guerra assimétrica presente no ciberespaço exige, pela própria dinâmica da área.

Ao iniciar este trabalho buscou-se analisar como utilizar os modelos PRINCE2, PMBOK e das Três Linhas de Defesas para identificar, tratar e gerenciar os riscos cibernéticos de um sistema, especialmente os sistemas da Força Aérea Brasileira.

Inicialmente, por meio da revisão bibliográfica, foi possível identificar as características da guerra irregular, assimétrica e guerras de 1ª, 2ª, 3ª e 4ª geração assim como as características da guerra cibernética. Observou-se que a guerra cibernética pode ser classificada dentro dos conflitos irregulares, assimétricos e se localizam temporalmente nas guerras de 3ª e 4ª geração. Em seguida foram apresentados os modelos PRINCE2, PMBOK e Três Linhas de defesa e como cada um trata a gestão de riscos cibernéticos.

Posteriormente, foram apresentados como a defesa cibernética é considerada na FAB em termos de tratamento de incidentes cibernéticos (Três Linhas de Defesa), gestão de riscos cibernéticos (aplicação dos modelos PMBOK e PRINCE2), política da informação, procedimentos de segurança, e garantia governamental da qualidade na FAB.

Por fim, foi realizada uma análise mostrando que os processos empregados na FAB estão consoantes com o preconizado pelos modelos de Três Linhas de Defesa, PRINCE 2 e PMBOK tanto no tratamento de incidentes cibernéticos como na avaliação e gerenciamento dos riscos cibernéticos. Cabe ressaltar apenas alguns pontos de melhoria nos processos de gestão de riscos cibernéticos, a saber:

- Melhorar o compartilhamento do risco cibernético;
- Melhorar a avaliação do risco geral do projeto;
- Explorar, Ampliar/Melhorar/Aumentar (AMA) as oportunidades relacionadas aos riscos cibernéticos;
- Saber rejeitar as oportunidades relacionadas ao risco cibernético;
- Provisão de orçamento de risco cibernético.

Deste modo, o objetivo geral deste trabalho foi alcançado pois foi possível realizar a análise da utilização dos modelos PRINCE2, PMBOK e de Três Linhas de Defesa na melhoria da gestão de riscos cibernéticos no Comando da Aeronáutica visando uma melhor governança, considerando ataques cibernéticos em potencial aos ativos de Tecnologia da Informação da FAB.

Quanto o objetivo específico de identificar como está estruturada a defesa cibernética na Força Aérea Brasileira, foi possível atender tendo em vista a estrutura de CTIR.FAB e ETIR detalhada no item 3.1.

Quanto ao objetivo específico de compreender como os modelos PMBOK, PRINCE2 e Três Linhas de Defesa tratam a gestão de riscos cibernéticos foi possível atender por meio do detalhamento desses modelos no item 3.2 e duas análises no item 4.2.

Quanto ao objetivo específico de analisar a utilização dos modelos PMBOK, PRINCE2 e Três Linhas de Defesa na Força Aérea Brasileira, foi possível contemplar visto análise feita no item 4.

Logo, a questão problema levantada: *Como utilizar os modelos PRINCE2, PMBOK e das três linhas de defesas para identificar e tratar os riscos cibernéticos de um sistema?* Pode ser respondida da seguinte forma:

Os modelos PMBOK e PRINCE2 podem ser utilizados no gerenciamento dos projetos e no robustecimento dos processos ligados à gestão da segurança da informação da FAB, pois possuem processos ligados à fase anterior ao acontecimento do incidente permitindo a identificação dos riscos cibernéticos desde o nascimento do projeto. E por meio da manutenção da aplicação do modelo das Três Linhas de Defesa, que continuará tratando os riscos cibernéticos dos sistemas da FAB a partir do Centro de Tratamento de Incidentes de Rede da Força Aérea Brasileira (CTIR.FAB) e das Equipes de Tratamento de Incidentes de Segurança em Redes Computacionais (ETIR) conforme detalhado no item 3.1.1, ou seja, uma abordagem reativa voltada para o pós acontecimento do incidente cibernético. Desta forma, o risco cibernético é previsto, tratado desde a origem do projeto e mitigado caso vier a se concretizar quando da implantação do sistema.

