ESCOLA DE GUERRA NAVAL

CMG(EN) HELIO MENDES SALMON

GESTÃO DE RISCOS CIBERNÉTICOS OPERACIONAIS:
Uma proposta para o aumento da capacidade cibernética da MB

Rio de Janeiro

2025

CMG(EN) HELIO MENDES SALMON

GESTÃO DE RISCOS CIBERNÉTICOS OPERACIONAIS:

Uma proposta para o aumento da capacidade cibernética da MB

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas (C-PEM).

Orientador: CMG(RM1-FN) Jorge Luís de Araujo Mello

Rio de Janeiro

Escola de Guerra Naval

2025

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

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

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

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

gov.br
Documento assinado digitalmente
HELIO MENDES SALMON
Data: 22/10/2025 10:55:07-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

Em primeiro lugar, a Deus pela saúde e por iluminar meu caminho.

Aos meus pais pela educação, apoio, incentivo e sacrifícios.

A minha esposa Andréa e aos meus filhos, Isabella e Arthur, pela compreensão e paciência ao longo deste ano. Vocês são o meu “porto seguro”.

À Marinha do Brasil por mais este curso, que me proporcionou agregar mais conhecimentos, contribuindo com a minha capacitação profissional e pessoal.

À Escola de Guerra Naval (EGN), especialmente nas pessoas do CMG (RM1) Alexandre Motta de Sousa e do CF Ribeiro Costa, assim como de toda sua equipe, pelas orientações e coordenações ao longo do ano.

Ao amigo CMG Humberto Ferreira Ramos Junior, que gentilmente aceitou fazer parte desta jornada assumindo o papel de revisor externo.

Ao meu orientador, CMG (RM1-FN) Jorge Luís de Araujo Mello, pelas orientações e correções assertivas, sempre indicando o rumo a seguir, servindo de “norte” para esta jornada e sendo fundamental para o sucesso deste trabalho.

Ao CF (RM1) Ohara Barbosa Nagashima, que com uma folha de papel “A3”, tirou este oficial das profundezas da dúvida e acendeu aquela “luz acadêmica”, fazendo com que este trabalho zarpasse.

Aos amigos da Turma C-PEM 2025, pelos excelentes momentos que passamos juntos ao longo deste ano! Desejo bons ventos a todos para que alcancem seus objetivos pessoais!

“Risk is a choice rather than a fate.”
Peter L Bernstein

RESUMO

A crescente dependência tecnológica da Marinha do Brasil (MB), impulsionada por seus projetos estratégicos, como as Fragatas Classe Tamandaré, o Submarino Nuclear Convencionalmente Armado (SNCA) e o Sistema de Gerenciamento da Amazônia Azul (SisGAAz), trouxe ganhos operacionais, mas também ampliou significativamente a exposição a riscos cibernéticos operacionais. Este trabalho tem como objetivo propor a implementação da Gestão do Risco Operacional (GRO) na MB, com foco no risco cibernético operacional, como instrumento para fortalecer a capacidade cibernética, proteger ativos críticos e assegurar a continuidade das operações. A metodologia adotada baseou-se na análise comparativa entre o modelo da Marinha dos Estados Unidos (USNAVY), consolidado pela norma OPNAVINST 3500.39D, e a situação atual da MB, observando os domínios de pessoas, processos, tecnologias e eventos externos. O diagnóstico evidenciou que, enquanto a USNAVY aplica a GRO de forma abrangente, tanto no ambiente administrativo quanto no operacional e cibernético, a MB mantém uma abordagem restrita, focada em aspectos administrativos e com lacunas relevantes na proteção dos Sistemas Digitais Operativos (SDO) e das infraestruturas críticas. Como resultado, são apresentadas propostas estruturadas para a criação de uma norma específica de GRO, de uma estrutura organizacional dedicada, da integração de *frameworks* internacionais (NIST e ABNT) e da implementação de um sistema informatizado de gestão de riscos, elevando a resiliência e a segurança cibernética da MB, além de recomendar a formalização do conceito de risco operacional no Glossário das Forças Armadas.

Palavras-chave: Gestão do Risco Operacional; Risco Cibernético Operacional; Marinha do Brasil; Resiliência Operacional; Segurança Cibernética.

ABSTRACT

OPERATIONAL CYBER RISK MANAGEMENT:
A proposal for increasing the Brazilian Navy's cyber capability

The growing technological dependence of the Brazilian Navy (MB), driven by its strategic projects, such as the Tamandaré Class Frigates, the Conventionally Armed Nuclear Submarine (SNCA) and the Blue Amazon Management System (SisGAAz), has brought operational gains, but has also significantly increased exposure to operational cyber risks. This paper aims to propose the implementation of Operational Risk Management (ORM) in the MB, focusing on operational cyber risk, as an instrument to strengthen cyber capability, protect critical assets and ensure the continuity of operations. The methodology adopted was based on the comparative analysis between the United States Navy (USNAVY) model, consolidated by the OPNAVINST 3500.39D standard, and the current situation of the MB, observing the domains of people, processes, technologies and external events. The diagnosis showed that, while USNAVY applies ORM comprehensively, both in the administrative and operational and cyber environments, the Navy maintains a restricted approach, focused on administrative aspects and with relevant gaps in the protection of Digital Operating Systems (DOS) and critical infrastructures. As a result, structured proposals are presented for the creation of a specific ORM standard, a dedicated organizational structure, the integration of international frameworks (NIST and ABNT) and the implementation of a computerized risk management system, increasing the resilience and cybersecurity of the Navy, in addition to recommending the formalization of the concept of operational risk in the Glossary of the Armed Forces.

Keywords: Operational Risk Management; Operational Cyber Risk; Brazilian Navy; Operational Resilience; Cybersecurity.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
ARMADAINST	Instruções para Implementação da Política de Gestão de Riscos da MB
BI	*Business Intelligence*
BIS	*Bank for International Settlements* (Banco de Compensações Internacionais)
C5IVR	Comando, Controle, Comunicações, Computação, Cibernético, Inteligência, Vigilância e Reconhecimento
C4ISR	Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento
CIDOC	Comissão Interescolar de Doutrina de Operações Conjuntas
CINDACTA	Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo
CSCMP	*Council of Supply Chain Management Professionals*
DoD	*Department of Defense* (Departamento de Defesa dos EUA)
DGMM	Diretoria-Geral do Material da Marinha
EMA	Estado-Maior da Armada
EMA-310	Estratégia de Defesa Marítima
EMA-419	Doutrina Cibernética da Marinha
EMCFA	Estado-Maior Conjunto das Forças Armadas
EMCj	Estado-Maior Conjunto
EMGEPRON	Empresa Gerencial de Projetos Navais
ESG	Escola Superior de Guerra
FCT	Fragatas Classe Tamandaré
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
GRO	Gestão do Risco Operacional
HM&E	*Hull, Mechanical and Electrical* (Casco, Mecânicos e Elétricos)
ICS	*Industrial Control Systems* (Sistemas de Controle Industrial)
MD	Ministério da Defesa
MB	Marinha do Brasil
NIST	*National Institute of Standards and Technol*ogy (Instituto Nacional de Padrões e Tecnologia dos EUA)

NAVPLAN	*Naval Plan* (Plano Naval dos EUA)
NAVSAFECOM	*Naval Safety Command* (Comando de Segurança Naval da USNAVY)
NPS	*Naval Postgraduate School* (Escola de Pós-Graduação Naval dos EUA)
ODG	Órgão de Direção Geral
ODS	Órgão de Direção Setorial
OPNAVINST	*Office of the Chief of Naval Operations Instruction* (Escritório de Instrução do Chefe de Operações Navais da USNAVY)
OT	*Operational Technology* (Tecnologia Operacional)
PEM 2040	Plano Estratégico da Marinha
PIT	Platform IT (Tecnologia de Informação de Plataforma)
PGR	Plano de Gerenciamento de Riscos
QBRN	Químico, Biológico, Radiológico e Nuclear
RDT&E	*Research, Development, Test and Evaluation* (Pesquisa, Desenvolvimento, Teste e Avaliação)
RECIM	Rede de Comunicações Integrada da Marinha
SCADA	*Supervisory Control and Data Acquisition* (Sistema de Controle de Supervisão e Aquisição de Dados)
SDA	Sistemas Digitais Administrativos
SDO	Sistemas Digitais Operativos
SEI	*Software Engineering Institute*
SEN	Sistema de Ensino Naval
SIPAAerM	Serviço de Investigação e Prevenção de Acidentes Aeronáuticos da Marinha
SGM-107	Normas Gerais de Administração da Marinha
SN-BR	Submarino com Propulsão Nuclear Brasileiro
SNCA	Submarino Nuclear Convencionalmente Armado
TIC	Tecnologia da Informação e Comunicações
TO	Tecnologia Operacional
USA	*United States of America* (Estados Unidos da América)
USNAVY	*United States Navy* (Marinha dos Estados Unidos)

SUMÁRIO

1 INTRODUÇÃO

O ambiente operacional do século XXI apresenta desafios sem precedentes para as Forças Armadas, em especial para a Marinha do Brasil (MB), cuja crescente dependência tecnológica redefine os conceitos de prontidão, resiliência e segurança. As inovações tecnológicas que impulsionam a modernização dos meios navais, dos sistemas de comando e controle e das cadeias logísticas também ampliam, de forma proporcional, as vulnerabilidades e os vetores de ataque cibernético. Nesse contexto, o espaço cibernético consolida-se, definitivamente, como o quinto domínio da guerra, ao lado dos domínios terrestre, marítimo, aéreo e espacial, exigindo uma revisão urgente dos processos de gestão, operação, manutenção e proteção dos ativos da MB.

Projetos estratégicos da MB, como a construção das Fragatas Classe Tamandaré (FCT), o Submarino Nuclear Convencionalmente Armado (SNCA) e o Sistema de Gerenciamento da Amazônia Azul (SisGAAz), exemplificam a crescente complexidade e interdependência tecnológica dos meios navais modernos. Esses projetos incorporam uma quantidade inédita de sistemas integrados, sensores, redes embarcadas e tecnologias operacionais (TO), presente nos Sistemas Digitais Operativos (SDO), que, se por um lado proporcionam superioridade tecnológica e eficácia operacional, por outro lado expõem a MB a ameaças cibernéticas com potencial de comprometer missões críticas, operações navais e até a segurança nacional pela expansão da superfície de ataque cibernético[1].

Essa nova realidade acarreta a necessidade inadiável de que a MB adote uma postura proativa, estruturada e institucionalizada no tocante à gestão dos riscos operacionais, especialmente nos riscos cibernéticos operacionais, foco deste trabalho.

A proteção dos SDO apresenta desafios significativamente mais complexos do que os dos SDA. Isso ocorre devido à natureza sensível, sigilosa e muitas vezes proprietária dos sistemas operacionais embarcados, que integram sistemas de armas, sensores, redes de navegação, controle de propulsão, sistemas de comando e controle e tecnologias operacionais embarcadas. A multiplicidade de fornecedores, a

[1] Superfície de ataque cibernético - conjunto de todos os pontos de vulnerabilidade em um sistema ou rede computacional que podem ser explorados por um invasor para obter acesso não autorizado e potencialmente causar danos.

integração de sistemas de origem diversa e a complexidade da cadeia de suprimentos tecnológica ampliam consideravelmente a superfície de ataque, criando pontos de vulnerabilidade que podem ser explorados por agentes estatais ou não estatais, bem como por atores criminosos altamente especializados.

O aumento da superfície de ataque decorrente da modernização tecnológica impõe a necessidade de revisão dos processos de aquisição, homologação, manutenção, descarte e operação dos ativos de informação da MB. Atualmente, os processos existentes estão fortemente voltados para os aspectos administrativos, deixando brechas significativas na proteção dos SDO, o que pode ser explorado por agentes hostis, inclusive por meio da cadeia de suprimentos — um vetor de ataque já reconhecido internacionalmente como crítico no ambiente cibernético militar.

O avanço tecnológico, embora essencial para a modernização da frota e para a eficácia do Poder Naval, torna cada vez mais sensível a dependência das infraestruturas críticas. Os sistemas modernos, pela própria natureza, são sistemas ciberfísicos, ou seja, sistemas que integram elementos físicos, digitais e informacionais em uma única arquitetura operacional. A degradação de qualquer um desses elementos, particularmente pela exploração de vulnerabilidades cibernéticas, pode inviabilizar uma missão, paralisar uma plataforma ou gerar impactos estratégicos com repercussões nacionais.

O reconhecimento dessa realidade está refletido nos documentos estratégicos da própria MB. O Plano Estratégico da Marinha (PEM 2040), por meio do Objetivo Estratégico Naval (OBNAV 8 – Desenvolver a Capacidade Cibernética na MB), estabelece explicitamente a necessidade de incrementar a capacidade cibernética da MB, com ênfase na proteção dos ativos críticos, na defesa dos meios operacionais e na resiliência das infraestruturas críticas de interesse da MB (Brasil, 2020a). Esse objetivo não é apenas uma diretriz, mas uma condição essencial para assegurar a continuidade operacional dos projetos estratégicos em desenvolvimento.

A Política Naval (2019d) também destaca que o desenvolvimento da capacidade cibernética é imperativo para que o Poder Naval se mantenha apto a enfrentar os desafios dos conflitos modernos, nos quais o espaço cibernético se consolidou como um campo de batalha ativo. Esse documento reforça que a proteção deve ser integral, abrangendo tanto as infraestruturas de Tecnologia da Informação e Comunicações (TIC) quanto os meios navais em operação, com ações que envolvem

a proteção dos ativos, a exploração do ambiente cibernético e a condução de operações ofensivas e defensivas no domínio digital.

De acordo com a Estratégia de Defesa Marítima (EMA-310), publicada em 2023, os riscos associados a ataques cibernéticos foram classificados como “críticos”, representando o maior grau na escala de risco da MB (Brasil, 2023d). Essa classificação reflete o reconhecimento institucional de que a degradação de sistemas de comando, controle, comunicações, computação, cibernético, inteligência, vigilância e reconhecimento (C5IVR) pode comprometer a eficácia das operações navais e afetar diretamente a segurança dos meios navais e dos sistemas de armas.

Essa avaliação crítica tem implicações diretas na necessidade de revisar as doutrinas existentes, os processos operacionais e as políticas de segurança. De acordo com a própria EMA-310, as ameaças cibernéticas são capazes de afetar tanto os Sistemas Digitais Administrativos (SDA), historicamente mais protegidos e regulados, quanto os SDO, cuja proteção normativa e procedimental ainda é incipiente ou mesmo inexistente.

De fato, ataques cibernéticos têm sido, nos últimos anos, os vetores iniciais em uma ampla gama de conflitos híbridos[2] e interestatais. A sofisticação desses ataques, muitas vezes perpetrados por grupos patrocinados por Estados ou organizações com elevado nível de capacitação técnica, demonstra que as vulnerabilidades cibernéticas devem ser tratadas como ameaças de primeira ordem à segurança nacional. A não proteção adequada dos sistemas embarcados coloca em risco não apenas a missão, mas a integridade da própria Força.

A relevância deste trabalho se dá, pois, pela busca em preencher essa lacuna crítica ao propor a adoção, pela MB, de um modelo de Gestão do Risco Operacional (GRO) com foco no risco cibernético operacional. A proposta aqui apresentada está alinhada às melhores práticas internacionais, notadamente ao modelo adotado pela Marinha dos Estados Unidos da América (USNAVY), cuja doutrina, consolidada na norma OPNAVINST 3500.39D, oferece um exemplo robusto de como a gestão de riscos operacionais pode ser institucionalizada, sistematizada e aplicada tanto nos níveis administrativos quanto operacionais, incluindo o domínio cibernético.

---

[2] Conflitos híbridos – estratégias de guerra que combinam táticas militares convencionais com ações não convencionais, como desinformação, ciberataques, e interferência em processos políticos.

Além disso, a adoção da GRO com foco no risco cibernético é um vetor essencial para elevar a capacidade cibernética da MB, um dos pilares estruturantes do próprio PEM 2040 e das diretrizes do Estado-Maior da Armada (EMA). Implementar a gestão de riscos como ferramenta de apoio à decisão estratégica, tática e operacional é condição indispensável para assegurar a resiliência da Força, sua capacidade de adaptação frente a ameaças emergentes e sua prontidão para enfrentar desafios em cenários multidomínio, cada vez mais voláteis e contestados.

Ademais, a construção de uma doutrina de GRO com ênfase no risco cibernético operacional permitirá à MB integrar, de forma mais eficaz, suas ações no domínio cibernético às operações conjuntas e combinadas, aumentando sua interoperabilidade com outras Forças Armadas e com parceiros internacionais. A proteção das infraestruturas críticas, o fortalecimento da consciência situacional cibernética e a adoção de práticas de resiliência digital tornam-se, assim, pilares fundamentais para a eficácia do Poder Naval no século XXI.

Diante desse cenário, o objetivo principal desta pesquisa é propor a implementação da Gestão do Risco Operacional na Marinha do Brasil, com foco no risco cibernético operacional, como instrumento estratégico para aumentar a capacidade cibernética da MB, proteger seus ativos críticos e garantir a continuidade e a eficácia de suas operações, respondendo às questões: “quais as similaridades e singularidades entre a USNAVY e a MB no que diz respeito aos princípios de GRO?”, quanto à fase investigativa; “como a MB gerencia o risco cibernético para seus sistemas, tecnologias operacionais e infraestruturas críticas?”, referente à fase diagnóstica; e, “que medidas de espectro mais amplo e derivadas do apurado nas fases investigativa e diagnóstica seriam do interesse da MB?”, na fase propositiva.

Para além da formulação conceitual e doutrinária, neste trabalho também se propõe a apresentar propostas voltadas à construção de uma estrutura organizacional dedicada à GRO, à definição de processos normativos robustos e à incorporação de ferramentas tecnológicas de suporte à decisão, tais como sistemas informatizados de gestão de riscos operacionais, capazes de apoiar o ciclo decisório em tempo real. Adicionalmente, serão discutidas as possibilidades de integração dos *frameworks*[3] internacionais de gestão de risco, notadamente os preconizados pelo NIST, em

[3] *Framework* – é uma estrutura abstrata que fornece um conjunto de ferramentas, componentes e diretrizes para o desenvolvimento de software, aplicações ou projetos de forma mais rápida e eficiente.

sinergia com os padrões adotados pela MB, de modo a fortalecer a interoperabilidade da Força no contexto de operações conjuntas e combinadas. Reconhecendo também a lacuna conceitual atualmente existente no âmbito da Defesa Nacional, nesta pesquisa também sugere-se, como desenvolvimento futuro, a formalização do conceito de risco operacional no Glossário das Forças Armadas, contribuindo assim para a padronização terminológica e doutrinária no Ministério da Defesa e nas Forças Singulares.

A metodologia empregada neste estudo é uma abordagem baseada na pesquisa bibliográfica e documental, concentrando-se na investigação da literatura e bibliografia pertinentes aos contextos de gestão de riscos, gestão de riscos operacionais, risco cibernético e guerra cibernética. Priorizou-se a utilização de fontes primárias e a análise de trabalhos de autores tanto nacionais quanto internacionais, visando à construção de um sólido embasamento de dados e informações para sustentar a pesquisa. A partir dessas informações selecionadas, realizou-se uma análise por meio de método dedutivo e estudo comparativo, culminando na elaboração das conclusões e na formulação de proposições direcionadas à Marinha do Brasil.

Esse enfoque permitiu considerar as similaridades e as singularidades entre as Forças Navais estudadas, estruturando-se em seis capítulos, incluindo a presente introdução, como o Capítulo 1. Segue-se o Capítulo 2, no qual se apresenta os fundamentos teóricos da Gestão do Risco Operacional, com destaque para o conceito de risco, suas origens, evolução e aplicação no contexto militar e cibernético. No Capítulo 3, são analisados os aspectos da GRO na Marinha dos Estados Unidos (USNAVY), com ênfase na doutrina OPNAVINST 3500.39D e na sua aplicação ao risco cibernético. No Capítulo 4, realiza-se o diagnóstico da situação da GRO na Marinha do Brasil (MB), considerando os mesmos eixos analíticos aplicados à USNAVY. No Capítulo 5, são apresentados os resultados da análise comparativa entre as duas Marinhas, suas similaridades e singularidades, culminando na formulação de propostas objetivas para a implementação e fortalecimento da GRO na MB, com foco no risco cibernético operacional, visando assegurar a proteção, a resiliência e a eficácia do Poder Naval brasileiro. Por fim, no Capítulo 6, são traçadas considerações finais e resumidas as contribuições desta pesquisa.

2 VISÃO GERAL SOBRE RISCO E GESTÃO DO RISCO OPERACIONAL

O conceito de risco evoluiu ao longo da história e, atualmente, é compreendido como a combinação entre a probabilidade e o impacto de eventos futuros incertos, aplicando-se a qualquer área do conhecimento e tipo de organização, civil ou militar. Com o amadurecimento dos estudos sobre o tema, diversos riscos passaram a ser identificados nas atividades institucionais, evidenciando a necessidade de gerenciamento. Nesse contexto, a gestão de riscos passou a ser formalizada como um processo contínuo, que envolve as etapas de identificação, análise, tratamento e monitoramento, sendo fundamental para o sucesso organizacional. Dentre os diferentes tipos de risco, destaca-se o risco operacional, presente em todas as atividades e caracterizado por falhas em pessoas, processos, sistemas e fatores externos, especialmente relevantes em contextos complexos, como o militar. Também são introduzidos conceitos relacionados ao espaço cibernético, operações cibernéticas e risco cibernético operacional, uma vertente específica do risco operacional.

2.1 RISCO

Risco é um termo compreendido e aplicado de diferentes maneiras em todos os campos disciplinares do conhecimento (Lupton, 2013). O que se entende por risco abrange os mais profundos aspectos de áreas como psicologia, matemática, estatística e história. Sua literatura é monumental e constantemente ampliada, mostrando-se um tema estudado desde a antiguidade e, ainda assim, atual (Bernstein, 1996).

A noção de que o ser humano pode compreender e influenciar o futuro, deixando de vê-lo como mero resultado do acaso ou da vontade divina, representa uma mudança revolucionária que marcou a transição do pensamento antigo para o moderno. Antes dessa transformação, o futuro era percebido como uma repetição do passado ou como um território desconhecido, acessível apenas a oráculos e adivinhos que detinham o monopólio da previsão dos acontecimentos (Bernstein, 1996). Quando diversos pensadores colocaram o futuro ao serviço do presente, mostrando ao mundo como entender, medir e pesar as consequências do risco, eles converteram a tomada de riscos em um dos principais catalisadores que impulsionam a sociedade ocidental moderna, convertendo as incertezas do futuro em oportunidades (Bernstein, 1996).

Segundo Bernstein (1996), as descobertas sobre a natureza do risco e a ciência e a arte de se fazer escolhas estão no cerne da economia moderna. Optar ou não por assumir riscos rege as nações ao redor do mundo, baseando-se no que pode acontecer no futuro e impulsionando a ciência e os empreendimentos nas áreas de energia, negócios e comunicações, por exemplo.

O conceito moderno de risco surgiu há cerca de setecentos ou oitocentos anos, mas seu estudo, como uma área de conhecimento, se deu na Renascença, período aproximado entre meados do século XIV e o fim do século XVI, representando a passagem da concepção medieval do mundo, cheia de viés religioso e supersticioso, para uma visão racional e científica. Neste mesmo período surgiu a teoria da probabilidade, considerada o "coração matemático" para o conceito do risco, fazendo com que as pessoas pudessem pela primeira vez tomar decisões e prever o futuro com a ajuda de números (Bernstein, 1996; Lupton, 2013).

A palavra risco deriva do italiano *risicare*, que significa ousar. Nesse sentido, o risco é fruto de uma escolha, ousada ou não, e não um destino. As ações que ousamos tomar, as quais dependem de quão livres somos para fazer escolhas, é do que se trata o risco (Bernstein, 1996).

Para esta pesquisa, é preciso considerar, além do conceito teórico e histórico apresentado para o risco, as definições estabelecidas pelas normas que fundamentam as Forças Armadas e, em especial as normas da MB.