As metodologias PRINCE2, PMBOK e Três Linhas de Defesa fornecem estruturas sólidas para o planejamento, execução e monitoramento de projetos de segurança cibernética, garantindo a incorporação de boas práticas e a consideração abrangente de riscos em todas as fases do projeto. Além disso, o modelo de Três Linhas de Defesa na FAB, materializado pela estruturação da rede de ETIR, facilita a integração eficaz de todas as partes interessadas,

garantindo que os riscos cibernéticos sejam devidamente avaliados e gerenciados em todos os níveis da organização. Isso não apenas aumenta a eficiência na resposta a incidentes cibernéticos, mas também promove uma cultura de melhoria contínua, e a aprendizagem com incidentes anteriores contribui para fortalecer a postura de segurança cibernética da FAB

Com o uso dessas metodologias será possível melhorar tanto a gestão dos projetos que envolvem riscos cibernéticos assim como permitir a melhoria contínua do tratamento dos riscos nos diversos níveis dentro das organizações da FAB.

Dessa forma a hipótese levantada de que os modelos PRINCE2, PMBOK e de Três Linhas de Defesa contribuirão para a Força Aérea Brasileira aprimorar a gestão dos riscos cibernéticos relacionados aos ativos de Tecnologia da Informação, pode ser comprovada como verdadeira mediante a conclusões apontadas anteriormente.

Vislumbra-se como possibilidade de trabalhos futuros trabalhos, estudos sobre a utilização dos modelos aqui apresentados em outros países da Ásia, Europa e América, no tratamento de riscos cibernéticos nas forças armadas desses países.

Poder-se-á ainda sugerir como trabalhos futuros, o CENCIAR incorporar a auditoria do processo de gestão dos riscos cibernéticos do CTIR.FAB em seus processos de auditoria interna.

REFERÊNCIAS

ANDERSON, D. J. e EUBANKS, G. **Guerra Cibernética. Leveraging COSO Across the Three Lines of Defense.** The Institute of Internal Auditors 2015.

BALLARD, C. , *et al.* **Information Governance Principles and Practices for a Big Data Landscape**. 1ª ed. Poughkeepsie: IBM Redbooks, 2014.

BALTAZAR, M. **Brainwriting: o que é, quais as melhores técnicas e as diferenças para um brainstorm**. ROCKCONTENT, 2019. Disponível em: < https://rockcontent.com/br/blog/brainwriting/>. Acesso em: 12 fev. 2021.

BATTISTA, A. *et al*. **The Global Risks Report 2023**. Fórum Econômico Mundial, Jan 2023.

BETZ, D. J. e STEVENS, T. **Cyberspace and the State: Towards a Strategy for Cyber-Power**. 1ª ed. Londres: Routledge, 2012.

BOSCO, N. **Ataque de hackers ao STJ é o mais grave da história no país**. Correio Braziliense, 2020. Disponível em: < https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html/>. Acesso em: 12 out. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República [2016]. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 23 jul. 2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. **Diário Oficial da União**: seção 1, p. 6. Brasília, DF, 18 junho. 2008.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Portaria Normativa nº 666/MD, de 4 de agosto de 2010. Cria o Centro de Defesa Cibernética do Exército e dá outras providências. **Boletim do Exército**: n° 31. Brasília, DF, 6 agosto. 2010.

BRASIL. Ministério da Defesa. Estado-Maior da Aeronáutica. Portaria normativa nº 278/GC3, de 21 de junho de 2012. Aprova a reedição da Doutrina Básica da Força Aérea Brasileira (DCA 1-1). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 121, 26 junho. 2012a.

BRASIL. Ministério da Defesa. Comando do Exército. Portaria Normativa nº 3.028/MD, de 14 de novembro de 2012. Atribui ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa

cibernética, no âmbito do Ministério da Defesa. **Diário Oficial da União**: seção 1. Brasília, DF, nº 223, 20 novembro. 2012b.

BRASIL. Ministério da Defesa. Gabinete do Ministro. Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Dispõe sobre a Política Cibernética de Defesa (MD31-P-02**). Diário Oficial da União**: seção 1, p. 11. Brasília, DF, nº 249, 27 dezembro. 2012c.

BRASIL. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF, 2012d. Disponível em: <http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 23 jul. 2017.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria COMGAP nº 31/3EM, de 06 de maio de 2013. Aprova a reedição da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 088, 09 maio. 2013a.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria DECEA nº 59/DGCEA, de 24 de maio de 2013. Aprova a edição da Instrução acerca do Processo de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo (ICA 7-26). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 120, 26 junho. 2013b.