Dessa forma, o conceito de risco adotado no Glossário das Forças Armadas, publicação que "contém, basicamente, termos, palavras, vocábulos e expressões de uso em operações nas Forças Armadas, com ênfase no emprego conjunto, a fim de contribuir para a integração entre as Forças e incrementar a interoperabilidade nas atividades de planejamento e emprego" (Brasil, 2015, p. 12), é considerado como a "quantificação da insegurança, por meio da combinação da probabilidade, com a gravidade de ocorrência de um evento" (Brasil, 2015, p. 243).

Do Glossário da Segurança da Informação do GSI (Brasil, 2019a), publicação válida para todos os órgãos da Administração Pública Federal (APF), tem-se o conceito geral de risco como a "possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade".

Na Marinha, o Estado-Maior da Armada (EMA) adota um conceito mais sucinto: "Efeito da incerteza nos objetivos da organização" na publicação Instruções para

Implementação da Política de Gestão de Riscos da Marinha do Brasil (MB) (Brasil, 2017b, p. C-3).

Já o Manual de Segurança de Aviação, publicação com o propósito de "regulamentar o Serviço de Investigação e Prevenção de Acidentes Aeronáuticos da Marinha (SIPAAerM) e de estabelecer normas e procedimentos abrangentes para o gerenciamento da segurança de aviação no âmbito da Marinha" (Brasil, 2023a, p. XIV), considera risco como a "quantificação da insegurança, ou seja, da ameaça decorrente da exposição a um perigo, expresso pela gravidade das possíveis consequências e respectiva probabilidade" (Brasil, 2023a, p. 1-26).

A Política de Gestão de Riscos do Ministério da Defesa (PGR-MD), publicação que "tem por finalidade estabelecer princípios, objetivos, diretrizes e instituir o sistema de gestão de riscos relacionados aos objetivos estratégicos organizacionais, projetos, processos e recursos no âmbito do Ministério da Defesa" (Brasil, 2024b), define o risco como "possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização, sendo medido em termos de impacto e de probabilidade" (Brasil, 2024b).

A publicação Normas Gerais de Administração da MB (SGM-107), tem o propósito de "orientar a implantação da Excelência em Gestão nas Organizações Militares(OM), fornecendo subsídios, princípios técnicos e sistemas de administração imprescindíveis para a correta condução de uma OM" (BRASIL,2024a, p. VI), segue a definição da ISO 31000, que considera risco sendo "o efeito da incerteza nos objetivos", podendo "ser expresso pela combinação percebida da sua probabilidade de ocorrência e do impacto resultante da ameaça ou oportunidade" (BRASIL,2024a, p. 5-1).

Das várias definições de risco pesquisadas, observa-se que, mesmo dentro da MB, são encontradas diversas interpretações do que seria o risco, prejudicando seu entendimento e confirmando as evoluções e interpretações do seu significado.

No Apêndice A, encontra-se o quadro 1, que relaciona as palavras-chave dos conceitos analisados. Deste quadro se depreende que a palavra "probabilidade" aparece mais vezes, seguida por "objetivo". Neste trabalho, será considerada a definição da SGM-107 quando for necessária a alusão ao significado de risco pois ela é a mais abrangente e mais recente.

Dessa forma, à medida que são analisadas as situações, independente dos cenários considerados, surgem diversos riscos, ou, como considerado por Bernstein

(1996), eles sempre existiram, mas ainda não haviam sido identificados. Manifesta-se, assim, a necessidade de gerenciá-los para seguir em frente com qualquer que seja a missão de uma organização militar.

2.2 GESTÃO DE RISCOS

A capacidade de identificar riscos é subjetiva, sendo realizada “com base no conhecimento e nos pontos de vista das partes interessadas”, considerando ainda “vieses, hipóteses e crenças dos envolvidos” (ABNT, 2018, p. 12). Ainda hoje, há ampla especulação em torno da gestão de riscos, levando alguns autores a questionarem se a identificação de riscos se configura como uma ciência ou uma arte (Bernstein, 1996; Brasil, 2020b).

A gestão de riscos abrange todos os processos, atividades e setores de uma organização, sendo fundamental que todas as suas áreas constituintes contribuam ativamente para a identificação e o tratamento dos riscos. O envolvimento coletivo é essencial para a construção de uma visão abrangente da organização, além de facilitar a implementação eficaz da gestão de riscos. Conforme as Diretrizes de gestão de riscos da ABNT, “o risco é gerenciado em todas as partes da estrutura da organização” e “todos na organização têm responsabilidade por gerenciar riscos” (ABNT, 2018, p. 6), sendo sua aplicação possível nos níveis estratégico, operacional, de programas, de projetos e, no caso das Forças Armadas, também no nível tático. A gestão de riscos deve ocorrer de maneira formal, dinâmica e iterativa, necessitando ser adaptada e personalizada para atender às necessidades, características e cultura da organização. No contexto das Organizações Militares (OM) da MB, espera-se que toda a tripulação, dentro de sua experiência e função, contribua ativamente na identificação e mitigação dos fatores que possam representar risco à missão.

De acordo com as Diretrizes de Gestão de Riscos da ABNT (ABNT, 2018), a gestão de riscos é um processo sistemático que envolve comunicação, estabelecimento de contexto, avaliação, tratamento, monitoramento e registro dos riscos. A comunicação busca conscientizar e integrar diferentes perspectivas de pessoas envolvidas com determinado tipo de risco, enquanto o estabelecimento do contexto personaliza o processo conforme as especificidades da organização. A avaliação dos riscos, que representa o cerne do processo, inclui identificação, análise e comparação, com base em dados e critérios específicos, levantados e estabelecidos por, preferencialmente, especialistas. O tratamento dos riscos envolve opções como

evitar, mitigar, compartilhar ou aceitar, sempre com monitoramento contínuo. Todo o processo deve ser documentado ao longo de sua execução, garantindo aprendizado, melhoria contínua e apoio à tomada de decisões estratégicas. No Anexo A, a figura 1 contém a ilustração do processo de gestão de riscos segundo as Diretrizes da ABNT.

Para este trabalho, foram pesquisadas e identificadas várias definições para a gestão de riscos nas normas e publicações seguidas ou produzidas pela MB, dentre elas: a definida no Glossário de Segurança da Informação (Brasil, 2019a), produzido pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), seguido *ipsis litteris* pela Política de Gestão de Riscos do MD (Brasil, 2024b); e pelas Instruções para Implementação da Política de Gestão de Riscos da Marinha do Brasil, definida sucintamente como "atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco" (Brasil, 2017b, p. C-2).

Na MB, as Normas Gerais de Administração (SGM-107) (Brasil, 2024a) estabelecem que gerenciamento ou gestão de riscos,

> "consiste na aplicação de princípios e processos para identificação e avaliação de riscos das organizações. Esse gerenciamento aborda os processos de planejamento, identificação, análise, planejamento de respostas e controle de riscos. Seus objetivos são aumentar a probabilidade e o impacto dos eventos positivos e reduzir ou minimizar os dos negativos" (Brasil, 2024a, p.1-3).

De acordo com a SGM-107, os riscos podem ser classificados como eventos negativos ou positivos, seguindo a mesma abordagem da Associação Brasileira de Normas Técnicas (ABNT, 2018), assim como de alguns autores modernos (Lupton, 2013). Ainda que esta abordagem não seja uma unanimidade dentre diversos autores, ela será a definição adotada nesta pesquisa.

Mediante os argumentos apresentados, a capacidade de gerenciar riscos e, com ela, o apetite[4] para assumir riscos e fazer escolhas com visão de futuro são elementos-chave da energia que impulsiona várias organizações e sistemas nacionais e internacionais como, por exemplo, o sistema econômico (Bernstein, 1996). Foi exatamente no sistema econômico que surgiu, pela primeira vez, a menção ao risco operacional, que representa um dos tipos de risco possíveis e observáveis nas organizações.

---

[4] Apetite a risco - nível de risco que uma organização está disposta a aceitar para atingir seus objetivos organizacionais (Brasil, 2024b).

2.3 RISCO OPERACIONAL

O conceito de risco operacional tem suas origens em estudos sobre falhas organizacionais e fraudes financeiras ocorridas desde a década de 1980. Ainda que o termo não fosse amplamente utilizado à época, sua essência já se manifestava em pesquisas como as de Perrow (1984), que analisavam acidentes organizacionais sob a perspectiva de falhas sistêmicas e da crescente complexidade operacional. Com o tempo, especialmente em setores como manufatura, tecnologia e telecomunicações, percebeu-se a necessidade de um planejamento rigoroso não apenas para garantir a eficiência de suas operações, mas também para evitar atrasos e interrupções, exigindo, segundo Coleman (2011), a necessidade de planejamento especializado e da existência de unidades dedicadas à gestão do risco operacional, capazes de apoiar decisões críticas. A partir disso, a medição e a modelagem desses riscos passaram a ser fundamentais para decisões estratégicas, tais como determinar investimentos em infraestrutura de segurança, definir reservas financeiras contra perdas inesperadas ou avaliar medidas de proteção contra desastres.

A percepção de que o risco operacional seria imensurável prevaleceu até o final do século XX, quando, em 2001, o setor financeiro, altamente regulado e suscetível a perdas expressas em termos monetários, passou a liderar os estudos sobre o tema. Foi nesse contexto que o Comitê de Basileia para Supervisão Bancária[5] formalizou, pela primeira vez, uma definição padronizada, estabelecendo que risco operacional era o risco de perdas resultantes de falhas ou inadequações de processos internos, pessoas, sistemas ou de eventos externos. A definição inclui riscos legais, mas exclui risco estratégico e reputacional (BIS, 2006).

Essa definição foi adotada por razões estratégicas, regulatórias e históricas, visando abranger todas as fontes principais de falha não-financeira que poderiam afetar uma instituição, especialmente no setor bancário. A ideia era consolidar em uma única categoria os riscos que não eram provenientes de operações de crédito nem de mercado, mas que afetavam diretamente a continuidade e a segurança das operações. Dessa forma, as pessoas, responsáveis por erros humanos, fraudes ou negligências; os processos, representando fluxos operacionais mal definidos ou mal executados; os sistemas, representando falhas tecnológicas, tecnologias obsoletas,

[5] O Comitê de Basileia para Supervisão Bancária (BCBS) é um órgão internacional que define padrões para a regulação bancária.

inseguras ou inapropriadas; e os eventos externos, representados por todas as fontes externas às instituições tais como desastres naturais, ataques cibernéticos ou pandemias, poderiam ser identificados e tratados (BIS, 2006).

Diversos colapsos financeiros marcantes nas últimas décadas tiveram as falhas operacionais como causa principal e não a inadimplência de crédito ou oscilações de mercado. Entre os exemplos mais notórios estão o colapso do Barings Bank, em 1995, resultado de fraudes cometidas por um único operador sem supervisão eficaz; o caso do Allied Irish Bank, em 2002, que acumulou perdas expressivas devido a fraudes internas não identificadas a tempo; e, mais recentemente, diversos incidentes críticos envolvendo falhas sistêmicas e ataques cibernéticos, causando prejuízos financeiros milionários. Esses episódios demonstram que os riscos operacionais possuem potencial destrutivo comparável ou até superior ao dos riscos financeiros tradicionais, comprovando a importância de conceituação precisa e de implementação de mecanismos de controle (BIS, 2006).

Desde então, a definição de risco operacional de Basileia foi consolidada e assumida por diversos autores e instituições, financeiras e não financeiras (Coleman, 2011; SEI, 2014; Stryker, 2024), transformando o risco operacional em um assunto de grande importância, passando a ser amplamente discutido e classificado como um dos principais tipos de risco enfrentados por organizações, ao lado dos riscos estratégico, de crédito e de mercado, acontecendo em todos os lugares e não apenas em um ambiente de negócios (Stryker, 2024).

Stryker (2024) classifica o risco operacional em seis categorias: riscos de processo, relacionados à eficiência dos processos internos; riscos de pessoas, ligados a falhas humanas, fraudes ou condutas inadequadas; riscos de sistemas, também chamado de risco tecnológico, associados a falhas tecnológicas e ciberataques; riscos financeiros, decorrentes de decisões econômicas inadequadas; riscos estratégicos, originados de escolhas organizacionais inadequadas; e eventos externos, provocados por fatores fora do controle da organização, como desastres naturais ou instabilidades políticas e econômicas.

Todos estes tipos de riscos estão presentes e, dependendo do grau e objetivo da missão, necessitam ser analisados e avaliados para o seu cumprimento.

Em um mundo cada vez mais dependente da tecnologia, onde o espaço cibernético se faz presente, surge um novo risco: o risco cibernético operacional.

Para o entendimento desse tipo específico de risco, são necessários alguns conceitos fundamentais sobre cibernética, a serem explicados nas seções seguintes.

2.3.1 Espaço Cibernético e Outros Conceitos Fundamentais

Anteriormente às explanações sobre o risco cibernético operacional, faz-se necessário fornecer uma visão geral sobre os seguintes conceitos fundamentais para este trabalho: espaço cibernético, segurança cibernética, defesa cibernética, guerra cibernética, capacidade cibernética, operações cibernéticas, infraestruturas críticas, tecnologia operacional, cadeia de suprimentos cibernética, vulnerabilidades e ameaças cibernéticas.

Espaço Cibernético

Em 2016, a Organização do Tratado do Atlântico Norte (OTAN) reconheceu formalmente o espaço cibernético como um novo domínio operacional, ampliando significativamente seu papel no planejamento de operações militares (Brasil, 2023c). Esse reconhecimento impulsionou a inclusão do conceito no Glossário de Segurança da Informação (Brasil, 2019a), onde o espaço cibernético é caracterizado como o ambiente virtual resultante da interconexão de dispositivos e redes de comunicação, no qual ocorrem atividades digitais em rede, abrangendo o armazenamento, processamento e compartilhamento de informações, bem como a condução de ações automatizadas ou humanas nesse meio.

Seguindo essa tendência internacional e atento aos eventos relevantes envolvendo este novo ambiente, o Brasil também passou a considerar o espaço cibernético como um domínio operacional. Nesse contexto, são desenvolvidas operações cibernéticas ofensivas e defensivas, atuando de forma integrada e complementar aos domínios tradicionais — terrestre, marítimo, aéreo e espacial —, atravessando-os e potencializando sua eficácia (Brasil, 2023c; Brasil, 2015).

Segurança Cibernética, Defesa Cibernética e Guerra Cibernética

De acordo com a Doutrina Militar de Defesa Cibernética (Brasil, 2023c), no Brasil, o espaço cibernético está estruturado em três níveis de decisão:

a) Nível Político: a Segurança Cibernética é coordenada pelo GSI/PR, abrangendo a Administração Pública Federal (APF), incluídas as Forças Armadas (FA) e as infraestruturas críticas (IC) nacionais. Neste nível, a Segurança Cibernética

refere-se a processos que buscam assegurar a existência e a continuidade do espaço cibernético de uma nação;

b) Nível Estratégico: a Defesa Cibernética é conduzida pelo Ministério da Defesa (MD), do Estado-Maior Conjunto das Forças Armadas (EMCFA) e dos Comandos das Forças Armadas, interagindo com o GSI/PR, APF, agências e IC de interesse para a Defesa Nacional. Neste nível, a Defesa Cibernética abrange ações realizadas no espaço cibernético, dentro de um planejamento nacional, com o objetivo de proteger sistemas de informação de interesse da Defesa Nacional;

c) Nível Operacional: a Guerra Cibernética fica a cargo de Comandos Operacionais ativados, os quais realizam o planejamento das ações cibernéticas de proteção, exploração e ataque. Nesse nível e no próximo, a Guerra Cibernética abrange as ações cibernéticas de proteção, exploração ou ataque no contexto de um planejamento militar; e

d) Nível Tático: a Guerra Cibernética fica a cargo das Forças Componentes, singulares ou conjunta, as quais executam o planejamento elaborado no nível operacional, executando as ações cibernéticas.

Capacidade Cibernética

Segundo a Doutrina Militar de Defesa Cibernética (Brasil, 2023c), a capacidade cibernética representa um recurso não cinético, uma vez que suas ações são conduzidas em um ambiente virtual, com elevado potencial de ampliar o poder de combate, que por sua vez permite a geração de efeitos tanto não cinéticos, no mesmo espaço cibernético, quanto cinéticos, nos outros domínios operacionais. Essa atuação pode, inclusive, provocar a paralisação das capacidades do oponente em níveis estratégicos, operacionais ou táticos.

Na MB, é compreendida como um recurso estratégico essencial, destinado a ampliar o poder de combate e a assegurar a superioridade operacional no ambiente virtual (Brasil, 2021).

Operações Cibernéticas

Segundo a Doutrina Cibernética da Marinha (EMA-419) (Brasil, 2021), no espaço cibernético são conduzidas operações cibernéticas ofensivas ou defensivas, as quais envolvem ações cibernéticas de proteção, exploração ou ataque com o objetivo de garantir a segurança e a superioridade nesse novo domínio. Essas

operações são planejadas, coordenadas e executadas com foco na defesa de redes operacionais específicas e no apoio direto a campanhas ou operações militares nos demais domínios operacionais.

As operações cibernéticas englobam a produção de inteligência, obtida por meio de sensores, da identificação de ameaças e da análise de vulnerabilidades, inerentes aos sistemas, tanto do setor de Defesa quanto de outras fontes de interesse da Defesa Nacional.

Tais operações dependem de infraestruturas de tecnologia da informação — em rede, autônomas, em nuvem ou embarcadas em plataformas aéreas, terrestres e marítimas —, executando ações destinadas a gerar efeitos no ambiente cibernético e, quando necessário, refletidos nos demais domínios operacionais.

Infraestruturas Críticas

As infraestruturas críticas são definidas, de acordo com a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), como “instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade” (Brasil, 2018b). Essas infraestruturas estão presentes em setores essenciais, como energia, transportes, comunicações, água e saneamento, saúde, segurança e serviços financeiros, desempenhando papel vital para a estabilidade e funcionamento da sociedade.

No âmbito das Forças Armadas, são consideradas infraestruturas críticas os sistemas e instalações essenciais para a defesa e a segurança nacional, incluindo bases militares, portos estratégicos, bases aéreas, sistemas de comunicação e comando, redes de energia e sistemas de informação. A sua proteção é considerada estratégica sendo definida como o “conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas” (Brasil, 2018b).

Dada a crescente dependência tecnológica, as infraestruturas críticas modernas dependem intensamente de Tecnologias Operacionais (TO) para seu funcionamento seguro e eficiente.

Tecnologia Operacional

Tecnologia Operacional (TO) refere-se aos sistemas de hardware e software utilizados para monitorar, controlar e automatizar dispositivos e processos físicos, como máquinas industriais, sensores, sistemas de controle de infraestrutura crítica e plataformas militares. Ao contrário da Tecnologia da Informação (TI), que trata prioritariamente do processamento e gestão de dados, a TO é orientada à operação segura e contínua de ativos físicos essenciais.

Conforme destacado na Doutrina Cibernética da Marinha (Brasil, 2021), a TO é fundamental para a condução de operações navais e de defesa, sendo diferente da TI justamente por seu foco em processos físicos e dispositivos operacionais, exigindo proteção específica no contexto do espaço cibernético.

Recentemente, a convergência entre TI e TO vem gerando novos e complexos desafios de segurança. A crescente interconexão de sistemas TO a redes de TI, impulsionada pela digitalização de infraestruturas militares e civis, ampliou significativamente a superfície de ataque cibernético[6]. Essa integração, como analisada por Kok et al. (2024), aumenta a vulnerabilidade de ativos físicos que eram tradicionalmente isolados e expõe sistemas críticos a ameaças cibernéticas antes inexistentes.

Atores maliciosos têm explorado essas novas fragilidades comprometendo e afetando a operação e, consequentemente, a segurança de sistemas de armas, redes de comando e controle, sensores navais e outros dispositivos embarcados, considerados infraestruturas críticas para as Forças Armadas. A proteção da TO, portanto, tornou-se estratégica no ambiente militar e de defesa cibernética, exigindo a adoção de medidas de segurança para ambientes híbridos TI/TO, conforme orientado tanto pela literatura especializada quanto pelas doutrinas da MB.

Cadeia de Suprimentos Cibernética

A cadeia de suprimentos cibernética compreende o conjunto de processos, organizações, tecnologias e componentes, incluindo equipamentos e programas que, de forma integrada, sustentam o desenvolvimento, a produção e a operação de sistemas tecnológicos. Em um mundo cada vez mais conectado, essa cadeia se tornou essencial para a inovação e o funcionamento de setores estratégicos como

---

[6] A superfície de ataque cibernético refere-se ao conjunto de ativos de informação de um espaço cibernético expostos publicamente na Internet às ações ofensivas cibernéticas ou dispostos em uma rede interna de conhecimento de uma ameaça cibernética (Brasil, 2023c).

defesa, saúde, finanças e infraestrutura crítica. Contudo, a sua complexidade amplia as vulnerabilidades a ameaças intencionais, como sabotagem, espionagem e inserção de componentes maliciosos. Nesse contexto, proteger a cadeia de suprimentos cibernética é indispensável para garantir a confiabilidade dos sistemas, preservar a continuidade operacional e assegurar a soberania tecnológica. A implementação do gerenciamento de riscos, em especial os cibernéticos, na cadeia de suprimentos é, portanto, uma prioridade estratégica para organizações que buscam resiliência e segurança em um ambiente de ameaças cada vez mais sofisticadas (Dunlap e Ortiz, 2022; Ghadge et al., 2019).

Considerando a ampla adoção de tecnologias digitais e a modernização as quais as Forças Armadas vêm se submetendo, eleva-se ainda mais a necessidade de sua proteção, uma vez que vulnerabilidades em qualquer um de seus componentes pode vir a ser explorada, comprometendo informações sensíveis e vindo a afetar a eficácia operacional ou mesmo a soberania nacional.

Vulnerabilidades e Ameaças Cibernéticas

Vulnerabilidade cibernética é definida como uma fraqueza inerente a sistemas, infraestruturas, instalações ou equipamentos que pode ser explorada por agentes adversários para obter vantagem ou causar dano. De acordo com o Glossário de Segurança da Informação (Brasil, 2019a) e com a Doutrina Militar de Defesa Cibernética (Brasil, 2023c), vulnerabilidade representa uma deficiência técnica, procedimental ou organizacional que expõe ativos críticos a riscos, afetando sua confidencialidade, integridade ou disponibilidade. Em termos práticos, vulnerabilidades podem incluir falhas de software, senhas fracas, configurações inadequadas de rede, ausência de atualizações de segurança ou ausência de segmentação adequada entre redes críticas e abertas.

Por outro lado, uma ameaça cibernética é caracterizada como qualquer conjunção de atores, entidades, forças ou fenômenos que possuem a intenção e a capacidade de explorar vulnerabilidades para realizar ações hostis, prejudicando sistemas de informação, operações militares, ou infraestruturas estratégicas. Conforme definido na Doutrina Militar de Defesa Cibernética (Brasil, 2023c), ameaças cibernéticas podem ser humanas (como agentes hostis, hackers, grupos patrocinados por Estados) ou naturais (como falhas imprevistas de sistemas críticos) e operam no espaço cibernético com o objetivo de comprometer as operações de defesa nacional.

A correlação entre vulnerabilidade e ameaça é central para a compreensão da gestão de risco cibernético. Uma vulnerabilidade, por si só, não resulta em dano se não houver uma ameaça capaz de explorá-la. Da mesma forma, uma ameaça isolada não gera impacto sem a existência de vulnerabilidades a serem exploradas. Assim, o risco cibernético é a combinação da probabilidade de uma ameaça explorar uma vulnerabilidade com a magnitude dos danos potenciais provocados por essa exploração (Brasil, 2015; Brasil, 2019a; Brasil, 2023c).

Com os conceitos apresentados, pode-se conceituar o risco cibernético operacional, foco desta pesquisa.

2.3.2 Risco Cibernético Operacional

Com base no arcabouço cibernético apresentado e segundo o Glossário das Forças Armadas (Brasil, 2015), o risco cibernético é representado pela "probabilidade de ocorrência de um incidente cibernético[7] associado à magnitude do dano por ele provocado".

A capacidade de um incidente cibernético afetar uma operação militar é significativa e, em certos casos, decisiva, dada a crescente digitalização dos meios e sistemas militares. Tais incidentes podem comprometer diretamente a eficácia, a segurança e a continuidade das operações em todos os níveis – estratégico, operacional e tático.

No nível operacional, podem ser mencionados os seguintes impactos de incidentes cibernéticos: comprometimento de sistemas de comando e controle, pela sua interrupção ou manipulação; perda da confidencialidade de informações sensíveis, pelo vazamento ou sequestro das mesmas; paralisação de infraestruturas críticas, pela corrupção ou desativação de sistemas que as controlem; manipulação ou sabotagem de plataformas operativas e armamentos, todas com amplo emprego de tecnologia moderna e de última geração, com alta complexidade de manutenção e grande dependência de programas e redes computacionais, tais como navios, aeronaves e sistemas embarcados diversos que controlam armas, propulsão,

---

[7] Incidente cibernético – ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso. Conforme o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos.

sensores e navegação; e efeitos psicológicos e estratégicos, pois também podem ser utilizados para desestabilizar o processo decisório, gerar incerteza no comando e minar a confiança da tropa e da população, impactando diretamente o moral e a legitimidade da operação (EMGEPRON, 2023; Greenberg, 2021).

A relação entre os impactos que incidentes cibernéticos podem causar em decorrência de vulnerabilidades de sistemas ou equipamentos e de ameaças externas aos mesmos é central para a compreensão da gestão do risco cibernético no contexto militar. Incidentes cibernéticos ocorrem quando ameaças externas exploram vulnerabilidades existentes em sistemas e equipamentos, resultando em diversos impactos operacionais, os quais afetarão as missões atribuídas à Força.

No Apêndice A, encontra-se o quadro 2 contendo uma relação entre ameaças, vulnerabilidades e impactos de variados tipos de incidentes cibernéticos relacionados às operações militares.

2.3.3 Taxonomia dos Riscos Cibernéticos Operacionais

Em 2014, o Instituto de Engenharia de Software (Software Engineering Institute – SEI), lançou um relatório apresentando uma taxonomia para os riscos cibernéticos operacionais. A taxonomia identificou, organizou e expandiu as quatro fontes deste tipo de risco (pessoas, processos, tecnologia e eventos externos), nomeando e detalhando-as em classes e subclasses (SEI, 2014).

De acordo com a taxonomia, as quatro classes são as seguintes (SEI, 2014):

a) Ações de pessoas: ações, ou omissões, tomadas por pessoas, deliberada ou acidentalmente que impactam a segurança cibernética;

b) Falhas de sistemas e tecnologia: falhas de hardware, software e sistemas de informação;

c) Falhas em processos internos: problemas nos processos internos de negócios que impactam a capacidade de implementar, gerenciar e sustentar a segurança cibernética, como design, execução e controle de processos; e

d) Eventos externos: problemas frequentemente fora do controle da organização, como desastres, questões legais, problemas comerciais e dependências de provedores de serviços.

A taxonomia, contendo as classes, as subclasses e seus elementos constituintes, pode ser visualizada na figura 2 do Anexo A.

Como elemento fundamental ao levantamento dos riscos cibernéticos operacionais, a taxonomia pesquisada fornece diversos elementos das classes de risco (pessoas, processos, tecnologia e eventos externos) que servem como orientação para mapeá-los nas missões que empregam tecnologias ou delas são dependentes, podendo ser usada como uma ferramenta para auxiliar na identificação de todos os riscos cibernéticos operacionais aplicáveis em uma organização.

Dessa forma, o crescente uso de tecnologias nos meios navais e de fuzileiros navais, bem como nos diversos sistemas administrativos e operativos empregados pela MB, tem ampliado a exposição a riscos operacionais associados ao domínio cibernético. Essa realidade torna imprescindível a identificação e o gerenciamento desses riscos, a fim de assegurar a continuidade, a resiliência, a segurança e a eficácia das operações navais.

2.4 GESTÃO DE RISCOS OPERACIONAIS

Com a diversidade de riscos operacionais presentes nas operações das instituições, torna-se imprescindível gerenciá-los de forma que não interfiram ou impeçam o atingimento dos objetivos das missões.

Nesta pesquisa, destaca-se a relevância da gestão do risco cibernético, considerado um tipo de risco operacional, uma vez que as empresas passaram a usar tecnologia para tudo, desde operações cotidianas até processos essenciais para os negócios e em seus sistemas de TI, que se tornaram maiores e mais complexos (Stryker, 2024).

Atualmente, essa realidade se aplica à MB, na qual o uso intensivo de tecnologia vem se expandindo continuamente. Meios navais e de fuzileiros navais, infraestruturas críticas, atividades administrativas e operativas, além de projetos de alta complexidade, como as Fragatas Classe Tamandaré (FCT) e o Submarino Nuclear Convencionalmente Armado (SNCA), têm incorporado soluções tecnológicas cada vez mais sofisticadas, incluídas suas cadeias de suprimentos.

2.5 CONSIDERAÇÕES PARCIAIS

Neste capítulo, constatou-se que o conceito de risco ainda é um tema controverso, o que leva as instituições a adotarem definições distintas, ajustadas às suas necessidades específicas. A única certeza é que há uma variedade de riscos

que devem ser identificados e tratados, a fim de minimizar sua influência sobre os resultados esperados.

Para que uma organização, independentemente de sua área de atuação, alcance seus objetivos e esteja preparada para enfrentar eventuais imprevistos, é essencial implementar uma gestão de riscos eficaz, considerando a possibilidade de surgimento de diferentes tipos de risco.

Entre os riscos identificáveis, destacam-se os riscos operacionais, em especial o risco cibernético operacional, em razão da ampla adoção de tecnologias avançadas, presentes em praticamente todas as áreas das organizações.

Esse tipo de risco já foi mapeado em taxonomia própria, indicando aspectos de pessoas, processos, tecnologias e eventos externos que podem ser identificados como causadores de eventos que ameaçam a operação das instituições, incluídas as militares.

O gerenciamento desse tipo de risco torna-se, portanto, fundamental para garantir a continuidade e a eficácia das atividades organizacionais, incluídas as operações e missões da Marinha do Brasil.

Este capítulo encerra-se corroborando o impacto e o crescente aumento desse tipo de risco nas operações militares modernas diante da crescente dependência tecnológica à qual as Forças Armadas vêm se submetendo.

No próximo capítulo será abordada a Gestão do Risco Operacional (GRO) na Marinha dos Estados Unidos, objetivando sua futura comparação com as práticas adotadas pela Marinha do Brasil.

3 GRO NA MARINHA DOS ESTADOS UNIDOS DA AMÉRICA

A Gestão do Risco Operacional (GRO) na Marinha dos Estados Unidos (USNAVY) é regida pela norma *Operational Risk Management* (OPNAVINST 3500.39D), que a define como uma política essencial de apoio à decisão, aplicável em todos os níveis hierárquicos e atividades da instituição. Seu objetivo principal é aumentar a eficácia das missões, proteger recursos e preservar vidas. Tal abordagem consolida a GRO como uma prática institucional contínua, promovendo uma cultura de prevenção, resiliência e melhoria permanente em toda a USNAVY.

Nesse contexto e complementando a GRO sob o ponto de vista da segurança cibernética, será também analisado o Manual de Segurança Cibernética da USNAVY (USA, 2022b). Esse manual estabelece as diretrizes do Programa de Segurança Cibernética da USNAVY, buscando garantir uma postura segura e resiliente em todo o ciclo de vida tecnológico daquela Força. O programa abrange desde a interoperabilidade entre sistemas até a proteção de dados e redes, assegurando o suporte integral às missões de combate, inteligência e apoio.

Dessa forma, neste capítulo, serão identificados os aspectos da GRO da USNAVY, diferenciando-os sob os prismas de pessoas, processos, tecnologia e eventos externos, segundo as bases teóricas proporcionadas pelo Capítulo 2, relacionando-os como riscos cibernéticos operacionais daquela instituição.

3.1 POLÍTICA DE GRO NA USNAVY

O risco operacional para a Marinha dos Estados Unidos (USNAVY), gerenciado pela Gestão de Riscos Operacionais (GRO), abrange o potencial de perdas ou danos devido a diversos fatores, incluindo erro humano, processos inadequados e eventos externos. Trata-se de um processo sistemático projetado para minimizar esses riscos, identificando perigos, avaliando sua probabilidade e gravidade e implementando controles para mitigá-los, de acordo com a *Naval Postgraduate School* (NPS, 2025).

A norma *Operational Risk Management* (OPNAVINST 3500.39D), da USNAVY, de 29 de março de 2018, estabelece a política, as responsabilidades e os procedimentos para a aplicação da Gestão do Risco Operacional (GRO) em todas as atividades da USNAVY, inclusive nas instituições por ela contratadas, com o objetivo de aumentar a efetividade da missão, preservar vidas e proteger os recursos da organização (USA, 2018). De acordo com o Manual de Segurança Cibernética da

USNAVY (USA, 2022b), as informações nele contidas também são aplicáveis a todo o pessoal contratado, reforçando a abrangência daquelas normas.

Na OPNAVINST 3500.39D, a GRO é definida como uma ferramenta de tomada de decisão utilizada por pessoal de todos os níveis hierárquicos e todas as instituições que compõem a USNAVY para aumentar a eficácia operacional por meio da identificação, avaliação e gerenciamento de riscos, minimizando-os a níveis aceitáveis. Segundo a publicação, ao se reduzir o potencial de perdas, a probabilidade de uma missão ser bem-sucedida aumenta, minimizando prejuízos e custos. Também permite aumentar a capacidade da USNAVY tomar decisões embasadas em um processo formal e padronizado.

Importante destacar que, para a USNAVY, a GRO não se limita ao ambiente profissional. Ela também deve ser aplicada em atividades fora de serviço, contemplando um amplo espectro de perigos e riscos relacionados à vida cotidiana de seu efetivo. A norma estabelece que a GRO deve ser incorporada de forma contínua e abrangente, sendo uma responsabilidade de todos os militares e civis da instituição, 24 horas por dia, sete dias por semana, 365 dias do ano (USA, 2018).

Essa norma possui alguns fundamentos, compostos por uma estratégia, quatro princípios básicos e três níveis de decisão abrangentes a todos os níveis.

A estratégia, também chamada de “quatro pilares”, sustenta a implementação eficaz e contínua da GRO na USNAVY. Seus quatro fundamentos são:

a) Política e Liderança: estabelece que os líderes devem implementar os requisitos da GRO por meio de políticas que abranjam toda a Força, promovendo sua utilização em todos os níveis hierárquicos e mantendo um ambiente que estimule um retorno de informações (*feedback*) e a comunicação de riscos, incentivando a realimentação das informações por meio da cadeia de comando, para que lições aprendidas sejam repassadas por toda a organização;

b) Treinamento e Educação: o treinamento em GRO deve ser parte essencial da formação de todo o pessoal militar e civil, adaptado ao respectivo nível hierárquico e função, promovendo o desenvolvimento contínuo ao longo da carreira;

c) Avaliação e Responsabilização: estabelece a necessidade de métodos para avaliar o desempenho na aplicação da GRO por todo o pessoal e em todas as atividades, utilizando estruturas e ferramentas existentes para garantir a responsabilização; e

d) Ferramentas e Recursos: ressalta a importância de prover os recursos necessários (tempo, pessoal, orçamento, equipamentos) e desenvolver ferramentas adequadas, incentivando o compartilhamento de boas práticas.

Os princípios básicos da estratégia são quatro, fornecendo a base da GRO e uma estrutura para a sua implementação, conforme descritos a seguir (USA, 2018).

a) Aceitar riscos quando os benefícios superam os custos: o processo de ponderar os riscos em relação aos benefícios e ao valor da missão ou tarefa contribui para maximizar as chances de sucesso. Como o equilíbrio entre custos e benefícios é subjetivo, é essencial que as decisões de risco envolvam pessoal com conhecimento e experiência na missão ou tarefa em questão;

b) Não aceitar riscos desnecessários: um risco desnecessário é qualquer risco que, ao ser assumido, não contribui de forma significativa para o cumprimento da missão ou tarefa, ou que coloque em risco, sem justificativa, o pessoal ou os meios materiais. Se os perigos detectáveis não forem identificados, então riscos desnecessários serão aceitos. A GRO permite identificar perigos que poderiam passar despercebidos e oferece ferramentas para reduzir ou compensar esses riscos. Devem ser assumidos apenas os riscos realmente necessários para alcançar os objetivos da missão ou tarefa;

c) Antecipar e gerenciar riscos por meio de planejamento: integrar a GRO ao planejamento, em todos os níveis e o mais cedo possível, permite tomar decisões bem fundamentadas e implementar controles de risco eficazes. Essa prática aumenta a efetividade da GRO e contribui para a redução de custos. Um planejamento detalhado permite identificar os perigos associados e definir as etapas necessárias para a execução segura da missão; e

d) Tomar decisões de risco no nível apropriado: qualquer pessoa pode tomar uma decisão de risco, porém o nível adequado é aquele no qual ela tem autoridade para eliminar ou minimizar o perigo, implementar controles para reduzir o risco ou aceitá-lo formalmente. Os líderes, em todos os níveis, devem assegurar que o pessoal saiba qual é o limite de risco que pode assumir e quando a decisão deve ser encaminhada a um escalão superior. Garantir que as decisões de risco sejam tomadas no nível correto estabelece uma cadeia de responsabilidade clara. Ou seja, caso o indivíduo encarregado da execução da missão conclua que os controles disponíveis não são suficientes para reduzir o risco a um nível aceitável, ele deve elevar a decisão ao próximo nível da cadeia de comando.

Os três níveis de decisão da GRO, por sua vez, são basicamente diferenciados pelo fator de tempo disponível para o planejamento e preparação da missão, destacando-se na norma que não existe uma linha definida indicando término de um nível e início do outro. São eles (USA, 2018):

a) Detalhado (*In-depth*): usado em operações complexas e de alto risco, com ampla disponibilidade de tempo para análise aprofundada. Aplica-se a situações em que o tempo não é um fator limitante e se exige a “resposta correta” para o êxito da missão ou tarefa. Nesse nível, são utilizadas ferramentas como pesquisa e análise detalhada de dados disponíveis, diagramas, instrumentos analíticos, testes formais e acompanhamento de longo prazo dos perigos associados. Exemplos de aplicação da GRO neste nível incluem, entre outros: o planejamento de longo prazo de operações complexas ou contingenciais; a gestão de riscos técnicos e de sistemas durante o projeto de engenharia, especialmente na aquisição e introdução de novos equipamentos ou sistemas; a elaboração de doutrina tática e currículos de treinamento; e grandes revisões ou reparos em sistemas críticos;

b) Deliberado (*Deliberate*): usado em planejamentos regulares de operações e treinamentos. Aplica-se a situações em que há tempo suficiente para empregar a GRO durante o planejamento detalhado, visando obter a “melhor” solução para o cumprimento de uma missão ou tarefa. Nesse nível, o planejamento envolve, preferencialmente, pessoal experiente e técnicas como *brainstorming*, sendo mais eficaz quando realizado em grupo. O processo de planejamento da USNAVY é um exemplo típico nesse nível. Outros exemplos incluem: planejamento de missões, tarefas ou eventos de unidades; revisão de procedimentos operacionais padrão, rotinas de manutenção ou treinamento; atividades recreativas; e elaboração de planos de controle de danos e resposta a emergências; e

c) Crítico (*Time-critical*): aplicado em situações que exigem decisões imediatas, durante a execução das tarefas. Nível no qual o pessoal atua diariamente, tanto em serviço quanto fora dele. O nível crítico no tempo refere-se ao momento imediatamente anterior ao início ou durante a execução de uma missão ou tarefa. Nesse contexto, há pouco ou nenhum tempo disponível para elaboração de um plano formal. A melhor abordagem possível consiste em uma avaliação mental ou verbal rápida da situação nova, alterada ou em mudança.

No Anexo A, encontra-se a figura 3, contendo os níveis da GRO na USNAVY.

Em 2022, a USNAVY estabeleceu o Comando de Segurança Naval (*Naval Safety Command*), responsável por aprimorar a capacidade de identificar, comunicar e contabilizar riscos. Esse comando cumpre sua missão, sendo direcionado pelo Chefe de Operações Navais, por meio de quatro tarefas principais: avaliações; investigações de acidentes para determinar fatores causais; gestão e análise de dados; e desenvolvimento de políticas. Esse comando atua em todas as áreas da USNAVY, realizando e apoiando a gestão de riscos, inclusive os operacionais. As origens daquele comando são de 1951, com a atividade de segurança da aviação naval dos EUA, com o objetivo inicial de avaliar e publicar informações sobre segurança da aviação (USA, 2025).

A GRO pode, então, ser analisada pelos aspectos de pessoas, processos, tecnologia e eventos externos, a serem posteriormente comparados com a Marinha do Brasil, visando identificar similaridades e singularidades entre elas.

3.1.1 Aspectos Relacionados a Pessoas

A GRO na USNAVY é centrada nas pessoas, reconhecendo nelas tanto o principal recurso quanto o principal vetor de risco em todas as atividades, desde as mais rotineiras até operações complexas. Conforme destacado pela *Naval Postgraduate School* (NPS, 2025), o risco está presente em todas as tarefas, treinamentos, missões, operações e atividades pessoais. A causa mais recorrente de falhas ou insucessos em missões é o erro humano, frequentemente originado por fadiga, distração, treinamento inadequado, julgamento falho ou negligência e, sobretudo, pela incapacidade de gerenciar riscos de maneira estruturada e consistente.

A USNAVY entende que a mitigação desses riscos se dá pela identificação, avaliação e controle sistemático, permitindo decisões mais seguras por parte dos profissionais diretamente responsáveis pelas atividades. Para isso, é promovido um ambiente organizacional em que cada militar ou civil, independentemente da função, seja treinado, motivado e capacitado para incorporar a gestão de risco em sua rotina operacional e pessoal. A educação, o treinamento contínuo e a liderança ativa são pilares essenciais para mitigar os riscos oriundos do fator humano.

Todos os integrantes da USNAVY têm a responsabilidade de aplicar a GRO nas atividades sob sua responsabilidade. Essa responsabilidade é compartilhada de forma hierárquica, sendo os líderes incumbidos de garantir a conformidade com os

procedimentos estabelecidos, sendo reforçada esta afirmação pelo Manual de Segurança Cibernética da USNAVY, que considera o apoio das lideranças como seu fator mais importante em um programa de segurança cibernética. A aplicação efetiva da GRO é, portanto, uma responsabilidade coletiva, que se estende desde o nível estratégico, representado pelo Assistente Especial para Assuntos de Segurança do Chefe de Operações Navais (*Chief of Naval Operations Special Assistant for Safety Matters*), exercido por um oficial general, até o nível operacional e tático, nos quais os operadores dos sistemas e os comandantes de unidades atuam diretamente (USA, 2018; USA, 2022b).

As instâncias superiores, representadas pelo alto escalão daquela Força, são responsáveis por, dentro de suas áreas de atuação, emitir diretrizes específicas, consolidar lições aprendidas, identificar melhores práticas e integrar os resultados das autoavaliações anuais. Tais comandos devem ainda planejar e supervisionar o treinamento em GRO, assegurando que seus subordinados estejam qualificados de acordo com padrões previamente definidos. A validação da prontidão e eficácia das unidades é realizada com base em métricas objetivas, que permitem avaliar o desempenho individual e coletivo, promovendo a melhoria contínua da Força.

No âmbito do treinamento formal, instituições como o *Naval Service Training Command, Naval War College, Naval Education and Training Command, United States Naval Academy, Naval Postgraduate School* e outras entidades educacionais da USNAVY são encarregadas de implementar programas contínuos de capacitação. Esses programas são estruturados para acompanhar toda a trajetória do profissional na USNAVY, desde seu ingresso na Força e ao longo de toda sua carreira, assegurando uma base sólida e progressiva em GRO (USA, 2018).

A *Naval Postgraduate School*, em especial, possui programas que abordam treinamento para gerenciamento individual de risco e treinamento para supervisor de risco em equipes, ambos com regularidade e necessidade de reavaliação trienal. Também é fornecido um treinamento anual, para recertificação, conforme instruído na OPNAVINST 3500.39D (NPS, 2025).

Nos níveis táticos e operacionais, os comandantes, gerentes e supervisores, devidamente qualificados em GRO, têm a missão de garantir que os procedimentos sejam cumpridos de forma proporcional à patente ou função do efetivo. São responsáveis por relatar riscos identificados, especialmente aqueles que excedem sua autoridade decisória, promovendo o escalonamento adequado pelas vias de

comando. É também papel desses líderes incentivar o uso da experiência acumulada pelos militares mais antigos, utilizando-os como mentores nos processos de avaliação de risco junto às equipes.

O treinamento contínuo contempla tanto aspectos técnicos quanto comportamentais, com foco em precisão procedural, tomada de decisão sob pressão, e análise pós-ação (*debriefing*) para extração de lições aprendidas.

Além disso, a norma reforça que a GRO não se restringe ao contexto operacional, devendo ser aplicada também nas atividades cotidianas e pessoais, como forma de preservar a saúde, o desempenho e a prontidão do pessoal, garantindo assim o aprestamento da Força.

Por fim, a norma OPNAVINST 3500.39D destaca que o treinamento em GRO é obrigatório para todo o efetivo, desde o momento do ingresso. Ela enfatiza a necessidade de um ciclo contínuo de capacitação e renovação anual das qualificações, sustentado por indicadores e avaliações que possibilitam aferir, de forma objetiva, o nível de prontidão e a eficácia das unidades militares. Assim, a USNAVY assegura que o gerenciamento do risco operacional seja não apenas uma prática institucional, mas uma competência cultivada ao longo de toda a carreira de seus integrantes.

3.1.2 Aspectos Relacionados a Processos

Conforme anteriormente mencionado, os líderes na USNAVY, em todos os níveis, são responsáveis por assegurar que os procedimentos da GRO estão sendo cumpridos e registrados em relatórios e que recursos apropriados estejam disponíveis para o pessoal desenvolver suas tarefas. Estes relatórios produzidos devem seguir uma padronização previamente estabelecida, visando seu melhor processamento por toda a USNAVY, facilitando, assim, a amplificação do conhecimento gerado (USA, 2018; USA, 2022b).

Segundo a norma OPNAVINST 3500.39D, a qual deve ser revisada a cada cinco anos, o processo de execução da GRO é composto por cinco etapas por suas qualidades e sistemáticas contínuas e repetíveis, compondo um ciclo. Essas etapas devem ser aplicadas em qualquer tipo de atividade, seja durante o planejamento nos níveis Detalhado ou Deliberado ou em situações de resposta imediata, no nível Crítico, conforme previsto na própria norma. Este ciclo exige revisão sistemática de procedimentos antes, durante e após cada operação, com foco na garantia da

eficiência e eficácia da missão. Ainda segundo a norma, a única garantia de que o processo será eficaz é envolvendo as pessoas expostas aos riscos e aquelas que possuem conhecimento especializado no assunto da missão ou tarefa para resolvê-lo. Deve-se registrar nos relatórios os resultados de todas as etapas do processo, visando servir de referência durante a execução e em ações futuras, compartilhando o referido conhecimento.

Essas cinco etapas são descritas a seguir, onde as duas primeiras etapas incluem o levantamento dos riscos, baseado nos perigos[8] identificados, e as três etapas seguintes representam as ações para tratar os riscos identificados. O processo encontra-se ilustrado na figura 4 do Anexo A.

a) Identificar os perigos: reconhecer e listar todos os perigos potenciais associados a uma missão, tarefa ou atividade. Isso envolve a análise do ambiente, equipamentos, pessoal e processos envolvidos. A identificação de perigos é a base de todo o processo de GRO pois, se um perigo não for identificado, não poderá ser controlado;

b) Avaliar os perigos: é a avaliação do impacto potencial de um perigo, determinando a gravidade e a probabilidade de ocorrência dos perigos identificados. Essa avaliação permite priorizar os riscos com base em seu impacto potencial na missão. A gravidade é representada por uma tabela, sendo dividida em quatro categorias, de maior impacto para o menor impacto para uma missão: catastrófico, crítico, moderado e insignificante. Já a probabilidade é classificada como cinco categorias, de maior probabilidade de ocorrência para a menor probabilidade: frequente, provável, ocasionalmente, raramente e improvável. Estas duas variáveis combinadas compõem uma matriz de levantamento de riscos, conforme figura 5 do Anexo A.

c) Tomar decisões sobre o risco: comparar os riscos avaliados com os benefícios da missão e decidir se os riscos são aceitáveis ou se é necessário adotar medidas de controle adicionais. A decisão deve ser tomada no nível de autoridade apropriado. Nesta etapa, surgem as opções de decisões sobre rejeitar, evitar, adiar, transferir e compensar um risco, com efeitos resultantes específicos para cada

[8] Perigo é qualquer condição real ou potencial que possa causar ferimentos, doenças ou morte ao pessoal; danos ou perdas de equipamentos ou propriedades; degradação da capacidade da missão ou impacto na realização da missão; ou danos ao meio ambiente (sinônimo do termo ameaça) (USA, 2018).

decisão. Após cada decisão, deverá ser avaliada a existência de risco residual e, caso este seja considerado aceitável, dar continuidade ao processo;

d) Implementar controles: Aplicar medidas para eliminar o risco ou reduzir sua probabilidade e/ou gravidade. Isso pode incluir mudanças em procedimentos, treinamentos adicionais, aquisição de produtos ou contratação de serviços, implementando-as de forma clara, para ser compreendida por todos os envolvidos; com responsabilidades definidas, para que o decisor apropriado assuma suas atribuições; e suporte adequado, para garantir que haja pessoal, recursos e liderança adequada.

e) Supervisionar: consiste em monitorar a eficácia dos controles implementados ao longo da missão ou tarefa, garantindo que estão sendo seguidos e fazer ajustes conforme necessário. A supervisão contínua também permite a coleta de lições aprendidas para aprendizado e melhoria de futuras atividades.