BRASIL. Ministério da Defesa. Comando da Aeronáutica**.** Portaria EMAER nº 1.966/GC3, de 30 de outubro de 2013. Aprova a reedição da Diretriz que estabelece a Política de Segurança da Informação do Comando da Aeronáutica (DCA 14-8**). Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 210, 01 novembro. 2013c.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Portaria normativa nº 3.010/MD, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética (MD31-M-07). **Diário Oficial da União**: Brasília, DF, nº 224, 18 novembro. 2014.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria EMAER nº 41/3SC, de 9 de setembro de 2016. Aprova a edição da Instrução que trata do Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica (ICA 7-42). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 161, 21 setembro. 2016a.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria EMAER nº 1164/GC3, de 19 de setembro de 2016. Aprova a reedição da Diretriz que dispõe sobre a Garantia da Qualidade e da Segurança de Sistemas e Produtos no COMAER (DCA 800-2). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 161, 21 setembro. 2016b.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria EMAER nº 70/7SC, de 04 de outubro de 2017. Aprova a edição da Diretriz que dispõe sobre a Gestão de Riscos no Comando da Aeronáutica (DCA 16-2). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 185, 27 outubro 2017.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria DCTA nº 32/SCPL, de 23 de janeiro de 2018. Aprova a reedição da Instrução que trata da Gestão de Riscos no DCTA (ICA 80-13). **Boletim do Comando da Aeronáutica**, São José dos Campos, BCA n. 020, 05 fevereiro 2018a.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria SEFA nº 68/AJUR, de 16 de julho de 2018. Aprova a edição da Instrução que trata da Gestão de Riscos na Secretaria de Economia, Finanças e Administração da Aeronáutica (ICA 12-30). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 125, 23 julho 2018b.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria COMPREP nº 160/ EMPREP-10, de 28 de setembro de 2018. Aprova a edição da ICA 16-3 que dispõe sobre orientações para a elaboração da Gestão de Riscos no Comando de Preparo (ICA 16-3). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 175, 4 outubro 2018c.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria nº 425/GC3, de 18 de março de 2019. Aprova a reedição da Norma do Sistema de Controles Internos da Aeronáutica. (NSCA 179-1). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 045, 20 março. 2019a.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Portaria COMGEP nº 546/AGESTÃO, de 02 de abril de 2019. Aprova a Instrução que trata da Gestão de Riscos do COMGEP. (ICA 16-1). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, BCA n. 061, 12 abril. 2019b.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. **Gestão de Riscos de Segurança da Informação do Departamento de Controle do Espaço Aéreo (DCA 7-3).** Brasília, DF, 2022a. Disponível em: < https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=33176>. Acesso em: 10 mar. 2023.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. **Diretriz de Gestão de Riscos no Comando da Aeronáutica (DCA 16-2).** Brasília, DF, 2022b. Disponível em:<https://www.sislaer.fab.mil.br/terminalcendoc/Busca/Download?codigoArquivo=34267>. Acesso em: 10 mar. 2023.

BRASIL. **CTIR.FAB – Centro de Tratamento de Incidentes de Rede**. Brasília, DF, 2021. Disponível em: < https://www2.fab.mil.br/ctir/index.php/missao-visao-e-valores>. Acesso em: 04 jan. 2021.

CARR, J. **Inside Cyber Warfare**. 1ª ed. Sebastopol: O'Reilly Media, 2009.

CARVALHO, B. R. **Metodologia Bow Tie ou Gravata Borboleta na Logística**. Logísticos Oficial, 2015. Disponível em: < https://www.logisticosoficial.com/post/2015/09/05/metodologia-bow-tie-ou-gravata-borboleta/>. Acesso em: 21 fev. 2021.

CERT.BR. **Núcleo de Informação e Coordenação do Ponto BR**. Brasília, DF, 2021. Disponível em: < https://www.cert.br/docs/certbr-faq.html#6>. Acesso em: 10 jan. 2021.

CHEUNG, S. *et al*. **Modeling Multistep Cyber Attacks for Scenario Recognition**. Proceedings of the DARPA Information Survivability Conference and Exposition, Washington, DC, USA, pp. 284-292, 2003.

CLARKE, J. SQL Injection Attacks and Defense. 2ª ed. Waltham: Elsevier, 2012.

CLARKE, R. A. e KNAKE, R. K. **Guerra Cibernética. A próxima ameaça à segurança e o que fazer a respeito**. 1ª ed. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, C. V. **Da Guerra**. 3ª ed. São Paulo - SP: Tahyu, 1984.

CULP, S. e THOMPSON C. **The Convergence of Operational Risk and Cyber Security.** Accenture Finance & Risk Services, 2016. Disponível em:<https://www.accenture.com/t20180529T062258Z__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf> Acesso em: 24 out. 2018.

DEFESA CIBERNÉTICA. **Em segundo lugar, Brasil lidera ranking como país mais atingido por ciberataques na américa latina**. Portal DCIBER, 2023. Disponível em: <https://dciber.org/em-segundo-lugar-brasil-lidera-ranking-como-pais-mais-atingindo-por-ciberataques-na-america-latina//>. Acesso em: 13 out. 2023.

DEFESA CIBERNÉTICA. **No Brasil, 80% das empresas não se adequaram à LGPD**. Portal DCIBER, 2023. Disponível em: <https://dciber.org/no-brasil-80-das-empresas-nao-se-adequaram-a-lgpd-2/>. Acesso em: 15 out. 2023.

DECATRON. **Defesa Cibernética - SIMOC**. Disponível em: https://www.decatron.com.br/index.php/portfolio/defesa-cibernetica-simoc/. Acesso em: 10 jan. 2020.

DIGNUM, V. Responsible Artificial Intelligence - How to Develop and Use AI in a Responsible Way. Artificial Intelligence: Foundations, Theory, and Algorithms. Springer, 2019., p.18)

DORNELLES JR., A. C. **A modernização militar da China e a distribuição de poder no Leste Asiático**. Contexto Internacional., Rio de Janeiro , v. 36, n. 1, p. 145-170, Junho 2014 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292014000100005&lng=en&nrm=iso>. Acesso em: 18 out. 2018.

DOUHET, G. **O domínio do ar**. 2ª ed. Rio de Janeiro - RJ: Editora Itatiaia, 1988.

FADOK, D. S. **John Boyd e John Warden. A busca da paralisia estratégica pelo poder aéreo**. Air University Press, 2001.

FERREIRA, Ivette Senise. A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes. Editora Edipro, 2011.

GRAÇA, R. B. **Regulação da Guerra Cibernética e o Estado Democrático de Direito no Brasil.** Revista de Direito, Estado e Telecomunicações, v. 6, n. 1, p. 63-86 (2014).

GOMES, Luiz Flávio. Crimes informáticos. 2000. Disponível em: www.ibcrim.org.br. Acesso em: 15 out. 2020.

HJARVARD, Stig; LÖVHEIM, Mia (eds.). **Mediatization and Religion**: Nordic.

HJARVARD, Stig. **The study of news production**. *In*: JENSEN, Klaus Bruhn (ed.), A Handbook of Media and Communication Research, 2ed. Londres: Routledge, p. 87-105, 2012ª Perspectives. Gothenburg: Nordicom, p. 21-44, 2012b

HEYDTE, Friedrich August, Freiherr von der, A Guerra irregular moderna em políticas de defesa e como fenômeno militar. Tradução de Jayme Taddei. Rio de Janeiro: Biblioteca do Exército, 1990.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. **As três linhas de defesa no gerenciamento eficaz de riscos e controles**. Disponível em: <http://www.planejamento.gov.br/assuntos/empresas-estatais/palestras-e-apresentacoes/2-complemento-papeis-das-areas-de-gestao-de-riscos-controles-internos-e-auditoria-interna.pdf>. Acesso em: 18 out. 2018.

ITGI - IT Governance Institute™. **Cobit 4.1**. 1ª ed. USA, 2007.

JORGE, B. W. G. A. **Estados Unidos, poder cibernético e a "guerra cibernética": Do Worm Stuxnet ao Malware Flame/Skywiper – e além.** Boletim Meridiano 47, vol. 13, n. 131, p. 43-48, 2012.

KOGAN, S. e QUARESMA, H. **Integração da gestão de riscos cibernéticos nas três linhas de defesa**. IBGC Análises & Tendências, São Paulo, v. 1, n. 4, p. 5-7, Jul 2018. Disponivel em: <http://www.bibliotecadeseguranca.com.br/wp-content/uploads/2018/08/ibcg-analises-e-tendencias-gerenciamento-de-riscos-no-4-2018.pdf>. Acesso em: 24 out. 2018.