Ao se tratar especificamente sobre risco cibernético operacional, o Manual de Segurança Cibernética da USNAVY (USA, 2022b), estabelece uma política na qual a segurança cibernética deve estar integrada e deve ser garantida em todos os processos de aquisições, desenvolvimentos ou modificações de sistemas de TI, necessitando também ser avaliada para o risco operacional.

De acordo com o referido Manual, para a USNAVY esses sistemas de TI possuem um significado mais abrangente, envolvendo tecnologias da informação e tecnologias operacionais, a serem descritos na seção a seguir neste Capítulo.

Ainda assim, aquelas soluções de TI que após suas avaliações de risco permaneceram com um risco residual “alto” ou “muito alto”, somente poderão ser implementadas ou adotadas após uma autoridade competente, em seu respectivo nível de delegação, aprovar seu uso.

Adicionalmente nesse Manual, os conceitos e diretrizes adotados pela USNAVY devem ser visíveis e identificáveis em todos os documentos de TI, da própria Força e de terceirizados, permitindo que sejam revisados e atestados para os resultados esperados das missões e para os objetivos estratégicos estabelecidos, incluindo salvaguardas para a proteção das referidas tecnologias. A norma prevê inclusive o monitoramento da performance das tecnologias contratadas visando garantir a conformidade delas com os requisitos de segurança estabelecidos (USA, 2022b).

De forma complementar, o Departamento de Defesa Americano (DoD) também definiu uma política para a estrutura de Gestão de Riscos de Segurança Cibernética para Sistemas do DoD, estabelecendo políticas, atribuindo responsabilidades e prescrevendo procedimentos para execução e manutenção dessa política em todos os órgãos a ele subordinado, incluindo a USNAVY (USA, 2022b). Nessa norma, são estabelecidos os *frameworks* de segurança da informação e segurança cibernética do *National Institute of Standards and Technology* (NIST) como os padrões a serem seguidos por todos os órgãos do DoD, inclusive ao se tratar de riscos operacionais cibernéticos.

Na abordagem adotada pela USNAVY, a GRO busca sistematizar a tomada de decisão sob risco em todas as atividades, do planejamento à execução, demonstrando que a falha ou a ausência de processos claros, consistentes e monitorados é uma fonte direta de risco operacional.

3.1.3 Aspectos Relacionados a Tecnologias

De acordo com a norma OPNAVINST 3500.39D, a GRO na USNAVY conta com diversas ferramentas de apoio que visam padronizar, facilitar e fortalecer a aplicação sistemática do processo de identificação, avaliação e controle de riscos em todos os níveis da organização (USA, 2018).

A efetiva integração da GRO em toda a USNAVY depende da disponibilidade de recursos adequados, como tempo, pessoal capacitado, orçamento e equipamentos, assim como do desenvolvimento e uso de ferramentas apropriadas às necessidades específicas de cada tipo de missão. Além disso, a norma destaca a importância de aproveitar os instrumentos já existentes e de fomentar o intercâmbio de ideias, experiências e boas práticas entre as suas unidades, promovendo uma cultura institucional de melhoria contínua na gestão de riscos (USA, 2018).

No Apêndice A, as ferramentas, técnicas e sistemas mencionados na norma encontram-se listadas no quadro 3. O aprofundamento nessas ferramentas e técnicas não faz parte deste trabalho.

Mesmo já existindo diversas ferramentas, é incentivada a pesquisa de novas tecnologias e treinamentos que venham a ser aplicáveis à cultura de GRO na USNAVY. Esta é uma das responsabilidades do Assistente Especial para Assuntos de Segurança do Chefe de Operações Navais, mais alto cargo que trata do assunto

naquela Marinha, devendo ser operacionalizada pelos Comandantes das instituições responsáveis pelos treinamentos formais (USA, 2018).

Nos níveis táticos e operacionais, os comandantes, gerentes e supervisores, devem garantir que os comandados utilizem tais ferramentas padronizadas.

Segundo o Manual de Segurança Cibernética da USNAVY (USA, 2022b), o programa de segurança cibernética engloba, dentro do termo Tecnologia da Informação (TI), todas as tecnologias e ativos de informação, incluindo mas não se limitando a: Sistemas de Informação (SI); aplicativos; Tecnologia Operacional (OT); Plataforma de TI (PIT) para incluir sistemas de armas, controle de propulsão e sensores diversos, por exemplo; Sistemas de Controle Industrial (ICS); Sistema de Controle de Supervisão e Aquisição de Dados (SCADA); Sistemas de Casco, Mecânicos e Elétricos (HM&E); Laboratório de TI de Pesquisa, Desenvolvimento, Teste e Avaliação (RDT&E); Produtos de TI; Serviços de TI, Serviços de Nuvem; e qualquer outro ativo de TI.

Embora a norma OPNAVINST 3500.39D não seja voltada especificamente para “sistemas de TI”, ela se refere à necessidade de se possuir contingência e redundâncias, as quais podem ser aplicadas aos equipamentos, sistemas de armas, comunicações, sensores e softwares embarcados como áreas nas quais falhas tecnológicas podem colocar em risco a missão, conforme ostensivamente indicados pelo Manual de Segurança Cibernética da USNAVY (USA, 2022b).

A tecnologia, cada vez mais presente nos meios e operações, necessita ser tratada como parte dos recursos críticos que devem ser avaliados quanto à confiabilidade, manutenção e suporte logístico, para o sucesso das missões.

3.1.4 Aspectos Relacionados a Eventos Externos

Segundo as normas em análise, os riscos decorrentes de eventos externos não são apresentados de forma taxativa, mas são claramente considerados dentro do processo de identificação de perigos e, posteriormente, na etapa de avaliação de riscos da GRO, como é o caso da OPNAVINST 3500.39D. Ao tratar das responsabilidades dos Comandantes, a OPNAVINST 3500.39D menciona que fatores externos podem comprometer o êxito de uma missão, embora não apresente uma lista específica dessas ocorrências (USA, 2018).

Entre os exemplos de eventos externos relevantes citados diretamente ou inferidos na norma, destacam-se (USA, 2018):

a) Condições meteorológicas adversas, como tempestades ou mar agitado;

b) Ambientes desconhecidos ou hostis, o que inclui riscos ambientais, geográficos ou relacionados ao teatro de operações;

c) Ameaças externas imprevistas, o que inclui fatores fora do controle da unidade, como ações inimigas ou mudanças no contexto operacional;

d) Eventos naturais ou técnicos fora do padrão, como falhas em infraestrutura, tecnologia indisponível ou atrasos logísticos; e

e) Riscos associados a atividades fora do serviço, abrangendo riscos externos diversos ao seu pessoal, como acidentes de trânsito ou pandemias, por exemplo.

Os ataques cibernéticos podem ser incluídos no terceiro caso, como uma das possíveis ameaças externas imprevistas, representando riscos que devem ser identificados na primeira etapa do processo da GRO, avaliados em termos de probabilidade e severidade, e, sempre que possível, mitigados por meio de controles operacionais e táticos adequados.

A norma OPNAVINST 3500.39D reconhece que os eventos externos são fatores incontroláveis, exigindo sua inclusão nos cenários de planejamento, tanto deliberado quanto crítico no tempo. Esses fatores são fundamentais na etapa de identificação de perigos, impactando diretamente a matriz de levantamento de riscos usada para orientar o emprego de recursos, a definição de medidas de contingência e a formulação de estratégias defensivas.

Os eventos externos identificados, bem como as estratégias adotadas para mitigá-los, devem ser posteriormente compartilhados pela cadeia de comando, de modo a disseminar boas práticas e fortalecer a cultura organizacional de gestão de riscos em todas as unidades.

3.2 CONSIDERAÇÕES PARCIAIS

Neste capítulo, foram realizadas as análises da norma OPNAVINST 3500.39D (USA, 2018), que estabelece a doutrina da Gestão do Risco Operacional (GRO) na Marinha dos Estados Unidos (USNAVY) e do Manual de Segurança Cibernética da USNAVY (USA, 2022b), que descreve aspectos fundamentais de segurança da informação para a USNAVY. A partir dessas análises, foi possível identificar como aquela instituição trata os riscos sob os aspectos de pessoas, processos, tecnologia e eventos externos, alinhando-se aos princípios originalmente estabelecidos pelo

Comitê de Basileia, que reconhece essas quatro categorias como fontes primárias de risco operacional em qualquer organização, seja ela militar ou civil.

A norma OPNAVINST 3500.39D sistematiza a GRO como um processo contínuo, padronizado e aplicado a todos os níveis hierárquicos, dentro e fora do serviço, sendo parte integrante da cultura de prontidão e eficácia da USNAVY. Estruturada em pilares estratégicos, princípios operacionais e níveis de aplicação (detalhado, deliberado e crítico), a doutrina norte-americana busca antecipar, mitigar e controlar riscos que possam comprometer a missão, o pessoal ou os recursos materiais da Força.

Já o Manual de Segurança Cibernética da USNAVY, também analisado, orienta a gestão de riscos cibernéticos ao longo de todo o ciclo de vida dos sistemas de tecnologia da informação (TI), assegurando-os contra ameaças internas e externas. Neste manual, tais sistemas englobam uma grande variedade de tecnologias tais como a Tecnologia Operacional (TO), que inclui sistemas de armas, controle de propulsão e sensores diversos, por exemplo. Dessa forma, a segurança cibernética, conforme estruturada no manual, é um componente essencial da gestão do risco operacional na USNAVY.

A USNAVY compreende a GRO não apenas como uma ferramenta de segurança, mas como um facilitador estratégico da decisão operacional, promovendo uma cultura institucional voltada à prevenção, preparação e adaptabilidade. A responsabilidade pela gestão de riscos é compartilhada de forma hierárquica, e todos os integrantes, civis e militares, são capacitados ao longo de suas carreiras para aplicar os procedimentos com base em critérios objetivos mensuráveis.

Além da abordagem interna, destaca-se a extensão da aplicação da GRO às organizações contratadas, com sua relevância abordada por ambas as normas analisadas, ampliando seu escopo a toda a cadeia de suprimentos[9] sob responsabilidade da USNAVY. Essa medida reforça a interdependência entre os sistemas militares e os parceiros civis, assegurando que a gestão de riscos seja abrangente, coerente e eficaz em todos os elos operacionais.

---

[9] Segundo o Conselho de Profissionais de Gestão da Cadeia de Suprimentos (em inglês, CSCMP), a gestão da cadeia de suprimentos visa integrar a gestão das ofertas e das demandas dentro e entre empresas, constituindo-se pelo planejamento e gerenciamento das atividades de demanda, aquisição e produção, assim como aquelas relacionadas ao gerenciamento da logística, por meio da coordenação e da colaboração dos fornecedores, intermediários, terceirizados e clientes (https://cscmp.org/CSCMP/Educate/SCM_Definitions_and_Glossary_of_Terms/CSC).

Assim, a GRO na USNAVY, com foco no risco cibernético operacional, configura-se como uma estrutura doutrinária robusta, adaptável e compatível com as melhores práticas internacionais, servindo como base para a futura comparação com o modelo adotado pela Marinha do Brasil (MB), a ser realizado no próximo Capítulo.

4 COMPARAÇÃO DA GRO ENTRE A USNAVY E A MARINHA DO BRASIL

A crescente complexidade dos ambientes operacionais modernos impõe às Forças Armadas a necessidade de estruturas robustas de Gestão do Risco Operacional (GRO), especialmente diante das crescentes ameaças cibernéticas.

Neste Capítulo serão comparadas as Gestões do Risco Operacional (GRO) da Marinha dos Estados Unidos da América (USNAVY) e da Marinha do Brasil (MB), observando-as sob os aspectos de pessoas, processos, tecnologia e eventos externos, segundo a base conceitual estabelecida no Capítulo 2. O risco cibernético operacional, enquanto especialização do risco operacional, será abordado como o foco desta pesquisa, evidenciando o modelo consolidado pela USNAVY, que abrange os níveis estratégico e operacional, em contraste com a abordagem predominantemente normativa e administrativa adotada pela MB.

Ao examinar os fundamentos doutrinários, a atribuição de responsabilidades, os mecanismos de capacitação, as ferramentas tecnológicas empregadas e a incorporação dos riscos cibernéticos, delineia-se um panorama que permite avaliar criticamente os avanços e as limitações de cada instituição. Ao tratar o risco cibernético operacional como variável estratégica e operacional, neste Capítulo busca -se subsidiar reflexões sobre o incremento da capacidade cibernética da MB, contribuindo para uma doutrina mais aderente aos desafios da atualidade.

4.1 POLÍTICA DE GRO NA MB COMPARADA À USNAVY

Assim como a Marinha dos Estados Unidos da América (USNAVY) deve seguir as normas do Departamento de Defesa (DoD), órgão ao qual está diretamente subordinado, a Marinha do Brasil (MB) também deve seguir os documentos de doutrinamento referentes às Forças Armadas Brasileiras emanados pelo Ministério da Defesa (MD), além de suas próprias normas internas.

Antes de analisar as normas da MB sob os aspectos de pessoas, processos, tecnologia e eventos externos, conforme o arcabouço teórico apresentado no Capítulo 2, faz-se necessário abordar alguns pontos abrangentes sobre tais normas.

Em maio de 2018, O Ministério da Defesa (MD) aprovou e publicou a Nota Escolar nº 002, “Gerenciamento do risco operacional (GRO) nas operações

conjuntas", da Comissão Interescolar de Doutrina de Operações Conjuntas (CIDOC[10]) (Brasil, 2018a), contendo orientações que servem "como convenção didática para a uniformização dos trabalhos escolares executados nas Escolas de Altos Estudos Militares" (Brasil, 2018a, p. 3/16). Tal documento, após a aprovação do Chefe do Estado-Maior das Forças Armadas (CEMCFA), subsidia o aperfeiçoamento da Doutrina de Operações Conjuntas e futuras atualizações de doutrinas e normas das Forças Armadas brasileiras.

Em setembro de 2020, o MD, aproveitando parcialmente o texto elaborado pela CIDOC, definiu para as Forças Armadas, em sua Doutrina de Operações Conjuntas (MD30-M-01), 2º volume, que os riscos operacionais são

> "conceituados como uma combinação de probabilidade e de gravidade dos potenciais danos ao andamento de uma operação, estarão associados à existência de perigos ou ameaças decorrentes de ações adversas advindas das possibilidades do oponente, fatores ambientais e demais incertezas da campanha" (Brasil, 2020b, p. 35).

Ao se analisar a Nota Escolar da CIDOC e a Doutrina de Operações Conjuntas comparando-as a norma *Operational Risk Management* (OPNAVINST 3500.39D), da USNAVY, emitida três meses antes, em março de 2018, é possível identificar similaridades e singularidades com relação ao risco operacional.

Na definição de risco operacional adotada pelo MD observa-se um alinhamento com a definição estabelecida pelo Comitê da Basileia, uma vez que as "ameaças decorrentes de ações adversas advindas das possibilidades do oponente" assim como "fatores ambientais" podem ser considerados como eventos externos e as "demais incertezas da campanha" podem ser atribuídas às pessoas, processos e tecnologias, completando os demais fatores de risco aos quais uma missão poderia estar exposta, ainda que de forma genérica. Observa-se na definição do MD uma priorização dos elementos externos em detrimento de elementos internos como fatores geradores de riscos operacionais. Essa pode ser considerada uma importante diferença entre as doutrinas das duas Marinhas analisadas.

Segundo a Doutrina de Operações Conjuntas, a gestão do risco operacional deve ser considerada como um processo "cíclico e intuitivo que contribui diretamente

---

[10] CIDOC - A CIDOC foi criada pela Portaria nº 316/MD, de 07 de fevereiro de 2012 com o objetivo de coordenar a uniformização do ensino da Doutrina de Operações Conjuntas nos Estabelecimentos de Ensino de Altos Estudos Militares das Forças Armadas e da ESG. Atualmente, a CIDOC tem as suas atividades reguladas pela Portaria GM-MD nº 3779, de 08 de julho de 2022 (https://www.gov.br/esg/pt-br/composicao/instituto-de-doutrina-de-operacoes-conjuntas/cidoc).

para o nível qualitativo das análises e decisões a serem tomadas” (Brasil, 2020b, p. 238), sendo, portanto, essencial para a segurança, a eficiência e a continuidade das operações, além de buscar reduzir a probabilidade e o impacto de possíveis perdas para a MB, similarmente ao identificado na USNAVY.

Conforme análise da Nota Escolar da CIDOC (Brasil, 2018a), verificou-se que o processo de GRO daquela Nota seguiu os mesmos princípios definidos nas normas da USNAVY. Porém, não apresentou os “quatro pilares” que sustentam aquela norma nem os níveis de decisão, que tratam do tempo disponível para o planejamento. O processo de gerenciamento dos riscos, ainda que seja diferente por apresentar-se com duas etapas a mais do que o processo apresentado pela USNAVY, contém as mesmas ações e atinge os mesmos objetivos.

Similarmente, o MD em sua Doutrina de Operações Conjuntas (Brasil, 2020b), não utilizou os “quatro pilares”, desconsiderando preceitos fundamentais que fortaleceriam o processo da GRO na MB. Com relação aos princípios, o MD nomeou-os como “pontos relevantes”, utilizando três dos quatro princípios básicos utilizados pela USNAVY: antecipação de riscos durante os planejamentos; aceitação de risco mediante relação custo x benefício; e decidir no nível adequado; e acrescentando outros dois novos pontos não existentes na USNAVY: integração entre os diversos componentes do Estado-Maior Conjunto (EMCj) e acompanhamento contínuo da efetividade das medidas de controle. Estas diferenças nas definições não afetam o processo de gestão de risco, uma vez que, em ambos os processos, os efeitos resultantes das ações adotadas pelas duas Forças são similares.

Já os níveis de decisão adotados pelo MD foram apenas dois, em contraste com os três níveis adotados pela USNAVY. No MD, foram estabelecidos os riscos para a campanha ou operação, no nível operacional; e os riscos para as Forças Componentes, com enfoque no nível tático, desconsiderando qualquer limite intermediário entre eles. NA USNAVY, os níveis “Detalhado”, “Deliberado” e “Crítico” não possuem uma linha definida separando-os e nível “Detalhado” é apropriado para o nível mais alto, o estratégico (Brasil, 2020b).

No âmbito interno da MB, são adotadas quatro normas básicas que tratam da gestão de riscos: a Portaria nº 110 do EMA, de 4 de maio de 2017, que aprova a Política de Gestão de Riscos da Marinha do Brasil (Brasil, 2017a); as Instruções para Implementação da Política de Gestão de Riscos da Marinha do Brasil (ARMADAINST nº 32-1), de 24 de maio de 2017 (Brasil, 2017b); as Normas Gerais de Administração

– 9ª Revisão (SGM-107), de 2024 (Brasil, 2024a); e o Manual de Segurança de Aviação – 5ª Revisão (DGMM-3010), de 2023, o qual trata especificamente do risco operacional aplicado à aviação naval (Brasil, 2023a).

A Política de Gestão de Riscos da Marinha do Brasil “tem como propósito orientar a gestão dos riscos associados ao alcance dos objetivos estratégicos da Marinha” (Brasil, 2017a, p. 22). Essa política, datada de 2017, identifica que a gestão de riscos é uma ferramenta consolidada a nível organizacional devendo ser aplicada por todas as Organizações Militares (OM) da MB, além de buscar a padronização e o alinhamento sobre o assunto na MB. Esclarece também que, no nível operacional, é aplicada nos planos de segurança orgânica e nos planos de prevenção de acidentes aeronáuticos, dentre outros. Porém, ao longo da pesquisa, não foram localizadas outras documentações da MB que tratassem do risco operacional. Diferentemente da USNAVY, uma publicação específica sobre o tema, a OPNAVINST 3500.39D, conforme analisado no capítulo anterior, é aplicada a toda aquela instituição.

A Política de Gestão de Riscos da MB considera que o risco pode ser “positivo”, representando oportunidades, ou “negativo”, representando ameaças à organização, conforme estabelecido nas normas da ABNT (ABNT, 2018). Na USNAVY, o risco é identificado apenas como um evento negativo, conforme as normas do *National Institute of Standards and Technology* (NIST), adotado pela USNAVY. A política na MB considera também que os riscos podem ser classificados pela sua origem, auxiliando na sua identificação e permitindo verificar se algum risco relevante não tenha sido considerado. Dessa forma, são classificados como:

a) riscos externos: associados ao ambiente externo, sobre os quais a MB não tem controle direto, ainda que ações possam ser tomadas quando necessário; e

b) riscos internos: associados à própria estrutura da MB, seus processos, sua estrutura de governança, pessoal, recursos ou ambiente tecnológico.

Os riscos também podem ser classificados de acordo com seu nível de tratamento, sendo:

c) risco estratégico: relacionados aos objetivos navais definidos pelo Órgão de Direção Geral (ODG);

d) risco setorial: impactam diretamente o alcance dos objetivos dos Órgãos de Direção Setorial (ODS); e

e) riscos locais: relacionados aos objetivos contidos nos planejamentos estratégicos das próprias OM.

Referente as Instruções para Implementação da Política de Gestão de Riscos da Marinha do Brasil (ARMADAINST nº 32-1), datada de 2017, define-se o propósito de estabelecer critérios claros que orientem e detalhem as instruções da Política de Gestão de Riscos da MB, estabelecendo uma estrutura de gestão de riscos na qual todas as OM da MB participam por meio de comissões e subcomissões de gestão de riscos. Não são mencionadas as instituições contratadas pela MB, constituindo sua cadeia de suprimentos, em nenhum momento, como pode ser verificado na USNAVY.

Segundo essa instrução, “a principal ferramenta da Gestão de Riscos da MB é o Plano de Gerenciamento de Riscos”, documento que “especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para o gerenciamento dos riscos” (Brasil, 2017b, p. 1), sendo detalhado e exemplificado na SGM-107, por meio do Programa Netuno[11] (Brasil, 2025).

Na ARMADAINST são estabelecidos critérios para as avaliações e para a gestão de riscos, mensurando as probabilidades e os impactos dos mesmos sobre os objetivos das OM da MB. Tais critérios são definidos por meio de tabelas contendo intervalos de probabilidades a serem empregadas às consequências dos riscos relacionados a execução de suas atividades constitucionais e subsidiárias. Dentre estas atividades, destacam-se duas, diretamente relacionadas com esta pesquisa: as “Tarefas Operacionais” e a “Segurança das Informações Digitais” (Brasil, 2017b, p. 8).

Na primeira, são mensurados os impactos dos riscos sobre as atividades operacionais da MB, enquanto na segunda, são mensuradas as eventuais ameaças que podem comprometer as informações da MB.

Similarmente à USNAVY, essa documentação da MB relaciona a importância da aferição dos riscos relacionados com o ambiente operacional e com a tecnologia da informação, ambos de importância fundamental para a mensuração do risco cibernético operacional. Porém, uma grande diferença entre a MB e a USNAVY é a indicação pela ARMADAINST de que são consideradas apenas as “bases de dados” e os “fluxos de informações” da MB para a gestão de riscos. Na USNAVY, de acordo com seu Manual de Segurança Cibernética (USA, 2022b), a Tecnologia da Informação (TI) é muito mais abrangente, preocupando-se não apenas com bases de dados e fluxos de informação, mas com tudo o que se refere a sistemas de TI, Tecnologia

[11] O Programa Netuno possui um conjunto de ferramentas para a excelência de gestão administrativa da MB. Ele encontra-se disponível na página http://netuno.dadm.mb na Intranet da MB (Brasil, 2025).

Operacional (TO), sistemas de armas, controle de propulsão, Sistemas de Controle Industrial (ICS); Sistema de Controle de Supervisão e Aquisição de Dados (SCADA), dentre outros. Esta visão holística da USNAVY aumenta consideravelmente sua capacidade de proteção cibernética uma vez que consegue prever o risco operacional cibernético para todos os seus sistemas tecnológicos, sejam eles administrativos ou operativos.

Na MB, os sistemas digitais são diferenciados pelo seu campo de aplicação e localização de instalação, sendo categorizados em dois tipos: Sistemas Digitais Administrativos (SDA) e os Sistemas Digitais Operativos (SDO). Os SDA são sistemas projetados para apoio às atividades administrativas da MB. Os SDO são projetados para o emprego em operações navais ou em benefício delas (Brasil, 2019c).

Segundo as Normas de Tecnologia da Informação da Marinha (2019c), as auditorias de segurança da informação e proteção cibernética, relativas aos ativos computacionais da MB são realizadas focando apenas nos SDA. Não existe norma específica quanto à segurança da informação e proteção cibernética dos SDO ou das infraestruturas críticas da MB que trabalham com tecnologia operacional. Esse hiato cria um risco cibernético operacional considerável.

Na USNAVY, conforme mencionado no Capítulo anterior, as normas abrangem todos estes aspectos, e não apenas a parte administrativa de suas infraestruturas computacionais como na MB.

Referente as Normas Gerais de Administração – 9ª Revisão (SGM-107), é uma publicação com foco na "gestão administrativa na Marinha do Brasil" e com o "propósito de orientar a implantação da Excelência em Gestão nas Organizações Militares (OM)" (Brasil, 2024a, p. VI). Os aspectos operacionais são abordados, porém com um viés totalmente administrativo. Ainda assim, essa norma categoriza os riscos em diversos tipos quanto a sua origem: riscos externos ou riscos internos; quanto ao seu tipo: legais, financeiros, reputacionais[12], humanos, dos processos, tecnológicos e à integralidade; e quanto ao contexto de análise: estratégico, gerencial e operacional. Desses, destacam-se os externos, internos, humanos, dos processos, tecnológicos e

[12] Riscos reputacionais – riscos que podem comprometer a confiança da sociedade em relação à capacidade da MB, ou das OM em cumprir sua missão institucional (Brasil, 2024a, p. 5-2).

operacional, pois são passíveis de serem mapeados para os riscos cibernéticos operacionais, conforme estudo nesta pesquisa.

Nessa norma, as etapas da gestão de riscos são similares às já pesquisadas, possuindo cinco passos: identificação de riscos; análise e avaliação de riscos; planejamento das respostas aos riscos; e implementação do gerenciamento de riscos, monitoramento e controle. Esse ciclo é similar aos adotados pelo MD e pela USNAVY quanto aos objetivos alcançados, ainda que se diferenciem nas fases.

Essa abordagem “administrativa” é confirmada e reforçada pela publicação Estruturação das Áreas de Conhecimento e das Habilitações da Marinha (EACH-MB), de 2019, que trata do gerenciamento das Áreas de Conhecimento (AC) de interesse da MB. Nessa publicação, a Diretoria de Administração da Marinha (DAdM), organização militar responsável por contribuir para a gestão administrativa da MB, abrangendo a gestão financeira, de recursos humanos, materiais e serviços gerais, é estabelecida como a Organização Militar Orientadora Técnica (OMOT) da área de conhecimento “Gestão de Riscos” para a MB (Brasil, 2019b). Não há nenhuma outra referência a uma gestão voltada para o risco operacional. Na USNAVY, o risco operacional é estudado a fundo pela *Naval Postgraduate School* (NPS, 2025), além de ser regulamentado pelo *Naval Safety Command* (USA, 2025).

Nesse contexto, cabe ainda referenciar o Manual de Segurança de Aviação – 5ª Revisão (DGMM-3010), publicação de 2023, que possui o propósito de regulamentar o Serviço de Investigação e Prevenção de Acidentes Aeronáuticos da Marinha (SIPAAerM) e estabelecer normas para gerenciar a segurança da aviação naval, orientando a prevenção e investigação de acidentes aeronáuticos. Ressalta-se que essa foi a única norma da MB identificada durante a pesquisa bibliográfica que trata especificamente sobre risco operacional presente em operações da MB (Brasil, 2023a).

Essa norma considera a GRO como uma ferramenta de prevenção e redução dos riscos inerentes às operações militares. Singularmente, na USNAVY a GRO, ainda que possua essa mesma finalidade, é aplicável a toda a Força Naval e não apenas à sua aviação.

Com todas essas normas sobre gestão de risco operacional às quais a MB deve seguir, pode-se realizar uma análise pormenorizada dos aspectos de pessoas, processos, tecnologia e eventos externos, comparando-os às normas da USNAVY visando identificar suas similaridades assim como suas singularidades.

4.1.1 Comparações Quanto aos Aspectos Relacionados a Pessoas

A USNAVY estabelece a importância da participação de todos, independentemente de seu nível hierárquico, na gestão dos riscos operacionais, de forma que esta participação se inicie o mais cedo possível no planejamento das operações. Na USNAVY, todos são responsáveis pela gestão de riscos, do mais moderno ao mais antigo e a gestão de riscos deve ser ensinada, treinada e aperfeiçoada por todos os militares e civis daquela instituição justamente por considerar que todos devem possuir tais conhecimentos (USA, 2022a).

Na Doutrina de Operações Conjuntas (Brasil, 2020b), essa importância não fica clara e recai no “Comandante e seu EMCj” além do “emprego judicioso de especialistas” (Brasil, 2020b). De acordo com essa Doutrina, a GRO é intuitiva, embasando-se nas análises e experiências dos participantes, constituindo-se mais em arte do que em ciência. Na USNAVY, busca-se racionalizar mais esse processo, desmistificando e tornando-o acessível a todos na Força, desde seu ingresso.

Ao se analisar as normas internas da MB, verifica-se que a Política de Gestão de Riscos da MB estabelece que a capacitação e os conhecimentos sobre gestão de riscos serão realizados para os “militares e/ou servidores civis da MB envolvidos com a Gestão de Riscos” (Brasil, 2017a, p. 27). Esse diferencial entre as Marinhas analisadas nesta pesquisa pode ser considerado como uma de suas maiores disparidades.

De acordo com a Política de Gestão de Riscos da MB (Brasil, 2017a), as decisões referentes à governança dos riscos estratégicos são de competência do Comandante da Marinha, assessorado pelo Almirantado quanto aos assuntos de gestão de riscos estratégicos. De maneira similar, na USNAVY as decisões são de responsabilidade de um alto escalão daquela Força (USA, 2022a).

Quanto a SGM-107, verifica-se o estabelecimento da responsabilidade sobre a gestão de riscos ao Conselho de Gestão, composto por um presidente e diversos outros membros, técnicos e administrativos. Porém, permanece uma atividade administrativa, conforme analisado.

Quanto ao Manual de Segurança de Aviação, estabelece-se que o processo da GRO provê aos Comandantes e seus subordinados uma ferramenta para reduzirem os riscos a operações militares, atribuindo aos Titulares das OM, no caso, daquelas com capacidade de conduzir ou apoiar operações aéreas, a responsabilidade de

certificar-se que todos os membros da tripulação possuam os conhecimentos necessários para a aceitação do risco operacional. É também estabelecida uma estrutura hierarquizada, similar ao observado na USNAVY, para o controle e prevenção dos riscos operacionais aeronáuticos, alcançando desde o Comandante da OM até os indivíduos em geral, em suas respectivas áreas de atuação (Brasil, 2023a).

4.1.2 Comparações Quanto aos Aspectos Relacionados a Processos

A gestão do risco operacional, no contexto das Forças Armadas no Brasil, deve ser conduzida conforme os sete passos enunciados na Doutrina de Operações Conjuntas (Brasil, 2020b), resumidamente expostos a seguir:

a) Identificação das Ameaças: realizado desde o início do Planejamento Operacional, devendo considerar diferentes aspectos da missão (inimigo, forças adversas, área de operações, vulnerabilidades da própria Força, fator de tempo e espaço, dentre outros). Cabe ressaltar que ameaças e vulnerabilidades deveriam ser apresentadas separadamente, pois a primeira representa “qualquer conjunção de atores, entidades ou forças com intenção e capacidade de, explorando deficiências e vulnerabilidades, realizar ação hostil contra o país e seus interesses nacionais” (Brasil, 2015, p. 27), enquanto a segunda é definida como uma fraqueza inerente a “uma força, sistema, instalação ou equipamento, que pode ser explorada por um oponente para auferir vantagens” (Brasil, 2015, p. 281). Este passo é similar ao primeiro passo do processo apresentado pela USNAVY;

b) Avaliação dos Riscos Decorrentes: avaliação dos potenciais impactos negativos à campanha ou operação, decorrentes das ameaças identificadas na etapa anterior, utilizando-se a matriz “Probabilidade de Ocorrência X Gravidade”, a partir da qual obtém-se uma classificação padronizada dos riscos identificados. A figura 6 do Anexo A contém uma ilustração da matriz. Assim como na USNAVY, este segundo passo apresenta a Matriz de Probabilidade versus Gravidade. No caso da norma brasileira, existem quatro níveis de probabilidade e quatro de gravidade. Já na USNAVY a probabilidade possui uma classificação a mais;

c) Formulação de Medidas de Controle do Risco: para cada risco associado a cada uma das ameaças ou vulnerabilidades identificadas, serão tomadas medidas de controle de risco, mitigando-os e identificando os responsáveis pela sua implementação e acompanhamento. Nesse passo e nos dois seguintes, a norma

brasileira separa o passo de “Tomar decisões sobre o risco” da norma americana, pormenorizando as ações a serem adotadas;

d) Avaliação do Risco Residual: após as medidas de controle de risco propostas, o comandante e seu Estado-Maior devem rever a classificação do risco, obtendo, assim, o risco residual[13];

e) Decisão do Risco: momento em que o comandante aceita ou rejeita o risco residual, formulando novas medidas de controle, ou a sua submissão à apreciação de autoridade superior, ou mesmo a rejeição do risco, caso inaceitável;

f) Implementação das Medidas de Controle do Risco: aplicação das medidas de controle formuladas pelos analistas de risco e aprovadas pelo comandante. Nesse passo, as normas se equivalem; e

g) Acompanhamento da Aplicação das Medidas de Controle do Risco: acompanhamento das medidas de controle, de forma oportuna e segura, verificando a efetividade das providências de mitigação do risco. Esse último passo também se equipara ao quinto passo da norma americana.

Diferentemente, na USNAVY são adotados cinco passos. Ainda assim, os resultados para esses processos permanecem os mesmos, identificando, tratando e acompanhando os riscos.

No Anexo A, a figura 7 ilustra o fluxo completo da gestão do risco operacional da Doutrina de Operações Conjuntas (Brasil, 2020b).

No âmbito interno da MB, a Política de Gestão de Riscos da MB (Brasil, 2017a) estabelece que o processo de gestão de riscos deverá seguir as normas técnicas da ABNT NBR ISO da série 31000 (ABNT, 2018). Similarmente, a USNAVY utiliza uma norma técnica especializada do *National Institute of Standards and Technology* (NIST), assim como a MB utiliza as normas da ABNT.

De acordo com essa Política, na MB, o processo de gestão de riscos segue cinco fases: Identificação de Riscos, Análise e Avaliação de Riscos, Tratamento de Riscos, Monitoramento de Riscos e Comunicação.

A fase de identificação define os riscos operacionais como

> “eventos que podem comprometer as atividades da MB e são normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, ou de eventos externos, tais como:

[13] Risco residual é aquele que permanecerá mesmo após aplicação das “medidas de controle” selecionadas.

> qualificação do pessoal, impacto ambiental, segurança e saúde no trabalho, qualidade dos produtos e serviços etc.” (Brasil, 2017a, p. 23).

Esta definição é similar a definição adotada pela USNAVY ao mencionar as possibilidades de problemas decorrentes, em linhas gerais, provenientes de pessoas, processos, tecnologias ou eventos externos.

O restante das fases é também similar ao adotado pela USNAVY, inclusive com a utilização de uma matriz de riscos, montada a partir da relação das probabilidades e dos impactos dos riscos identificados. Ainda que na MB tais fases possuam descrições ligeiramente diferentes, todas abordam os mesmos procedimentos adotados na USNAVY, completando um ciclo de levantamento, análise, mitigação, supervisão e comunicação dos riscos identificados.

Ainda dentro do âmbito da MB, de acordo com a ARMADAINST, o processo de elaboração do Plano de Gerenciamento de Riscos deve ser integrado aos demais processos de planejamento da MB, permitindo a avaliação de seus riscos, auxiliando a Alta Administração Naval em tomadas de decisões mais efetivas. O resultado desse processo é um documento que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para o gerenciamento dos riscos (Brasil, 2017b). Porém, não é fornecido um modelo padronizado a ser seguido pela MB.

Segundo o Manual de Segurança de Aviação (Brasil, 2023a), o processo da GRO possui seis etapas: Identificar os perigos; Avaliar os riscos; Analisar medidas de controle do risco; Decisão de risco; Implementar as medidas de controle do risco; e Supervisionar. Essas etapas são similares às etapas apresentadas pelas publicações analisadas, incluindo aquelas adotadas pela USNAVY, diferenciando-se apenas na quantidade de passos desde a identificação dos riscos até seu tratamento e supervisão. Destaca-se como uma metodologia própria, voltada para a aviação naval, adotada nesse Manual para a análise dos perigos a serem identificados. Nessa metodologia, deve-se: inicialmente, estabelecer o perigo genérico; a seguir, identificar os componentes específicos do perigo; e, finalmente, orientar para as consequências específicas. Esta metodologia busca simplificar a identificação dos perigos aos quais a missão está sujeita. Similarmente, a USNAVY em sua etapa de identificação de perigos, busca simplificar e orientar a identificação dos perigos às suas missões, ainda que forneça instruções mais aprofundadas para alcançar tal objetivo.

Nesse Manual são adotados os mesmos três níveis de aplicação do risco operacional observado na USNAVY, quais sejam: Tempo Crítico, similar ao nível

Crítico adotado pela USNAVY; Deliberado, com o mesmo nome utilizado por aquela Marinha; e em Profundidade, com as mesmas características do nível Detalhado daquela Força. Esses níveis são aplicados de acordo com a complexidade das tarefas, tempo e recursos disponíveis para cada operação (Brasil, 2023a). Igualmente, adota os mesmos princípios observados naquela Marinha: Antecipar e gerenciar os riscos durante o planejamento; Considerar a relação custo x benefício antes de aceitar o risco; Decidir no nível adequado; e Rejeitar riscos desnecessários.

Essas similaridades observadas aproximam esta norma com a OPNAVINST 3500.39D da USNAVY que trata do risco operacional.

4.1.3 Comparações Quanto aos Aspectos Relacionados a Tecnologias

Segundo a Doutrina de Operações Conjuntas do MD, são disponibilizadas como ferramentas de apoio ao planejamento das operações, os anexos “H” e “O”, àquela norma, que tratam de defesa cibernética e do gerenciamento do risco operacional, respectivamente. Ainda que não seja diretamente mencionado, esses anexos poderiam ser utilizados para o levantamento também dos riscos cibernéticos operacionais, em especial o “H”, que trata do levantamento dos sistemas a serem protegidos ciberneticamente.

De acordo com a ARMADAINST, “A principal ferramenta da Gestão de Riscos da MB é o Plano de Gerenciamento de Riscos” (Brasil, 2017b, p. 1). Neste documento são especificadas as faixas de probabilidades de ocorrência dos riscos, assim como as probabilidades de suas consequências, permitindo a confecção da matriz de risco. Tanto as ocorrências quanto as consequências são definidas em cinco classificações. Diferentemente na USNAVY, são adotados cinco níveis para a probabilidade de ocorrência e apenas quatro para o impacto ou consequência. Uma maior quantidade de classificações, como ocorre na tabela da ARMADAINST, permite uma distribuição mais acurada dos riscos identificados.

Destaca-se na SGM-107 uma ferramenta de gestão de risco utilizada por todas as OM da MB conhecida como Programa Netuno (Brasil, 2025). Esse Programa “estabelece estratégias e práticas de gestão relacionadas às responsabilidades e deveres do administrador em auxílio à tomada de decisão” (Brasil, 2024a, p. 1-1). Por meio desse Programa os Titulares das OM realizam o levantamento dos riscos às suas OM, por meio de um Plano de Gerenciamento de Riscos (PGR), incluindo aqueles relacionados à Tecnologia da Informação (TI) ou cibernéticos, de uma

maneira geral. De acordo com o EMA-419, a segurança da informação possui uma área de interseção com a segurança cibernética, a qual abrande os riscos cibernéticos. A figura 8 do Anexo A ilustra tal interseção. Dessa forma, é possível utilizar as informações contidas nos relatórios das OM no Programa Netuno como fonte de informações para esta pesquisa.

Dessa forma, foi realizada uma análise dos relatórios, todos ostensivos, disponíveis na página do referido Programa, acessados em 29 de março de 2025, buscando-se analisar quais OM consideram os riscos tecnológicos em suas gestões. Obtiveram-se os resultados a seguir (Brasil, 2025).

Foram identificadas 69 OM com PGR disponibilizados, representando um espaço amostral de 17% das OM de toda a MB, que contabilizam um total de 417 OM, de acordo com o Organograma da MB, de 14 de janeiro de 2025. Desse espaço amostral, todos os Órgãos de Direção Setorial (ODS) e o Órgão de Direção Geral (ODG) tiveram ao menos uma OM subordinada representante. Dessas OM, observou-se que 13% não mencionou nenhuma informação referente a segurança da informação ou risco cibernético; enquanto 16% mencionaram, especificamente, o risco cibernético como risco em seu planejamento; e 87% mencionaram, ao menos, o risco em segurança da informação. Observou-se também que: 7% das OM não indicou uma validade para seus PGR; 12% possuem um PGR com validade para 2025 ou 2026; 16% possuem PGR vencido a um ano (2024); e 65% possuem PGR vencido a dois ou mais anos (Brasil, 2025).

Os riscos operacionais tecnológicos identificados e relatados pelas OM em seus PGR, foram: a necessidade de investimentos nos equipamentos obsoletos, a exposição da imagem da OM em redes sociais e a interrupção da operação da Rede de Comunicações Integrada da Marinha (RECIM). Porém, não foram relacionados riscos cibernéticos operacionais referentes às atividades das OM, sejam elas administrativas ou operativas. Tampouco foram identificados riscos referentes às infraestruturas críticas navais, excetuando-se a RECIM, conforme mencionado.

Analisando os números referentes aos PGR das OM, verifica-se que a preocupação com riscos cibernéticos operacionais ainda não está totalmente difundida na MB.

Essas estatísticas sobre os Planos de Gerenciamento de Riscos (PGR) das OM da MB estão apresentadas no quadro 4 do Apêndice A.

No Manual de Segurança de Aviação (Brasil, 2023a), são mencionadas as técnicas de *Brainstorming*, o uso de diagramas e ferramentas de análise, testes e ensaios, planilhas de risco, a análise do histórico dos riscos associados a determinado sistema ou operação, assim como a Matriz de Gerenciamento de Riscos que, nesta norma, adota cinco níveis de gravidade e cinco níveis de probabilidade. Conforme já mencionado, na USNAVY são adotados cinco níveis para a probabilidade de ocorrência e apenas quatro para o impacto. Uma matriz de risco com mais níveis permite uma classificação mais acurada dos riscos identificados.

4.1.4 Comparações Quanto aos Aspectos Relacionados a Eventos Externos

Segundo a Doutrina de Operações Conjuntas (Brasil, 2020b), todas as ameaças e vulnerabilidades relevantes e conhecidas que possam comprometer ou interferir nas ações das Forças necessitam ser relacionadas no planejamento de uma campanha/operação. Nas normas da USNAVY esses riscos externos existem, porém não estão claramente definidos, tendo sido inferidos nas normas analisadas.

Nessa Doutrina, o ataque cibernético é considerado na análise operacional de defesa cibernética, constituindo uma das necessidades a serem identificadas como risco para as operações. São mencionadas as necessidades de proteção às infraestruturas críticas e redes computacionais, assim como a necessidade de identificar as forças inimigas, suas capacidades e as possibilidades das forças amigas. Todos esses fatores possuem uma grande diversidade de riscos operacionais, inerentes e mapeáveis do ponto de vista do risco cibernético, considerando os aspectos abordados por esta pesquisa (Brasil, 2020b).

Na Nota Escolar da CIDOC (Brasil, 2018a), são sugeridas e apresentadas as seguintes ameaças cibernéticas, todas classificadas como risco “alto” para a Força:

a) Ataque cibernético ao computador do sistema de armas de um navio escolta;

b) Ataque cibernético a múltiplos sistemas de comando e controle de uma Diretoria Especializada impossibilitando o gerenciamento de unidades subordinadas e prejudicando a coordenação de fogos e apoio da Força Aérea Componente; e

c) Ataque cibernético ao Centro de Operações Militares (COpM) de um Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA), ocasionando a manipulação, pelo inimigo, dos dados de voo e rotas de aeronave na Área de Operações.

Conforme mencionado, o investimento da MB na modernização de seus meios navais e de fuzileiros navais, assim como a responsabilidade na proteção cibernética de suas infraestruturas críticas, faz com que essas ameaças sejam consideradas nos planejamentos das operações. Porém, esses exemplos da CIDOC não foram utilizados na Doutrina de Operações Conjuntas do MD (Brasil, 2020b).

No Manual de Segurança de Aviação (Brasil, 2023a), os riscos provenientes de eventos externos são apresentados como eventos que afetam a segurança aeronáutica, tais como existência de aglomeração de pássaros e condições meteorológicas desfavoráveis, por exemplo. Também são relacionados os equipamentos e sistemas de tecnologia da informação sendo empregados no controle do espaço aéreo como possíveis fatores de risco, o que não abrange todas as possibilidades de riscos cibernéticos operacionais existentes nas operações aéreas ou em missões que as utilizem, tais como os sistemas embarcados e suas tecnologias operacionais. Diferentemente, a USNAVY entende que as tecnologias operacionais fazem parte dos riscos operacionais.

4.2 CONSIDERAÇÕES PARCIAIS

A comparação entre os modelos de Gestão do Risco Operacional (GRO) da Marinha dos Estados Unidos (USNAVY) e da Marinha do Brasil (MB) evidencia alinhamentos conceituais com normas internacionais, como a ISO 31000, no caso da MB, e o NIST, no caso da USNAVY, e as diretrizes de Basileia, mas revela diferenças estruturais ao se tratar de pessoas, processos, tecnologias e eventos externos.

A USNAVY adota uma doutrina consolidada e operacionalizada, por meio da OPNAVINST 3500.39D, de aplicação institucional. Na MB, a normatização é fragmentada e predominantemente administrativa, com escassa presença operacional, limitada ao Manual de Segurança de Aviação (DGMM-3010), no qual o risco operacional é ostensivamente tratado e regulado.

A abordagem norte-americana, por sua vez, valoriza e cobra a participação de todos os níveis hierárquicos, imputando responsabilidades na aplicação e aprimoramento da GRO naquela Força, sendo aplicada e mensurada em todos os seus militares, desde seu ingresso na Força, aplicável também a todos os seus contratados. A MB, por sua vez, restringe essa atribuição aos setores técnicos especificamente voltados para a gestão de riscos em detrimento do restante da

tripulação, o que limita a difusão da cultura de risco entre os níveis operacionais e táticos.

Os processos de gestão de risco são similares entre as Forças quanto às suas etapas, mas a USNAVY foca a criticidade da missão e o tempo disponível para a decisão, ao passo que a MB aplica uma metodologia formal com ênfase institucional e critérios administrativos.