LAM, J. **Implementing Enterprise Risk Management: From Methods to Applications**. 1ª ed. Nova Jersey: John Wiley & Sons Nova Jersey, 2017.

LEVY, P. **Cibercultura**. 1ª ed. São Paulo: Editora 34, 1999.

LIBICKI, M. **Cyberdeterrence and Cyberwar**. 1ª ed. Santa Monica - CA: RAND Corporation, 2009.

LIMA, A. **Gestão da segurança e infraestrutura de tecnologia da informação**. 1ª ed. São Paulo: Editora Senac São Paulo, 2018.

LINDSAY, J. R. Et al. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1ª ed. New York: Oxford University Press, 2015.

MAALI, M. e SCHWARTZ, B. **Governance Risk and Compliance (GRC) technology: Enabling the three lines of defense.** PwC Global, 2016. Disponível em:<https://www.pwc.com/us/en/risk-assurance/publications/grc-technology-three-lines-defense.pdf> Acesso em: 24 out. 2018.

MACHANIC, A. Et al. Expert SQL Server 2005 Development. 1ª ed. New York: Apress, 2007.

MILHAZES, J. **O monumento da discórdia russo-estónia**. Disponível em: <http://darussia.blogspot.com.br/2007/04/o-monumento-da-discrdia-russo-estnia.html> Acesso em: 27 jul. 2017.

MULCAHY, R. **Rita's Course in a Book**. 1ª ed. EUA: RMC Publications, 2011.

NEILPATEL. **Brainstorming: O Que É, Como Fazer (Passo a Passo)**. Neipatel, 2021. Disponível em: < https://neilpatel.com/br/blog/o-que-e-brainstorming/>. Acesso em: 08 fev. 2021.

OFFICE OF GOVERNMENT COMMERCE-OGS. **Gerenciando Projetos de Sucessos com PRINCE2™**. 1ª ed. United Kington, TSO, 2011.

PROJECT MANAGEMENT INSTITUTE-PMI. **Um Guia do Conhecimento em Gerenciamento de Projetos**. Guia PMBOK 6ª ed. Pensilvânia: Project Management Institute, 2017.

RAZA, S. **A Cassandra Cibernética ou Porque Estamos na Contramão da Tecnologia e Ninguém no Governo Quer Acreditar**. Disponível em: <https://www.sul21.com.br/opiniaopublica/2013/11/cassandra-cibernetica-ou-porque-estamos-na-contramao-da-tecnologia-e-ninguem-governo-quer-acreditar-por-salvador-raza/> Acesso em: 09 jun. 2018.

REVISTA EM DISCUSSÃO – SENADO FEDERAL. **Espionagem de aliados expõe poder dos EUA**., no.21, p.12, Julho. 2014.

VASCONCLEOS, R. Ativismo x espionagem: relembre a polêmica entre Assange, Wikileaks e EUA. UOL – Fique por Dentro, 2022. Disponível em: < https://www.uol.com.br/tilt/noticias/redacao/2022/06/17/hacker-programador-jornalista-e-ativista-assange-e-a-polemica-wikileaks.htm#:~:text=A%20WikiLeaks%20%C3%A9%20considerada%20por,e%2C%20at%C3%A9%20ent%C3%A3o%2C%20secretas/>. Acesso em: 13 out. 2023.

SAKUDE, M. **ITA LAB C² Laboratório de Comando e Controle**. São José dos Campo, SP, 2015. Disponível em: <http://www.labc2.ita.br/cc.html>. Acesso em: 10 out. 2019.

SINGH, A. *et al*. **Vulnerability Analysis and Defense for the Internet**. 1ª ed. Fairfax: Springer US, 2008.

SINGER, P. W. e FRIEDMAN A. **Cybersecurity and cyberwar : what everyone needs to know**. 1ª ed. New York: Oxford University Press, 2014.

SINGER, P. W. e BROOKING E. T. **LikeWar - The Weaponization of Social Media**. Boston, New York: Houghton Mifflin Harcourt Publishing Company, 2018.

SITEWARE. **Entenda o que é compliance nas empresas e a importância desse conceito**. Siteware, 2017. Disponível em: <https://www.siteware.com.br/processos/o-que-e-compliance-nas-empresas/>. Acesso em: 08 jan. 2021.

SOMMERVILLE, I. **Engenharia de Software**. 9ª ed. São Paulo: Pearson Prentice Hall, 2011.

TRIBUNAL DE CONTAS DA UNIÃO. **Gestão de riscos: modelos de referência**. Portal TCU, 2019. Disponível em: <https://portal.tcu.gov.br/governanca/governancapublica/gestao-de-riscos/modelos.htm#IIA>. Acesso em: 09 dez. 2019.

TELEM, D. **The three lines of defense: Making the transition to a mature risk management model.** KPMG International Cooperative, 2016. Disponível em:<https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2017/01/three-lines-of-defense-kpmg.pdf> Acesso em: 24 out. 2018.

TRIBUNAL SUPRIOR ELEITORAL. **Gestão de riscos: modelos de referência**. Portal TSE, 2020. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2020/Novembro/tentativas-de-ataques-de-hackers-ao-sistema-do-tse-nao-afetaram-resultados-das-eleicoes-afirma-barroso>. Acesso em: 13 out. 2023.

TURLEY, F. **Risco.** Lovânia, Bélgica, 2022. Disponível em:< https://prince2.wiki/pt/temas/risco/> Acesso em: 17 jan. 2022.

VARELLA, L. Et al. **Como se Tornar um Profissional em Gerenciamento de Projetos**. 2ª ed. Rio de Janeiro-RJ: QualityMark, 2005.

VARGAS, R. V. **Gerenciamento de Projetos: Estabelecendo diferenciais competitivos**. 7ª ed. Rio de Janeiro: Brasport, 2009.

VELTSOS, C. **Take a Load Off: Delegate Cyber Risk Management Using the Three Lines of Defense Model.** Security Intelligence Security, Nov. 2017. Disponível em:<https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-the-three-lines-of-defense-model> Acesso em: 24 out. 2018.

VIANNA, E. W. **CDCIBER: perspectivas em face da espionagem eletrônica**. 2014. 31 slides. Disponível em: <https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviiicedn.pdf>. Acesso em: 13 jan. 2020.

VISACRO, A. **Guerra irregular: Terrorismo, guerrilha e movimentos de resistência ao longo da história**. 1ª ed. São Paulo - SP: Editora Contexto, 2009.

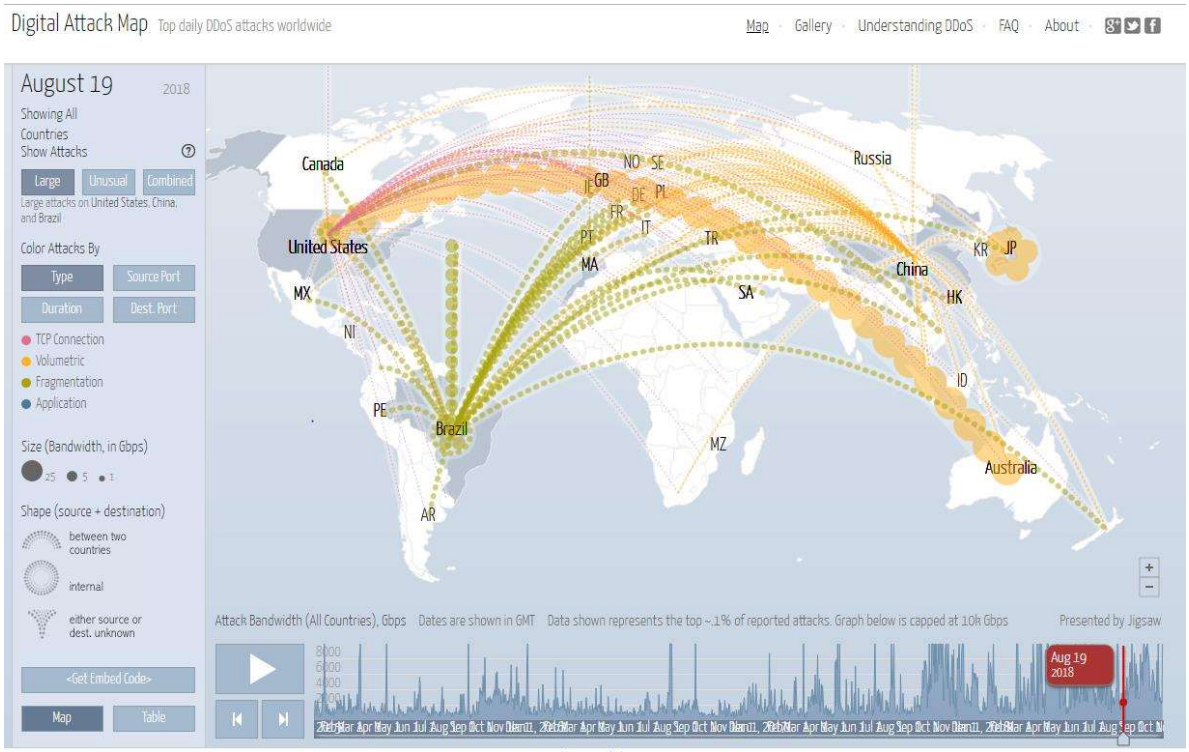
VISACRO, A. **O Desafio da Transformação**. Military Review. Kansas - EUA: Centro De Armas Combinadas Forte Leavenworth, vol. 2, p.46 - 55, março-abril 2011.