Ao abordar sobre tecnologia, a USNAVY trata os riscos de forma abrangente, envolvendo sistemas de armas, redes de tecnologia da informação, tecnologia operacional e infraestruturas críticas, enquanto a MB limita sua análise à segurança da informação dos sistemas administrativos, desconsiderando os sistemas operativos e as infraestruturas críticas, desconsiderando sua ampla adoção em todos os seus setores.

A USNAVY também incorpora ameaças externas como parte central da análise de missão, enquanto a MB reconhece tais riscos, mas com baixa integração operacional.

Por fim, o risco cibernético é tratado de forma holística pela USNAVY, integrando-o como variável essencial da segurança operacional, ao passo que, na MB, sua aplicação ainda é restrita, sendo muitas vezes ignorado por diversas organizações militares. Em síntese, a MB possui estrutura normativa coerente, mas carece de integração operacional e maturidade cultural em gestão de riscos operacionais comparável àquela observada na USNAVY.

No quadro 5 do Apêndice A, encontram-se todos os aspectos observados nas GRO das Forças, indicando as similaridades e as singularidades entre elas pesquisadas neste trabalho, servindo como subsídio para o desenvolvimento e apresentação das propostas de emprego da GRO na MB. No próximo capítulo, voltado para o aumento da capacidade cibernética da Força, especialmente quanto às ações de proteção cibernética, assim como a apresentação de possibilidades de trabalhos futuros sobre os temas abordados.

5 PROPOSTA DE GRO PARA A MB COM ENFOQUE NO RISCO CIBERNÉTICO OPERACIONAL

Em um cenário global marcado pela crescente complexidade dos ambientes operacionais e pela ascensão do domínio cibernético como elemento decisivo nos conflitos contemporâneos, torna-se imprescindível que as Forças Armadas adotem práticas de gestão de riscos capazes de proteger seus ativos, garantir a continuidade de suas operações e assegurar o cumprimento de suas missões. Inserida nesse contexto, a Marinha do Brasil (MB) enfrenta o desafio de revisar e modernizar seus modelos de Gestão do Risco Operacional (GRO), sobretudo no enfrentamento dos riscos cibernéticos operacionais. Diferente das ameaças tradicionais, o risco cibernético ultrapassa fronteiras físicas, afetando sistemas administrativos, operacionais, plataformas de combate, sensores, redes de comando e controle, além de infraestruturas críticas que sustentam o Poder Naval.

Neste capítulo apresentam-se propostas baseadas na análise comparativa entre os modelos da Marinha dos Estados Unidos (USNAVY) e da MB, à luz da teoria do risco operacional e dos fundamentos doutrinários discutidos nos capítulos anteriores e ilustradas no quadro 5 do Apêndice A. Dessa forma, as propostas são estruturadas sob cinco eixos centrais — generalidades, pessoas, processos, tecnologias e eventos externos — e visam corrigir lacunas existentes na MB e alinhar sua doutrina e suas práticas às melhores referências pesquisadas na USNAVY.

Ao percorrer as seções deste capítulo, o leitor será conduzido por uma reflexão crítica e propositiva, que revela a urgência de se transformar a gestão de riscos em uma ferramenta efetiva de apoio à decisão operacional, capaz de fortalecer a resiliência, a prontidão e aumento da capacidade cibernética da MB diante dos desafios do século XXI.

5.1 ASPECTOS RELACIONADOS A GENERALIDADES DAS NORMAS

A análise comparativa das práticas adotadas pela USNAVY evidencia que a criação de uma Organização Militar (OM) específica e especializada para a Gestão do Risco Operacional (GRO) — representada atualmente pelo *Naval Safety Command* (NAVSAFECOM) — constitui-se como um dos pontos críticos para o sucesso da implementação de uma cultura institucional de segurança e gerenciamento de riscos naquela Força. Esta estrutura remonta à década de 1950, quando foi inicialmente

concebida como *Naval Aviation Safety Center*, com o propósito de reduzir os índices alarmantes de acidentes na aviação naval da época (USA, 2025).

Ao longo das décadas, sua missão foi ampliada de forma sistemática, incorporando as áreas de segurança de superfície, submarina, de forças especiais e, mais recentemente, a segurança cibernética associada às operações navais. Em sua configuração atual, desde a sua reformulação em 2022, o NAVSAFECOM não apenas estabelece as normas e diretrizes de segurança da USNAVY, mas também desempenha papel central na prevenção de acidentes, proteção de vidas, preservação de meios, resiliência operacional e fortalecimento da prontidão das forças, integrando a gestão do risco como elemento estruturante da doutrina, do treinamento e do emprego operacional.

A ausência de uma estrutura similar na MB representa uma limitação à consolidação de um modelo institucionalizado de GRO. Reconhecendo as restrições orçamentárias, estruturais e de pessoal, é possível propor como solução a criação de um Departamento em uma Diretoria, Centro ou Núcleo especializado no âmbito da MB, com atribuições claramente definidas para:

a) Formular políticas, normas e procedimentos de GRO alinhados às melhores práticas nacionais e internacionais;

b) Realizar estudos técnicos e pesquisas aplicadas, com ênfase nos domínios cibernético, tecnológico e operacional;

c) Apoiar Estados-Maiores, Comandos e OM no desenvolvimento de planos e na gestão dos riscos durante as operações;

d) Supervisionar a implementação da GRO em toda a MB, promovendo auditorias e recomendações de boas práticas;

e) Atuar como centro de excelência na formação e capacitação contínua, desde os níveis tático até o estratégico; e

f) Assessorar diretamente a Alta Administração Naval nas decisões que envolvam análise de risco, especialmente nos campos operacional, logístico, estratégico e cibernético.

Adicionalmente, é imprescindível que a MB redefina e atualize o escopo e os objetivos centrais de sua atual Política de GRO, que permanece excessivamente focada nos riscos administrativos, sem refletir de maneira adequada os riscos associados às operações navais, à segurança das plataformas, à prontidão dos

sistemas de armas, e, particularmente, aos riscos cibernéticos operacionais, cada vez mais críticos nas operações modernas.

É necessário que a MB avance para uma mudança de paradigma, na qual a gestão do risco não seja percebida apenas como ferramenta de conformidade administrativa, mas sim como uma ferramenta de apoio a decisão essencial para a proteção da vida, a preservação dos meios, a integridade dos sistemas críticos e, sobretudo, para a maximização da eficácia e da superioridade operacional da Força, como é feito pela USNAVY.

Para isso, sugere-se incorporar às normas e doutrinas da MB que o risco está presente em toda a cadeia de valor, abrangendo:

a) Operações Navais, Aeronavais e de Fuzileiros Navais;

b) Operações cibernéticas, tanto defensivas quanto ofensivas;

c) Processos de comando, controle, comunicações, computadores, inteligência, vigilância e reconhecimento (C4ISR);

d) Treinamentos, adestramentos, certificações e exercícios;

e) Atividades administrativas, logísticas e de manutenção; e

f) Processos relacionados à cadeia de suprimentos físicos e digitais.

Nesse sentido, sugere-se que a definição de risco operacional, atualmente restrita, seja expandida com base em práticas de referência como as do NIST e da própria USNAVY. Dessa forma, neste trabalho propõe-se a seguinte definição genérica para o risco operacional, a qual também abrange o risco cibernético operacional:

> Risco operacional é a probabilidade de ocorrência de um evento, associado à vulnerabilidade de pessoas, processos, tecnologias ou às ameaças externas, que possa comprometer total ou parcialmente a missão, a capacidade operacional, os meios, as informações críticas ou a vida humana, em especial nos ambientes operacional, logístico, administrativo e cibernético.

Essa definição abrange ameaças externas — como ataques cibernéticos, sabotagens, crises geopolíticas e eventos climáticos extremos — e vulnerabilidades internas — como falhas humanas, falta de treinamento, erros de processos, deficiências tecnológicas e obsolescência.

Portanto, ao adotar essa abordagem, a MB se alinha às melhores práticas internacionais e fortalece sua capacidade de antecipar, avaliar, mitigar e tratar os riscos de forma proativa e consistente, elevando seus níveis de prontidão operacional, resiliência cibernética, segurança institucional e eficácia no cumprimento das missões atribuídas pelo Estado Brasileiro.

5.2 ASPECTOS RELACIONADOS ÀS PESSOAS

A USNAVY adota uma abordagem na qual as pessoas são reconhecidas simultaneamente como o principal ativo da organização e como um dos mais relevantes vetores de risco, seja no ambiente físico, operacional ou cibernético. Essa visão é absolutamente estratégica, pois reconhece o papel central do fator humano na geração, condução, mitigação e resposta aos riscos. Esse entendimento fundamenta a construção de uma cultura institucional de risco, na qual o indivíduo, independentemente de sua função, patente ou graduação, assume o protagonismo na preservação da segurança, da prontidão operacional e da eficácia da missão (USA, 2018).

Essa cultura na USNAVY não é construída de forma reativa ou eventual, mas sim como resultado de um processo estruturado, permanente e transversal de capacitação, sensibilização, treinamento e desenvolvimento de competências, desde o ingresso do militar, civil ou contratado, até sua desvinculação da Força, seja por reserva, aposentadoria ou encerramento contratual.

Atualmente, a MB adota uma abordagem ainda restritiva, na qual os processos de capacitação em gestão de riscos são majoritariamente direcionados aos profissionais diretamente vinculados às atividades administrativas de gestão, especialmente no nível de governança e controle interno. Essa limitação exclui uma parcela significativa do efetivo, particularmente os envolvidos nas atividades operativas, nos ambientes cibernéticos, nas forças de superfície, submarinas, de fuzileiros navais e de apoio logístico.

Diante desse cenário, torna-se imprescindível adotar uma mudança de paradigma, em que a capacitação em GRO não seja percebida como uma atividade de nicho, mas sim como um pilar fundamental da formação e desenvolvimento profissional de todos os integrantes da MB, abrangendo:

a) Oficiais e praças de todos os corpos e quadros;

b) Servidores civis de carreira ou contratados;

c) Militares temporários e prestadores de serviço; e

d) Fornecedores e parceiros envolvidos em atividades sensíveis.

Assim como na USNAVY, a MB deve tornar essa capacitação obrigatória, contínua e progressiva, estruturada por níveis hierárquicos e funções operacionais. Recomenda-se que o conteúdo aborde não apenas conceitos teóricos de risco, mas também aspectos práticos, estudos de caso, análises de acidentes, incidentes e falhas operacionais, bem como simulações e exercícios que permitam consolidar as competências necessárias à gestão dos riscos.

De acordo com o observado na USNAVY, a cultura de risco deve ser incorporada como valor organizacional, extrapolando os limites do ambiente profissional para também orientar comportamentos no cotidiano dos integrantes da Força. Essa estratégia impacta diretamente na preservação da força de trabalho, na redução de acidentes e afastamentos, na melhoria da saúde mental e física dos militares e servidores, bem como no fortalecimento da coesão organizacional.

Outro elemento crítico observado na USNAVY, que deve ser incorporado pela MB, é a descentralização da tomada de decisão sobre risco, especialmente no contexto operacional, conforme indica o OPNAVINST 3500.39C em um de seus princípios “*Make Risk Decisions at the Right Level*” (USA, 2018, Anexo 1, p. 3). Isso significa atribuir responsabilidades aos responsáveis diretos pelas atividades — sejam comandantes de navios, oficiais de operações, chefes de divisão ou gestores de sistemas cibernéticos — a adotar medidas de controle, mitigação, aceitação ou comunicação dos riscos, desde que dentro de parâmetros e limites formalizados, estabelecidos em normas, manuais operacionais e diretrizes específicas em suas áreas de atuação.

Esse modelo descentralizado é fundamental para operações em ambientes dinâmicos como cenários de guerra cibernética ou situações de resposta rápida, nos quais as decisões não podem depender exclusivamente de escalões superiores, sob pena de comprometer a prontidão, a segurança e a eficácia da missão.

Para viabilizar essa transformação, recomenda-se que a MB desenvolva e implemente um Programa Estruturado de Capacitação em Gestão de Risco Operacional, que contemple:

a) Cursos modulares diferenciados por nível hierárquico e função, aplicáveis desde a formação básica até os cursos de aperfeiçoamento, altos estudos e especializações;

b) Certificação periódica, assegurando que os conhecimentos sejam atualizados e revisados conforme a evolução dos cenários operacionais, cibernéticos e tecnológicos;

c) Simuladores e exercícios práticos específicos, com cenários que envolvam análise, tratamento e tomada de decisão sobre riscos operacionais e cibernéticos;

d) Criação de um Sistema de Lições Aprendidas, que permita o compartilhamento sistemático de boas práticas, incidentes, falhas e sucessos relacionados à gestão de risco nas diversas esferas da atuação naval; e

e) Inserção de conteúdos sobre cultura de segurança, fatores humanos, resiliência e segurança cibernética.

A execução dessas iniciativas deve estar sob responsabilidade do Sistema de Ensino Naval (SEN), em estreita articulação com as Diretorias Especializadas, os Comandos Operacionais e as OM responsáveis pelos sistemas de comando, controle, segurança cibernética e operações. Esse alinhamento garante coerência metodológica e aderência às necessidades operacionais da Força.

Por fim, a consolidação de uma cultura robusta e institucionalizada de gestão de risco, centrada no elemento humano, será decisiva para elevar os níveis de prontidão, resiliência, segurança e eficácia operacional da MB, especialmente em face dos desafios impostos pelos ambientes operacionais complexos e dinâmicos que caracterizam o presente e, sobretudo, o futuro do Poder Naval.

5.3 ASPECTOS RELACIONADOS AOS PROCESSOS

Tanto a USNAVY quanto a MB seguem diretrizes próprias, alinhadas a marcos regulatórios de órgãos superiores, como o *Department of Defense* (DoD) e o Ministério da Defesa (MD), respectivamente. Contudo, evidencia-se que a MB carece de uma norma específica e atualizada, que discipline institucionalmente a Gestão do Risco Operacional (GRO), aplicável a todos os ambientes — administrativo, operacional, logístico e cibernético.

A ausência dessa norma representa uma fragilidade institucional, pois, sem uma diretriz normativa, as práticas de gestão de risco na MB permanecem fragmentadas, pouco padronizadas e, como pesquisado, restritas a setores administrativos.

Diante desse cenário, sugere-se a elaboração e promulgação de uma Norma Geral de Gestão do Risco Operacional da MB, que consolide os princípios,

fundamentos e procedimentos aplicáveis, e que também estabeleça um ciclo de revisão sistemático e periódico, assegurando sua permanente aderência às rápidas transformações tecnológicas, às ameaças emergentes — em especial no domínio cibernético — e às exigências operacionais decorrentes do emprego do Poder Naval.

Inspirada na doutrina e nas melhores práticas da USNAVY, essa norma deve explicitar a obrigatoriedade da GRO não apenas no âmbito interno da MB, mas também como requisito contratual, vinculando fornecedores, empresas parceiras e toda a cadeia de suprimentos, especialmente no que diz respeito à segurança cibernética de todos os tipos de ativos computacionais, sejam eles administrativos ou operativos, e à proteção de infraestruturas críticas. Esta abordagem é alinhada aos princípios da Gestão de Riscos da Cadeia de Suprimentos Cibernéticos[14], prática já consolidada no contexto da defesa norte-americana.

Adicionalmente, é imprescindível que a MB promova a construção de uma cultura organizacional de prevenção, resiliência, gestão proativa e melhoria contínua, na qual todas as decisões — operacionais, logísticas, tecnológicas e administrativas — estejam fundamentadas em análises formais de risco, devidamente documentadas por meio de relatórios técnicos padronizados. Esses relatórios não devem se restringir ao ambiente interno das OM, mas constituir um banco de dados institucional, fomentando a memória organizacional e a disseminação de boas práticas no âmbito da Força.

Conforme evidenciado na prática da USNAVY, os quatro pilares fundamentais da GRO — liderança, treinamento, avaliação e recursos — devem ser formalizados como elementos doutrinários estruturantes, vinculando diretamente os Comandantes, Diretores, Chefes de OM e líderes operacionais à responsabilidade indelegável pela implementação, supervisão e avaliação da gestão de risco em suas áreas de competência, não apenas no âmbito administrativo ou na Aviação Naval, conforme observado na MB, quanto também nas esferas operacional e cibernética.

No mesmo sentido, recomenda-se a implantação de um Programa de Certificação em GRO, com renovação periódica. Tal programa deve prever critérios objetivos de qualificação, que influenciem nas avaliações funcionais e na habilitação para funções sensíveis ou de comando, controle e decisão, por exemplo. A ausência

---

[14] Gerenciamento de Riscos da Cadeia de Suprimentos (SCRM) é o processo de identificar e resolver vulnerabilidades potenciais na cadeia de suprimentos de uma empresa. O SCRM tem como objetivo minimizar o impacto desses riscos nas operações, reputação e desempenho financeiro da empresa.

dessa qualificação poderá ser considerada fator limitante para o exercício de determinadas funções críticas, dado que falhas no processo de gestão de risco podem gerar consequências operacionais, materiais e humanas irreparáveis.

Observa-se na USNAVY uma preocupação constante e estruturada com a alocação de recursos específicos — humanos, financeiros, tecnológicos e logísticos — para sustentar o ciclo da GRO, o que deve ser replicado, na medida do possível, pela MB. Entretanto, destaca-se que diversas melhorias podem ser implementadas sem custos financeiros, dependendo apenas de ajustes normativos, revisões processuais, readequações de procedimentos internos e otimização dos recursos já existentes.

Outro avanço essencial é a adoção dos três níveis de decisão — Detalhado, Deliberado e Crítico —, já aplicados na Aviação Naval da MB e na USNAVY, incorporando o fator tempo como variável determinante. Dessa forma, é providenciada uma resposta proporcional à urgência, à complexidade e à criticidade do risco envolvido. Tal abordagem aumenta significativamente a flexibilidade, a acurácia e a eficácia das decisões operacionais, especialmente em contextos como operações de guerra naval ou cibernética, cujo tempo de resposta é crítico.

Outra dimensão crítica se refere à gestão de risco aplicada a aquisições, contratos e desenvolvimento de sistemas. A MB necessita adotar uma abordagem proativa de proteção cibernética e de integridade dos sistemas críticos, por meio da inserção obrigatória de cláusulas contratuais que imponham aos fornecedores padrões mínimos de segurança, governança de risco e conformidade com as normas da Força. Esses contratos devem prever:

a) Requisitos de segurança cibernética durante todo o ciclo de vida do produto ou serviço;

b) Planos de mitigação de riscos específicos;

c) Auditorias periódicas e avaliações de conformidade;

d) Reporte de incidentes, vulnerabilidades e não conformidades; e

e) Mecanismos de resposta e contingência compartilhados com a MB.

Adicionalmente, a MB deve implementar um Sistema de Monitoramento da Performance dos Fornecedores que contemple critérios de eficiência administrativa e, sobretudo, parâmetros de segurança operacional, resiliência cibernética, conformidade normativa e aderência às práticas de GRO. Com a crescente incorporação de tecnologias digitais, inteligência artificial, sistemas autônomos e

redes interconectadas nas operações navais, essa medida deixa de ser uma recomendação e passa a ser uma necessidade crítica para a preservação da prontidão e da superioridade operacional da Força.

Tanto a USNAVY quanto a MB se utilizam de *frameworks* de segurança cibernética[15], como o NIST e a ABNT, respectivamente. Recomenda-se uma estratégia que preveja a integração e a interoperabilidade entre ambos, de forma a aumentar a robustez das operações cibernéticas e facilitar a atuação em coalizões e operações conjuntas.

Finalmente, torna-se imprescindível a criação de um Sistema Informatizado de Gestão de Riscos Operacionais da MB, que permita:

a) Registro estruturado de todos os riscos identificados nas OM;

b) Classificação por criticidade, impacto e probabilidade;

c) Escalonamento automático dos riscos para níveis superiores de decisão;

d) Acompanhamento do status dos planos de tratamento, mitigação ou aceitação dos riscos;

e) Geração de relatórios analíticos, *dashboards*[16] e indicadores estratégicos e

f) Compartilhamento seguro de dados, lições aprendidas e melhores práticas entre OM, Comandos, Diretorias e Estados-Maiores.

Esse sistema fortalecerá a memória organizacional e servirá como instrumento de gestão estratégica permitindo à MB antecipar riscos, reduzir incertezas, otimizar a tomada de decisão e elevar sua capacidade de adaptação em face das ameaças, especialmente aquelas oriundas do ambiente cibernético.

5.4 ASPECTOS RELACIONADOS ÀS TECNOLOGIAS

No âmbito tecnológico, a análise evidencia uma lacuna significativa da MB no que se refere à aplicação efetiva e abrangente da GRO aos sistemas de armas, sensores, redes de comando e controle, plataformas de combate e às infraestruturas críticas embarcadas e terrestres. Tais ativos permanecem, em grande parte, fora do escopo das práticas atuais de GRO na MB, que ainda se concentram

---

[15] *Framework* de segurança cibernética – é uma estrutura que fornece diretrizes e práticas recomendadas para gerenciar e reduzir o risco de ataques cibernéticos. Ela oferece um roteiro para avaliar, monitorar e mitigar ameaças potenciais, ajudando as organizações a proteger seus sistemas, dados e operações.

[16] *Dashboard* - também conhecido como painel de controle, é uma interface gráfica que apresenta informações, métricas e indicadores de desempenho de forma organizada e de fácil compreensão.

predominantemente nos Sistemas Digitais Administrativos (SDA), relegando a segundo plano os Sistemas Digitais Operativos (SDO), cuja criticidade é significativamente maior, especialmente em cenários nos quais estão sendo cada vez mais empregados, como é o caso da MB. Essa lacuna expõe a Força a riscos operacionais, cibernéticos e estratégicos relevantes, uma vez que esses sistemas são, por definição, alvos prioritários em cenários de guerra cibernética, sabotagem, guerra eletrônica e ataques híbridos.

Em contraste, a USNAVY adota uma abordagem holística e integrada, considerando de forma indissociável tanto a Tecnologia da Informação (TI) — voltada ao apoio administrativo, logístico e de gestão — quanto a Tecnologia Operacional (TO) — que abrange sistemas de armas, plataformas navais, sistemas de sensores, combate, comando e controle, além das infraestruturas críticas de apoio às operações. Esse modelo assegura que os riscos sejam identificados, avaliados, mitigados e monitorados de maneira transversal e contínua, tanto nos ambientes administrativos quanto, principalmente, nos ambientes operacionais e cibernéticos.

Diante desse cenário, torna-se imprescindível que a MB reconheça formalmente em suas normas que as ferramentas e metodologias de GRO não devem se restringir ao campo administrativo, mas devem ser tratadas como instrumentos estratégicos de apoio à decisão operacional. Isso implica integrá-las diretamente ao processo decisório nos níveis tático, operacional e estratégico, ampliando seu emprego para as áreas de operações, engenharia, manutenção, logística, guerra cibernética e suporte ao combate.

Faz-se necessária, também, a incorporação imediata de ferramentas, metodologias e sistemas de apoio à decisão. A USNAVY já adota esse modelo, conforme detalhado no Quadro 3 do Apêndice A. Isso inclui:

a) Programas de modelagem e simulação de riscos operacionais e cibernéticos;

b) Sistemas de gerenciamento de vulnerabilidades em infraestruturas críticas, redes operacionais e sistemas de armas;

c) Ferramentas de avaliação quantitativa e qualitativa de riscos, utilizando inteligência artificial, *machine learning*[17] e *big data analytics*[18] para predição de falhas e incidentes;

d) Sistemas integrados de monitoramento contínuo de riscos, aderentes aos princípios de Consciência Situacional Cibernética; e

e) *Frameworks* especializados, como o NIST *Cybersecurity Framework* (CSF)[19], aplicados diretamente a ambientes operacionais, não restritos ao contexto administrativo.

No campo das metodologias, destaca-se a importância do uso estruturado da técnica de *Brainstorming*, amplamente adotada tanto pela USNAVY quanto, pontualmente, pela MB. Quando aplicada de forma metodológica e com rigor técnico, essa metodologia se constitui como uma ferramenta fundamental em todas as fases da GRO, desde a identificação dos riscos, análise, avaliação, tratamento, até sua supervisão e comunicação. Sua eficácia reside na capacidade de:

a) Estimular a colaboração multidisciplinar;

b) Promover a integração de diferentes níveis hierárquicos e especialidades;

c) Fomentar a criatividade na identificação de ameaças não convencionais e riscos emergentes, especialmente no domínio cibernético e nas operações em ambientes contestados; e

d) Possuir custo próximo de zero para ser implementada.

Importante observar que, na USNAVY, o emprego da técnica de *Brainstorming* e de outras metodologias colaborativas ocorre dentro de um ambiente institucional que estimula formalmente a inovação, a pesquisa aplicada, o desenvolvimento de novas soluções e a adaptação constante das ferramentas de GRO às mudanças do ambiente operacional e tecnológico. Esse ambiente de inovação é, no entanto, ainda pouco desenvolvido na MB, carecendo de fomento a evolução contínua dos instrumentos de gestão de risco.

Adicionalmente, a análise documental revela que a MB ainda opera com múltiplos modelos de matrizes de risco, sem critérios de padronização formalizados.

---

[17] *Machine learning* – é um ramo da inteligência artificial que se concentra no desenvolvimento de algoritmos que permitam os sistemas aprender com os dados apresentados sem programação prévia.

[18] *Big data analytics* – é um processo em que é realizada a análise de grandes volumes de dados a fim de se descobrir padrões, correlações e tendências, por exemplo.

[19] NIST *Cybersecurity Framework* (CSF) – é um conjunto de diretrizes e práticas recomendadas para ajudar organizações a gerenciar e reduzir riscos de segurança cibernética.

Tal condição compromete a consistência das avaliações, assim como impacta negativamente na comparabilidade dos dados, na confiabilidade das análises e, consequentemente, na qualidade da tomada de decisão. Este é um fator crítico, especialmente quando se trata de riscos associados a sistemas tecnológicos, nas quais as interdependências são complexas e os efeitos cascata são imprevisíveis.

A padronização das matrizes de risco, devidamente calibradas e ajustadas à realidade operacional e tecnológica da MB, representa, portanto, uma medida essencial e inadiável. Essa padronização deve contemplar:

a) Critérios objetivos e escaláveis de impacto, probabilidade e severidade;

b) Parâmetros específicos para riscos cibernéticos, tecnológicos e operacionais, distintos dos riscos administrativos tradicionais;

c) Modelagem de cenários específicos para ambientes navais, de guerra cibernética, de operações anfíbias, aeronaval e submarina; e

d) Integração de critérios de segurança física, lógica, ambiental, de continuidade operacional e resiliência cibernética.

Outro elemento essencial é a adoção de processos automatizados de gestão de risco tecnológico, por meio de sistemas informatizados, *dashboards* e plataformas de *Business Intelligence* (BI)[20], que possibilitem aos comandantes, chefes de OM e Estados-Maiores o monitoramento em tempo real da exposição a riscos operacionais e cibernéticos, além da geração de alertas, relatórios executivos e planos de resposta contingencial.

Dessa forma, além de atender a um requisito normativo e às boas práticas, a gestão do risco tecnológico torna-se essencial. Em especial, a gestão do risco cibernético passa a ser um elemento central no ciclo de planejamento, execução, monitoramento e avaliação das operações navais e cibernéticas.

Por fim, deve-se destacar que a adoção plena e transversal da GRO aplicada às tecnologias é uma condição *sine qua non* para a preservação da prontidão operacional, da superioridade tecnológica e da resiliência cibernética da MB no século XXI. Sem essa transformação, a Força permanecerá vulnerável, tanto aos riscos tradicionais quanto, sobretudo, às ameaças emergentes do ambiente cibernético e das operações multidomínio, as quais são altamente dependentes de tecnologia,

---

[20] *Business Intelligence* (BI) - é um conjunto de estratégias, processos, tecnologias e aplicações que visam transformar dados brutos em informações significativas e acionáveis para apoiar a tomada de decisões estratégicas e operacionais em uma empresa.

comprometendo sua capacidade de cumprir com eficácia as atribuições que lhe são conferidas pela Estratégia Nacional de Defesa e pelos objetivos estratégicos do Estado brasileiro.

5.5 ASPECTOS RELACIONADOS AOS EVENTOS EXTERNOS

É indispensável que a MB avance na formalização dos riscos operacionais aos seus processos de planejamento, decisão e execução em seus contextos estratégico, operacional e tático. Embora haja um reconhecimento da existência de riscos externos — como ataques cibernéticos, sabotagem, degradação de sistemas críticos, interferências eletromagnéticas e ameaças físicas —, observa-se uma lacuna nas normas quanto a sua efetiva incorporação ao ciclo da GRO.

Atualmente, um dos exemplos mais evidentes dessa limitação é a insuficiente consideração das vulnerabilidades associadas à cadeia de suprimentos, tanto física quanto digital (Gestão de Riscos da Cadeia de Suprimentos Cibernéticos). Esse vetor representa, na atualidade, uma das principais superfícies de ataque para atores hostis, sejam eles estatais ou não estatais. A não inclusão dessas ameaças compromete a segurança cibernética, a disponibilidade e a resiliência das capacidades operacionais da MB, especialmente em cenários que dependam de alta complexidade tecnológica.

A experiência da USNAVY evidencia que tais riscos — embora muitas vezes classificados como imprevisíveis, incontroláveis ou de difícil mensuração — devem ser abordados desde as fases iniciais do planejamento operacional (USA, 2018). Na MB, está previsto um anexo de Defesa Cibernética a documentos de operações conjuntas, porém nenhum documento que trate de gestão de riscos menciona este tipo de anexo.

Diante desse cenário, torna-se essencial que a MB passe a considerar de maneira estruturada, no escopo dos processos de GRO, uma gama abrangente de eventos externos, incluindo, mas não se limitando a:

a) Ameaças cibernéticas de origem externa, como malware direcionado, *ransomware*[21] contra sistemas embarcados, ataques de negação de serviço contra redes críticas, exploração de vulnerabilidades em sistemas de armas e plataformas;

---

[21] *Ransomware* - é um tipo de software malicioso (malware) que impede o acesso a arquivos, sistemas ou redes de computador, criptografando-os e exigindo o pagamento de um resgate para que o acesso seja restaurado.

b) Ameaças híbridas, combinando ações cibernéticas, informacionais, eletrônicas, psicológicas e físicas, com impactos diretos sobre sistemas de comando e controle, sensores e redes logísticas;

c) Interferências nas cadeias de suprimento, tanto materiais (sobretudo microeletrônica, sobressalentes críticos e combustíveis) quanto digitais (*software*, *firmware*, atualizações de sistemas e dependências tecnológicas externas);

d) Falhas ou degradações em sistemas de navegação, comunicações e geolocalização, especialmente oriundas de interferências eletromagnéticas, *spoofing*[22] ou *jamming*[23] de sinais GNSS (*Global Navigation Satellite Systems*);

e) Eventos climáticos extremos, como tempestades, ciclones, ondas de calor, que impactam tanto a segurança das operações quanto a integridade de infraestruturas terrestres e embarcadas;

f) Desastres naturais, como terremotos, tsunamis ou enchentes, que afetam bases navais, arsenais, centros de comando e redes de apoio logístico;

g) Crises sanitárias e pandemias, que reduzem a prontidão operacional por meio do impacto sobre o efetivo, as cadeias de suprimento e as capacidades hospitalares e de suporte biomédico;

h) Crises geopolíticas, bloqueios marítimos, embargos, sanções e outros eventos que impactem direta ou indiretamente o fluxo de suprimentos, o acesso a tecnologias críticas ou a liberdade de navegação; e

i) Ameaças aos sistemas de energia e infraestrutura crítica, especialmente considerando a crescente interdependência entre os sistemas da MB e os provedores externos de energia, telecomunicações, dados e logística.

Além disso, o conceito de risco externo deve ser expandido para incorporar, formalmente, os fatores socioambientais e psicossociais, atualmente abordados apenas na Aviação Naval na MB. Esses fatores, muitas vezes subestimados, impactam diretamente sobre a prontidão operacional, a capacidade de sustentação de campanhas e a resiliência da Força. Nesse contexto, incluem-se:

a) Riscos à saúde física e mental do efetivo, agravados por jornadas prolongadas, isolamento operacional, estresse extremo e fadiga operacional.;

---

[22] *Spoofing* – é a prática de mascarar ou falsificar informações de identificação para parecer uma entidade confiável ou legítima com o objetivo de enganar a vítima e obter acesso a informações confidenciais, dinheiro, ou para espalhar malware.

[23] Jamming – refere-se a interferência ou bloqueio deliberado de sinais de comunicação.

b) Riscos ao bem-estar social e familiar, que impactam diretamente os níveis de moral, coesão e desempenho das tripulações; e

c) Ameaças à segurança ambiental, sobretudo em operações em ambientes contaminados, zonas de guerra química, biológica, radiológica e nuclear (QBRN) ou áreas com desastres industriais.

A formalização e a integração desses entendimentos no ciclo de GRO da MB não representam apenas uma evolução metodológica, mas uma necessidade imprescindível frente aos desafios impostos pelos cenários contemporâneos de guerra multidomínio e conflitos de alta contestação, nos quais o espaço cibernético, o espectro eletromagnético, as infraestruturas críticas e os ambientes logísticos passaram a ser, eles próprios, teatros de operações.

Portanto, incorporar esses aspectos no processo decisório da MB permitirá não apenas aprimorar sua capacidade de antecipação, adaptação e resiliência, mas, sobretudo, fortalecerá sua aptidão para operar de forma segura, eficaz e sustentável em ambientes operacionais caracterizados pela incerteza, volatilidade, complexidade e ambiguidade — atributos indissociáveis dos cenários estratégicos atuais e futuros.

5.6 CONSIDERAÇÕES PARCIAIS

As análises realizadas neste capítulo, observadas pelos aspectos de generalidades, pessoas, processos, tecnologias e eventos externos, evidenciam que a Marinha do Brasil (MB) necessita evoluir significativamente na implementação de uma Gestão do Risco Operacional (GRO), especialmente no que se refere ao risco cibernético operacional, foco deste trabalho.

No aspecto das generalidades, destaca-se a necessidade de criar uma estrutura especializada nos moldes do *Naval Safety Command* da Marinha dos Estados Unidos da América (USNAVY), ou, no mínimo, um Departamento com esta função em alguma Organização Militar (OM) da MB, capaz de institucionalizar a GRO como elemento central da doutrina, do treinamento e do apoio à decisão. Atualmente a MB ainda concentra esforços em abordagens restritas, fortemente voltadas ao ambiente administrativo.

No aspecto das pessoas, fica evidente a abordagem restrita adotada pela MB, limitando o conhecimento em GRO ao ambiente administrativo, a exceção da Aviação Naval, que possui visão operacional, porém, específica sobre o assunto. A necessidade de incorporar o risco cibernético ao ciclo decisório, bem como de

expandir a capacitação do pessoal, em todos os níveis hierárquicos, incluídos os contratados e os fornecedores, aparece como ponto central, adotando programas permanentes, estruturados e certificados, alinhados às práticas operacionais e cibernéticas na Força.

Quanto aos processos, a inexistência de uma norma específica sobre o assunto que seja abrangente a todos os setores da MB compromete a padronização e a efetividade da GRO. Sugere-se que esta norma seja mandatória não apenas internamente, mas também aplicada às instituições participantes da cadeia de suprimentos, contemplando cláusulas contratuais voltadas à segurança cibernética e à integridade dos sistemas.

Quanto às tecnologias, verifica-se uma lacuna crítica na aplicação da GRO aos Sistemas Digitais Operativos (SDO), plataformas, sistemas de armas e infraestruturas críticas de interesse da MB. A Força necessita incorporar ferramentas de gestão de vulnerabilidades, monitoramento contínuo, com possibilidades de emprego de inteligência artificial e automação, garantindo consciência situacional cibernética em tempo real.

Quanto aos aspectos dos eventos externos, torna-se indispensável incorporar ao ciclo de GRO riscos decorrentes de ameaças híbridas, falhas na cadeia logística, crises geopolíticas, eventos climáticos extremos, impactos psicossociais sobre o efetivo e os ataques cibernéticos, pois representam um complemento aos elementos que afetam diretamente a prontidão, a resiliência e a eficácia operacional da Força.

Finalmente, as propostas estruturadas nos quatro aspectos da pesquisa — pessoas, processos, tecnologias e eventos externos — além das generalidades apresentadas, revelam que a transformação da GRO na MB não é apenas desejável, mas imprescindível. A ausência de uma visão integrada dos riscos, particularmente daqueles associados às tecnologias operacionais, sistemas críticos e cadeias de suprimento cibernético, compromete diretamente a prontidão e a resiliência da Força, impactando na capacidade da MB operar em cenários caracterizados por elevada complexidade, volatilidade e multidomínio, elementos cada vez mais presentes nas operações contemporâneas.

No próximo capítulo, será concluída a pesquisa com a apresentação das considerações finais sobre o trabalho realizado.

6 CONSIDERAÇÕES FINAIS

Neste trabalho teve-se como objetivo central analisar e propor melhorias para a Gestão do Risco Operacional (GRO) na Marinha do Brasil (MB), com ênfase no risco cibernético operacional, a partir de uma abordagem comparativa entre o modelo adotado pela Marinha dos Estados Unidos da América (USNAVY) e a MB. Ao longo do desenvolvimento dos capítulos, foi possível compreender os conceitos fundamentais que embasam a gestão de riscos, assim como mapear as fragilidades, os desafios e as oportunidades de evolução da MB ante as demandas contemporâneas de segurança, prontidão e eficácia operacional, buscando-se, nestas considerações finais, responder às questões de pesquisa das fases investigativa, diagnóstica e propositiva.

Na fase investigativa, a partir da análise teórica inicial, evidenciou-se que o conceito de risco, embora amplamente utilizado, ainda carece de uniformidade conceitual, tanto no meio acadêmico quanto nos ambientes institucionais, inclusive na MB. Essa pluralidade de entendimentos, longe de ser uma fragilidade teórica, reflete a necessidade de que cada organização adapte a definição de risco às suas realidades, objetivos e contextos operacionais. Nesse sentido, o risco cibernético operacional se destaca como uma categoria emergente, particularmente sensível às características das Forças Armadas modernas, cuja crescente dependência de sistemas digitais, sejam eles administrativos ou operativos, plataformas informatizadas e cadeias de suprimento digitalizadas impõe uma nova lógica de vulnerabilidades e ameaças. Identificou-se que o risco cibernético operacional poderia ser analisado sob a ótica dos aspectos de pessoas, processos, tecnologia e eventos externos, conforme taxonomia identificada na pesquisa.

Ao estudar a doutrina da USNAVY, especialmente por meio da norma OPNAVINST 3500.39D e do seu Manual de Segurança Cibernética, constatou-se a existência de uma estrutura doutrinária robusta, abrangente e plenamente operacionalizada. Naquela Marinha, a GRO é mais do que uma prática administrativa; trata-se de uma cultura institucional, incorporada aos processos decisórios, aos treinamentos, à condução das missões e ao desenvolvimento de projetos. A gestão de riscos é aplicada não apenas aos Sistemas Digitais Administrativos (SDA), mas de forma inequívoca aos Sistemas Digitais Operativos (SDO), aos sistemas de armas, às plataformas navais, aos sensores, aos sistemas de comando e controle (C2) e, de

maneira destacada, à proteção da cadeia de suprimentos, inclusive sob a ótica da segurança cibernética.

Na USNAVY, o risco é tratado como uma variável decisiva para o sucesso ou fracasso da missão. Sua gestão segue uma metodologia estruturada em quatro pilares — liderança, treinamento, avaliação e recursos —, complementada por três níveis de decisão, que consideram, como variável crítica, o tempo disponível para a tomada de decisão. Essa abordagem permite que o gerenciamento de riscos se adapte desde situações de planejamento de longo prazo até momentos de decisão sob pressão operacional.

Em contrapartida, na fase diagnóstica, foi revelado que a MB adota uma abordagem fragmentada e excessivamente voltada ao ambiente administrativo. Sua gestão de riscos é guiada, majoritariamente, por normas alinhadas à ISO 31000, com forte viés burocrático, e carece de uma aplicação sistemática nos ambientes operacionais e no domínio cibernético. A exceção identificada encontra-se na Aviação Naval, que possui práticas alinhadas, em alguma medida, à doutrina norte-americana, ainda que restritas ao escopo específico da atividade aeronaval.

Atualmente, a MB não dispõe de uma norma abrangente sobre GRO. O que se verifica é a existência de normas dispersas — como a ARMADAINST nº 32-1, a SGM-107 e a DGMM-3010 — que, embora tratem do tema risco, fazem-no de forma fragmentada, limitando sua eficácia como ferramenta de apoio à decisão no ambiente operacional. Adicionalmente, as políticas de gestão de risco na MB estão centradas na segurança da informação dos Sistemas Digitais Administrativos (SDA), negligenciando por completo os Sistemas Digitais Operativos (SDO) e as infraestruturas críticas embarcadas e de terra.

Essa lacuna se torna ainda mais crítica no contexto do risco cibernético operacional. A análise demonstrou que, enquanto a USNAVY trata o risco cibernético como uma extensão natural do risco operacional, a MB ainda não incorporou, formalmente, esse entendimento. As ameaças cibernéticas, as falhas na cadeia logística digital, os impactos decorrentes de ataques cibernéticos aos sistemas de armas, sensores, redes de comando e controle, permanecem à margem do ciclo de gestão de riscos da Força.

Dessa forma, na fase propositiva, as propostas desenvolvidas ao longo deste trabalho apontaram para a necessidade de uma transformação estrutural no modelo de GRO da MB, oferecendo como contribuições relevantes para o aprimoramento da

doutrina e dos processos da MB, especialmente no que se refere aos riscos cibernéticos operacionais os seguintes pontos: a proposta de uma nova definição do risco operacional, conforme a pesquisa realizada e que compreenda os ambientes operacional, logístico e cibernético, além do administrativo; a adoção do conceito de risco cibernético operacional como uma especialização do risco operacional; a elaboração de uma Norma Geral de Gestão do Risco Operacional da MB, que consolide os princípios, fundamentos e procedimentos aplicáveis; e a adoção de uma metodologia baseada nos quatro aspectos do risco operacional, conforme definidos pelo Comitê da Basileia (pessoas, processos, tecnologia e eventos externos).

A transformação proposta poderia iniciar-se pela criação de uma estrutura organizacional especializada, nos moldes do *Naval Safety Command* da USNAVY, ou, no mínimo, por meio da criação de um Departamento ou Núcleo de GRO em uma Organização Militar (OM) de referência. Tal estrutura deveria ser responsável pela formulação, implantação, supervisão e avaliação contínua da política de GRO na MB. Além disso, é necessário que a MB desenvolva uma norma específica e abrangente de GRO, aplicável a todas as OM e a todos os níveis hierárquicos. Essa norma deveria ser mandatória tanto internamente à MB quanto externamente, sendo estendida aos fornecedores, contratados e parceiros da cadeia de suprimentos, inclusive incorporando cláusulas contratuais relativas à segurança cibernética e à integridade dos sistemas críticos.

No que diz respeito aos aspectos da taxonomia dos riscos cibernéticos operacionais, primeiramente quanto ao aspecto relacionado às pessoas, torna-se necessário implementar programas permanentes de capacitação, certificação e reciclagem em GRO, abrangendo desde os níveis operacionais até os estratégicos, contemplando não apenas militares e servidores civis em todos os seus níveis hierárquicos, mas também empresas contratadas e terceiros que tenham interface com sistemas ou informações sensíveis. A disseminação da cultura de risco, com enfoque na prevenção, na resiliência e na capacidade adaptativa, deve ser institucionalizada como valor fundamental da MB.

No campo dos processos, a gestão do risco deveria ser integrada desde a fase inicial de qualquer projeto, operação ou aquisição, abrangendo todo o ciclo de vida dos sistemas, desde a concepção até o descomissionamento. A adoção dos três níveis de decisão (Detalhado, Deliberado e Crítico), bem como a incorporação do tempo como variável decisiva e os quatro pilares (liderança, treinamento, avaliação e

recursos), da mesma forma como é realizado na USNAVY, deveria ser formalizada como uma doutrina operacional abrangente na MB, a ser formalizada pelo Estado-Maior da Armada (EMA). Também foi identificada a necessidade de se propor um modelo de GRO que não se limite ao ambiente administrativo, mas que se estenda às operações navais, às infraestruturas críticas e às cadeias de suprimento cibernéticas.

Quanto às tecnologias, existe a necessidade de expandir a aplicação da GRO para além dos sistemas administrativos, incluindo os Sistemas Digitais Operativos (SDO), as infraestruturas críticas, os sistemas de armas, sensores, controle de propulsão, navegação, C2 e SCADA. Para isso, recomenda-se a adoção de ferramentas robustas de monitoramento contínuo, análise de vulnerabilidades, gestão de riscos cibernéticos, detecção proativa de anomalias e automação dos processos de segurança, preferencialmente com as tecnologias de ponta disponíveis atualmente tais como a inteligência artificial. A MB deve buscar, inclusive, integrar sua política de GRO com *frameworks* reconhecidos internacionalmente, como o NIST *Risk Management Framework* (RMF), complementando a abordagem da ISO 31000 com práticas mais aderentes ao ambiente operacional militar. Ao longo do trabalho, foi identificada a necessidade de se criar um Sistema de Monitoramento da Performance dos Fornecedores, que contemple critérios para sua eficiência segundo parâmetros de segurança cibernética, além das administrativas, assim como um Sistema Informatizado de Gestão de Riscos Operacionais da MB, em complemento ao Programa Netuno, que possibilite estruturar os dados, classificá-los e gerenciá-los em seus ciclos de tratamento, referente a todos os riscos identificados nas OM.

No tocante aos eventos externos, o ciclo de GRO da MB poderia incorporar, de maneira explícita, riscos associados a ameaças híbridas, interferências na cadeia logística, ataques cibernéticos, falhas em sistemas de geoposicionamento, crises climáticas e impactos psicossociais e de prontidão no efetivo. A integração desses elementos no ciclo de risco permitiria à Força melhorar sua capacidade de resposta e sua resiliência diante de um ambiente operacional caracterizado pela incerteza, pela volatilidade e pela interdependência dos domínios tradicionais (terra, mar, ar e espaço) e o domínio cibernético.

Como sugestões para pesquisas futuras, propõe-se realizar estudos de caso aplicados a Organizações Militares específicas, testando a aplicabilidade das propostas aqui desenvolvidas; expandir a análise comparativa para outras Marinhas

e Forças Armadas, ampliando o *benchmarking*[24] internacional; investigar os impactos econômicos e operacionais decorrentes da adoção ou não de práticas robustas de gestão de risco na MB; desenvolver simulações de cenários operacionais, integrando variáveis de risco cibernético segundo os aspectos observados (pessoas, processos, tecnologias e eventos externos), para validação dos modelos propostos; aprofundar o estudo da GRO no âmbito das operações conjuntas; e sugerir a inclusão da definição de risco operacional no Glossário das Forças Armadas, como forma de consolidar terminologias, doutrinas e práticas de referência no âmbito da Defesa Nacional.

O ambiente operacional contemporâneo, caracterizado pela crescente convergência entre os domínios tradicionais e o cibernético, impõe desafios sem precedentes às Organizações Militares (OM), exigindo respostas estratégicas à altura das ameaças emergentes. Nesse contexto, a segurança das operações navais, das infraestruturas críticas e das cadeias de suprimento revela-se intrinsecamente dependente de uma abordagem integrada, abrangente e sistematizada de GRO, com ênfase no risco cibernético operacional. As análises e evidências apresentadas ao longo desta pesquisa demonstram que a adoção de um modelo de GRO robusto, institucionalizado e transversal deixou de constituir mera recomendação normativa, passando a configurar-se como um requisito estratégico indispensável para a preservação da capacidade operativa, da segurança dos sistemas digitais administrativos e operativos, e da resiliência das infraestruturas críticas.

A adoção das propostas aqui apresentadas representa, portanto, um passo decisivo para consolidar uma MB mais segura, resiliente, eficiente, com uma capacidade cibernética aprimorada e, finalmente, apta a cumprir suas atribuições no século XXI.

---

[24] *Benchmarking* – prática que compara processos ou produtos de uma empresa com os de outras consideradas referências no mercado, com o objetivo de identificar oportunidades de melhoria.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Gestão de riscos — Diretrizes**. ABNT NBR ISO 31000:2018. 2. ed. 2018.