WINTER, L. M. **A concepção de Estado e de poder político em Maquiavel**. Tempo da Ciência, vol. 13, p.117-128, 1º semestre 2006.

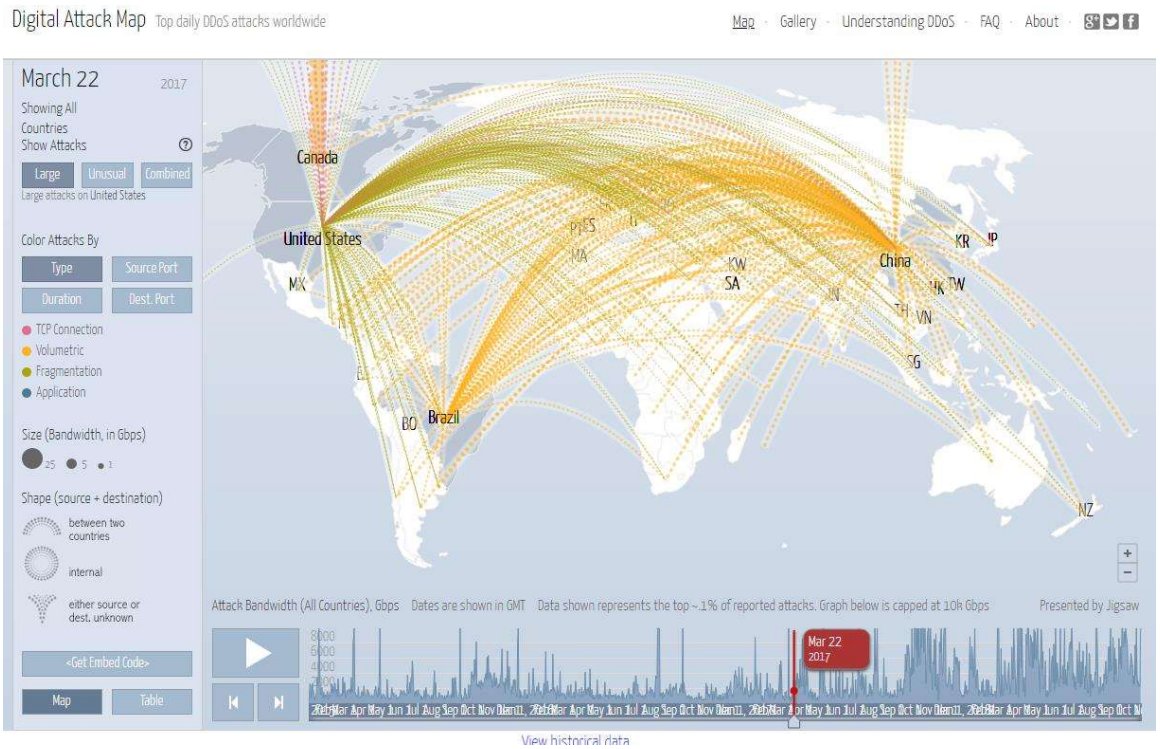
ZENDRON, S. **Cultura da segurança da informação é a chave para superar pandemia de ataques cibernéticos,** 2023. Disponível em: < https://dciber.org/cultura-da-seguranca-da-informacao-e-a-chave-para-superar-pandemia-de-ataques-ciberneticos/>. Acesso em: 15 out. 2023.

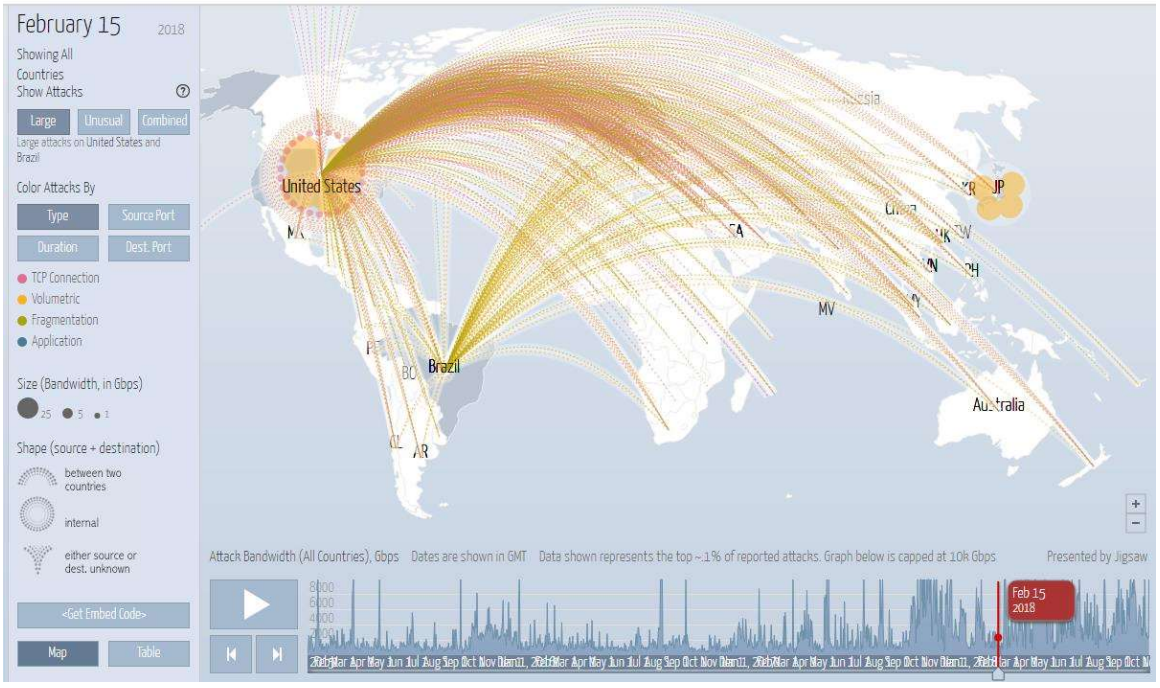
ANEXO A - Mapa de Ataques digitais

Este mapa traz os principais ataques diários de DDoS[17] em todo o mundo assim como sua visualização histórica ao longo dos anos. Este mapa pode ser visualizado por meio do site <http://www.digitalattackmap.com> e foi criado pela *Arbor Networks* , uma empresa de software fundada em 2000 e com sede em Massachusetts, Estados Unidos em parceria com a Google.



[17] Ataque distribuído de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus usuários por meio da inundação do sistema com uma grande quantidade de requisições proveniente de diversos locais diferentes.


Digital Attack Map
Top daily DDoS attacks worldwide
Map · Gallery · Understanding DDoS · FAQ · About
March 22
2017
Showing All Countries
Show Attacks
Large
Unusual
Combined
Large attacks on United States
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
Shape (source + destination)
between two countries
internal
either source or dest. unknown
<Get Embed Code>
Map
Table
Canada
United States
MX
Brazil
BO
China
KR
JP
TW
VN
SG
NZ
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~1% of reported attacks. Graph below is capped at 10k Gbps
Presented by Jigsaw
Mar 22
2017
View historical data


February 15
2018
Showing All Countries
Show Attacks
Large
Unusual
Combined
Large attacks on United States and Brazil
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
Shape (source + destination)
between two countries
internal
either source or dest. unknown
<Get Embed Code>
Map
Table
United States
MX
Brazil
BO
AR
MV
Australia
JP
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~1% of reported attacks. Graph below is capped at 10k Gbps
Presented by Jigsaw
Feb 15
2018