BERNSTEIN, Peter L**. Against the gods: The remarkable story of risk**. 1. ed. EUA. John Wiley & Sons, Inc. 1996.

BIS - BANK OF INTERNATIONAL SETTLEMENTS. **International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version**. 2006. Disponível em: http://www.bis.org/publ/bcbs128.pdf. Acesso em: 27 abr 2025.

BRASIL, Marinha do Brasil. **Portaria Nº 110/EMA, Política de Gestão de Riscos da Marinha do Brasil, de 4 de maio de 2017**. Estado-Maior da Armada, Brasília, DF, 2017a.

BRASIL. Gabinete de Segurança Institucional**. Glossário de Segurança da Informação**. Portaria nº 93, de 26 set. 2019. 2019a.

BRASIL. Marinha do Brasil. Diretoria de Administração da Marinha. Rede de Comunicações Integrada da Marinha (RECIM). **Programa Netuno**. Rio de Janeiro, RJ. 2025. Disponível em: https://netuno.dadm.mb/?q=riscos/. Acessado em: 29 mar. 2025.

BRASIL. Marinha do Brasil. Diretoria-Geral do Material da Marinha. **Manual de segurança da aviação (DGMM-3010).** Rio de Janeiro, RJ. 2023a.

BRASIL. Marinha do Brasil. Diretoria-Geral do Pessoal da Marinha. **Estruturação das áreas de conhecimentos e das habilitações da Marinha (EACH)**. 2019b.

BRASIL. Marinha do Brasil. Diretoria-Geral do Pessoal da Marinha. **Normas de Tecnologia da Informação da Marinha (DGMM-0540)**, 3. rev. 2019c.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **ARMADAINST nº 32-1**. Brasília, DF, 2017b.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Doutrina Cibernética da Marinha (EMA-419)**. Brasília, DF: Marinha do Brasil, 119 p. 2021.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Política Naval (EMA-323)**, 2019d.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Estratégia de Defesa Marítima (EMA-310)**, 1. edição. 2023b.

BRASIL. Marinha do Brasil. **Plano Estratégico da Marinha (PEM 2040)**. Estado-Maior da Armada, Brasília – DF, 2020a.

BRASIL. Marinha do Brasil. Secretaria-Geral da Marinha. **Normas Gerais de Administração (SGM-107)**. Brasília, DF. 2024a.

BRASIL. Ministério da Defesa. Comissão Interescolar de Doutrina de Operações Conjuntas (CIDOC). **Nota escolar nº002/CIDOC/2018, Gerenciamento do risco operacional (GRO) nas operações conjuntas,** 4. ed. 2018a.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas (MD30-M-01), 2º Volume**. Brasília, DF: Ministério da Defesa, 393 p. 2020b.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. 2. ed. Brasília, DF: Ministério da Defesa, 42 p. 2023c.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Glossário das Forças Armadas (MD35-G-01)**. Brasília, DF, 2015.

BRASIL. Ministério da Defesa. Gabinete do Ministro. **Resolução CG-MD nº 3, de 25 de novembro de 2024. Aprova a Política de Gestão de Riscos do Ministério da Defesa – PGR-MD**. 2024b.

BRASIL. Ministério da Defesa. **Portaria nº 3.781/GM, de 17 de novembro de 2020. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências**. 2020c.

BRASIL. Presidência da República. **Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas**. 2018b.

COLEMAN, Rodney. **Operational Risk**. 2011. Disponível em: https://www.researchgate.net/publication/227576075_Operational_Risk. Acesso em: 21 fev. 2025.

DUNLAP, H.; ORTIZ, C. J. **Cyber Supply Chain Risk Management (C-SCRM) a System Security Engineering Role in the Future of Systems Engineering** in INCOSE, Vol 25, Issue 2. 2022.

EMGEPRON. **Ordem do dia nº 1 de 2023**. Disponível em: https://www.marinha.mil.br/emgepron/en/pt-br/41o-aniversario-da-empresa-gerencial-de-projetos-navais-emgepron. Acesso em: 15 mar. 2025.

GHADGE, A. et al**. Managing cyber risk supply chains: A review and research agenda**. Em Supply Chain Management An International Journal. 2019.

GREENBERG, Andy**. Sandworm: Uma nova era na guerra cibernética e a caça pelos hackers mais perigosos do Kremlin**. 1. ed. Rio de Janeiro: Alta Books. 2021.

KOK, A.; MARTINETTI, A; BRAAKSMA, J. **The Impact of Integrating Information Technology With Operational Technology in Physical Assets: A Literature Review**. IEEE Access. v. 12, p. 111832 – 111845, 2024.

LUPTON, Deborah. Risk. 2. ed. Routledge. 2013.

NPS - NAVAL POSTGRADUATE SCHOOL. **Operational Risk Management.** Disponível em: https://nps.edu/web/safety/orm/. Acessado em: 25 abr. 2025.

PERROW, Charles. **Normal Accidents: Living with High-Risk Technologies**. 1. ed. BasicBooks. 1984. Disponível em: https://archive.org/details/normalaccidentsl0000perr/mode/2up/. Acessado em: 25 mar. 2025.

SOFTWARE ENGINEERING INSTITUTE (SEI). **A Taxonomy of Operational Cyber Security Risks Version 2**. 2014. Disponível em: https://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf. Acesso em: 27 abr. 2025.

STRYKER, Cole. **O que é risco operacional?** 23 mai 2024. Disponível em: https://www.ibm.com/br-pt/topics/operational-risk/. Acessado em: 26 mar. 2025.

USA - UNITED STATES OF AMERICA. Department of Defense. **Risk Management Framework for DoD Systems**. 2022a.

USA - UNITED STATES OF AMERICA. Department of the Navy. **Chief Information Officer. Cybersecurity Manual**. 2022b.

USA - UNITED STATES OF AMERICA. Department of the Navy. **Naval Safety Command**. Disponível em: https://navalsafetycommand.navy.mil/. Acesso em: 10 jun. 2025.

USA - UNITED STATES OF AMERICA. Department of the Navy. Office of the Chief of Naval Operations**. OPNAVINST 3500.39D N09F**, 29 Mar 2018. 2000 Navy Pentagon, Washington, DC 20350-2000. 2018.

APÊNDICE A – Quadros Explicativos da Pesquisa

Quadro 1 – Palavras identificadas nas definições de “risco”.

Palavras identificadas nas definições de “risco”	Política de Gestão de Riscos do MD (BRASIL, 2024a)	Glossário das Forças Armadas (BRASIL, 2015)	Glossário de Segurança da Informação (BRASIL, 2019a)	ARMADAINST nº 32-1 (BRASIL, 2017a)	DGMM-3010 (BRASIL, 2023b)	**SGM-107 (BRASIL, 2024b)**
Ameaça					x	x
Consequências					x	
Efeito						x
Evento	x	x	x			
Gravidade		x			x	
Impacto	x		x			x
Incerteza				x		x
Insegurança		x			x	
Objetivo	x		x	x		x
Oportunidade						x
Perigo					x	
Possibilidade	x		x			
Probabilidade	x	x	x		x	x

Fonte: O Autor.

Quadro 2 – Relação entre Ameaças, Vulnerabilidades e Impactos de Incidentes Cibernéticos.

Ameaças Externas	**Vulnerabilidades dos Sistemas/Equipamentos**	**Impactos Potenciais nas Operações Militares**
Ataques cibernéticos (malware, ransomware, phishing)	Sistemas desatualizados, falta de antivírus, falhas de autenticação	Interrupção de comunicações e comando, perda de controle operacional
Ciberespionagem (ex: por Estados ou grupos hostis)	Falta de criptografia, credenciais fracas, políticas de acesso ineficazes	Vazamento de informações estratégicas, comprometimento de missões
Ataques de negação de serviço (DoS/DDoS)	Serviços críticos expostos à Internet sem proteção adequada	Paralisação de sistemas logísticos e administrativos
Sabotagem de programa ou equipamento (ex: backdoors, implantes em firmware)	Aquisição de equipamentos sem inspeção de segurança, falta de validação de integridade	Inutilização ou controle externo de armamentos, sensores, navegação e plataformas
Interferência em sistemas de navegação e posicionamento (GPS spoofing/jamming)	Ausência de redundância em sistemas de navegação, dependência exclusiva de GNSS	Desorientação de tropas e vetores, falha na execução de rotas e alvos
Intrusão em redes de controle (SCADA, ICS, C2)	Redes sem segmentação, ausência de monitoramento contínuo	Comprometimento de instalações de infraestruturas críticas e sistemas autônomos de propulsão, navegação, armas, sensoriamento e navegação, por exemplo
Ameaças da cadeia de suprimentos (supply chain)	Softwares e componentes de origem não confiável, sem verificação de integridade	Introdução de vulnerabilidades intencionais, afetando confiabilidade e segurança operacional

Fonte: O Autor.

Quadro 3 – Ferramentas de apoio à GRO na USNAVY (USA, 2018).

Ferramenta	Descrição	Finalidade/Aplicação
OPNAV 3502/1 – Evolution ORM Assessment Sheet	Planilha padronizada para avaliação de risco em uma atividade ou evolução específica.	Usada para documentar os perigos identificados, os controles aplicados, os riscos residuais e as responsabilidades de supervisão.
OPNAV 3502/2 – Tailorable Evolution ORM Assessment Sheet	Versão personalizável da planilha OPNAV 3502/1.	Permite adaptação a diferentes tipos de operações ou ambientes específicos, mantendo a estrutura de avaliação.
OPNAV 3502/3 – ORM Program Assessment Sheet	Ferramenta para avaliação do programa ORM da unidade.	Usada para revisar a implementação da GRO em nível organizacional e durante autoavaliações anuais.
Job Hazard Analysis (JHA)	Análise sistemática de tarefas para identificar perigos e estabelecer controles.	Identifica perigos associados a tarefas específicas, especialmente úteis para tarefas rotineiras ou repetitivas. Gera uma base de dados para consulta e compartilhamento.
Root Cause Analysis (RCA)	Técnica para investigar causas fundamentais de incidentes ou falhas.	Auxilia na identificação de falhas sistêmicas e prevenção de recorrência.
Fall Risk Assessment Tool	Ferramenta para avaliar riscos de quedas em ambientes operacionais.	Específica para situações nas quais quedas representam ameaça significativa à segurança.
Federal Aviation Administration (FAA) Flight Risk Assessment Tool (FRAT)	Ferramenta desenvolvida pela FAA para avaliar riscos em voos.	Aplicada especialmente em operações aéreas navais, adaptada para prever e mitigar riscos em missões de voo.
Joint Risk Assessment Tool (JRAT)*	Ferramenta digital desenvolvida para forças conjuntas, com interface Web.	Permite planejamento de missões com base em análises de risco integradas entre serviços militares.
Feedback e Lições Aprendidas (Lessons Learned Databases)	Sistemas que coletam e compartilham experiências operacionais.	Fornecem insumos para ajustar procedimentos e treinar pessoal com base em experiências passadas.
Página Web de GRO	Página online com as informações mais atualizadas sobre políticas, treinamentos, boas práticas, ferramentas e recursos relacionados à GRO.	Apoiar a integração da GRO em toda a USNAVY, fornecendo acesso centralizado a conteúdos relevantes.
Brainstorming	Técnica de geração de ideias em grupo, utilizada para identificar soluções, alternativas ou perigos potenciais de forma criativa e sem julgamentos iniciais. Os participantes são incentivados a contribuir livremente, promovendo um ambiente colaborativo.	No contexto da GRO, o "*brainstorming*" é útil na etapa de identificação de perigos, permitindo reunir percepções variadas da equipe sobre riscos associados a uma tarefa ou missão. Isso enriquece a análise e amplia a detecção de ameaças que poderiam passar despercebidas em avaliações individuais.

* Ferramenta acessível apenas pelo pessoal autorizado pela USNAVY.
Fonte: USA, 2018.

Quadro 4 – Estatísticas sobre os Planos de Gerenciamento de Riscos (PGR) das OM da MB, organizados por ano de publicação do PGR.

PGR das OM	ANO do PGR	Risco Cibernético	SIC	ODS	OM
DelLaguna	2017	0	1	ComOpNav	Com5ºDN
DFM	2017	0	1	SGM	
BFLa	2018	0	0	ComOpNav	Com6ºDN
CPBA	2018	0	1	ComOpNav	Com2ºDN
UMEsq	2018	0	1	ComOpNav	ComemCh
IPqM	2018	0	1	DGDNTM	
DAdM	2018	0	1	SGM	
CMM	2018	0	1	SGM	
CPesFN	2019	0	0	CGCFN	
PNSPA	2019	0	0	ComOpNav	ComemCh
DOCM	2019	0	1	DGMM	
CIAGA	2019	0	1	DGN	
CEFAN	2020	0	1	CGCFN	
AgCamocim	2020	0	0	ComOpNav	Com3ºDN
FUniao	2020	0	0	ComOpNav	ComemCh
CeIMMa	2020	0	1	ComOpNav	Com9ºDN
CEDAM	2020	0	1	SGM	
FLiberal	2021	0	0	ComOpNav	ComemCh
CeIMNa	2021	0	1	ComOpNav	Com3ºDN
CeIMPL	2022	0	1	CGCFN	
BAeNSPA	2022	0	0	ComOpNav	ComemCh
CFAT	2022	0	1	ComOpNav	Com7ºDN
GptFNB	2022	0	0	ComOpNav	Com7ºDN
AMRJ	2022	0	1	DGMM	
DHN	2022	0	0	DGN	
EsIMar	2022	0	0	EMA	
PAPEM	2022	0	1	SGM	
CNBE	2022	0	1	SGM	
ENRG	2023	0	0	ComOpNav	Com5ºDN
ERMS	2023	0	1	ComOpNav	Com2ºDN
Com3°DN	2023	0	1	ComOpNav	Com3ºDN
GptFNSa	2023	0	1	ComOpNav	Com2ºDN
BAMRJ	2023	0	1	SGM	
CCCPM	2023	0	0	SGM	
CIASC	2024	0	1	CGCFN	
BNA	2024	0	1	ComOpNav	Com2ºDN
CFJ	2024	0	1	ComOpNav	Com2ºDN
EAMCE	2024	0	0	ComOpNav	Com3ºDN
Com7ºDN	2024	0	1	ComOpNav	Com7ºDN
BHMN	2024	0	1	DGN	
ERMB	2025	0	0	ComOpNav	Com7ºDN

Com4°DN	2025	0	1	ComOpNav	Com4ºDN
SSN-3	2025	0	1	ComOpNav	Com3ºDN
DPHDM	2025	0	1	SGM	
BNN	2026	0	0	ComOpNav	Com3ºDN
CPAL	2026	0	0	ComOpNav	Com3ºDN
ComEsqdE-1	x	0	1	ComOpNav	ComemCh
IEAPM	x	0	1	DGDNTM	
SIM	x	0	1	DGPM	
EAMES	2022	1	1	ComOpNav	Com1ºDN
Com2ºDN	2022	1	1	ComOpNav	Com2ºDN
CTIM	2022	1	1	DGMM	
ERMN	2023	1	1	ComOpNav	Com3ºDN
Com6°DN	2023	1	1	ComOpNav	Com6ºDN
Com5°DN	2024	1	1	ComOpNav	Com5ºDN
ComGptPatNavNE	2024	1	1	ComOpNav	Com3ºDN
HNBra	2024	1	1	ComOpNav	Com7ºDN
CMS	2024	1	1	DGMM	
ComemCh	2026	1	1	ComOpNav	ComemCh
Setor SGM*	2026	1	1	SGM	
LFM	2018	x	x	DGPM	
HNMD	2019	x	x	DGPM	
ERMRG	2022	x	x	ComOpNav	Com5ºDN
GrEOpRibMT	2022	x	x	ComOpNav	Com6ºDN
SASM	2022	x	x	DGPM	
ComForMinVar	2023	x	x	ComOpNav	Com2ºDN
CPRJ	2024	x	x	ComOpNav	Com1ºDN
Com1°DN	x	x	x	ComOpNav	Com1ºDN
HNSa	x	x	x	ComOpNav	Com2ºDN

* Todas as Diretorias Especializadas do ODS SGM. O ODS centralizou e publicou um único PGR para todo o seu Setor.
Legenda:
0 – ausente;
1 – mencionou algum risco cibernético em seu PGR (Risco Ciber) ou algum risco em segurança da informação (SIC) em seu PGR; e
x – informação não encontrada no PGR.

Fonte: Programa Netuno, Intranet da Marinha do Brasil, 2025.

Quadro 5 – Quadro diagnóstico comparativo entre USNAVY e MB.

	GRO na USNAVY	GRO na MB
Generalidades	Possui uma unidade específica para realizar e apoiar a gestão de riscos, inclusive os operacionais (*Naval Safety Command*).	Ausente na MB.
	Objetivo principal é aumentar a eficácia operacional das missões, proteger recursos e preservar vidas.	Gestão de Riscos na MB possui um foco administrativo, também sendo aplicada nos planos de segurança orgânica e nos planos de prevenção de acidentes aeronáuticos.
	Reconhece-se que o risco está presente em todas as tarefas, treinamentos, missões, operações e atividades pessoais.	Risco operacional presente apenas nas atividades relacionadas às missões.
	Definição do risco operacional abrange o potencial de perdas ou danos devido a diversos fatores, incluindo erro humano, processos inadequados e eventos externos.	Segundo a Doutrina de Operações Conjuntas, a definição do risco operacional foca em eventos externos, tais como perigos ou ameaças decorrentes de ações do oponente e fatores ambientais, em detrimento dos eventos internos como fatores geradores de riscos. Na MB, o risco operacional assemelha-se ao identificado na USNAVY, considerando eventos externos e internos, relacionados a pessoas, sistemas e infraestruturas.
	Risco é definido como um efeito negativo, conforme norma do NIST.	Risco pode ser “positivo” ou “negativo”, conforme norma da ABNT.
Pessoas	Pessoas são consideradas o principal recurso na GRO para identificação dos riscos, assim como o principal vetor de risco em todas as atividades, das mais simples às operações mais complexas.	A Doutrina de Operações Conjuntas foca no processo de planejamento e suas ferramentas de apoio como principais recursos para o risco operacional.
	Aplicável em todos os níveis hierárquicos.	Não são definidos quais níveis hierárquicos devem aprender sobre gestão de riscos.
	Aplicável a todo seu efetivo, nas rotinas operacionais e fora de serviço, em sua vida cotidiana como forma de preservar sua saúde, desempenho e prontidão.	A Política de Gestão de Riscos estabelece que a capacitação e os conhecimentos sobre gestão de riscos serão realizados para os “militares e/ou servidores civis da MB envolvidos com a Gestão de Riscos”. Não é aplicável a vida cotidiana do pessoal.
	Responsabilidade de militares, civis e contratados.	Aplicável apenas aos militares e civis da MB. Não possui referência aos contratados.
	Obrigatoriedade de aplicação da norma.	Obrigatoriedade de aplicação da norma.
	Pessoal no nível adequado possui autoridade para implementar controles visando eliminar ou minimizar o risco ou aceitá-lo formalmente.	Na Doutrina de Operações Conjuntas essa autoridade recai sobre o “Comandante e seu EMCj”, apoiado por especialistas.
	Líderes devem estabelecer os níveis adequados de risco para as equipes.	Na Doutrina de Operações Conjuntas o comandante responsável pela condução das operações possui esta responsabilidade.
	É estabelecida uma cadeia de responsabilidade clara, visando escalar o risco caso supere o nível de decisão atual.	Similar a MB, ainda que concentrado na figura do comandante, segundo a Doutrina de Operações Conjuntas.
	Decisões de risco devem envolver pessoal com conhecimento, experiência na missão ou tarefa em questão.	Similar a MB, ainda que concentrado na figura do comandante, segundo a Doutrina de Operações Conjuntas.
	Treinamento contínuo e a liderança ativa são considerados pilares essenciais.	Não identificado nas publicações pesquisadas.
	Alto escalão da Força deve emitir diretrizes específicas, dentro de sua área de atuação.	Também realizado pela MB em suas normas internas.

	Programas de treinamentos implementados continuamente por instituições de ensino da Força, para todos, desde o ingresso até sua passagem para a reserva.	Na MB são realizados cursos sobre gestão de riscos com enfoque administrativo e de controle interno. Não existe curso sobre Gestão de risco Operacional.
	Treinamentos diferenciados para todos os níveis hierárquicos e de acordo com o respectivo nível.	O curso de Gestão de Risco é genérico e único.
	Incentivo de compartilhamento de experiências e boas práticas para aumento do conhecimento.	Não identificado nas publicações pesquisadas.
Processos	Segue diretrizes do órgão superior (*Department of Defense*).	Segue diretrizes do Ministério da Defesa.
	Estabelece a política, as responsabilidades e os procedimentos, aplicáveis a toda USNAVY e suas atividades, revisada a cada 5 anos.	Ausente na MB. Uma das normas da MB que trata de Gestão de Riscos já possui quase oito anos desde sua publicação.
	Política válida também para todas as instituições por ela contratadas.	Na MB, suas políticas são aplicáveis apenas a própria instituição.
	Promove a cultura institucional de prevenção, resiliência e melhoria permanente.	Não identificado nas publicações pesquisadas.
	Decisões passam a ser embasadas em um processo formal e padronizado, aumentando a capacidade de tomada de decisões.	O Processo de Gestão de Riscos é definido em norma da MB apoiando a tomada de decisão, porém com viés administrativo. Aspectos operacionais são encontrados apenas em norma específica para a Aviação Naval.
	Quatro pilares fundamentais: liderança, treinamento, avaliação e recursos.	Presente na MB apenas em norma específica para a Aviação Naval.
	Líderes devem implementar políticas, promover sua utilização, planejar e supervisionar o treinamento e estimular *feedbacks*.	Presente na MB apenas em normas específicas para a administração e para a Aviação Naval.
	Programas de treinamento e certificação individuais, sustentada por indicadores e avaliações que verificam o nível de prontidão do pessoal, refeito a cada 3 anos, sob coordenação da *Naval Postgraduate School*.	Não identificado nas publicações pesquisadas.
	Programa de certificação de supervisor de riscos em equipes, refeito a cada 3 anos, sob coordenação da *Naval Postgraduate School*.	Não identificado nas publicações pesquisadas.
	Líderes devem disponibilizar recursos como tempo, orçamento e ferramentas.	Não identificado nas publicações pesquisadas.
	Oferece diversas ferramentas para reduzir ou compensar esses riscos.	A MB estabelece o Plano de Gerenciamento de Riscos como sua principal ferramenta. Na Aviação Naval outras ferramentas são disponibilizadas, porém com aplicabilidade limitada aquela atividade.
	Deve ser integrada ao planejamento, em todos os níveis, o mais cedo possível.	Na Doutrina de Operações Conjuntas a identificação das ameaças deve ser realizada desde o início do planejamento. Nas normas da MB, este início não está claramente definido.
	Possui três níveis de decisão, diferenciados pelo tempo disponível para o planejamento: Detalhado, Deliberado e Crítico.	O MD define os níveis de decisão em duas categorias: operacional e tático. Não é abordado o fator tempo como no GRO da USNAVY, estando ausente um nível estratégico de decisão.

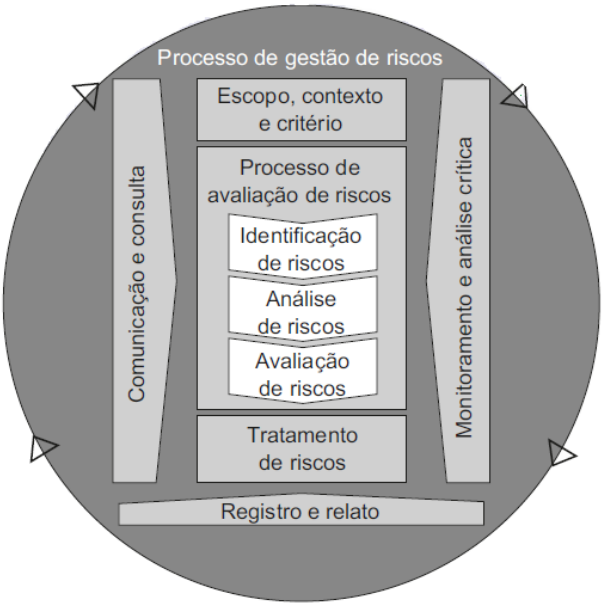
		Especificamente na Aviação Naval são considerados os três níveis como observado na USNAVY.
	Líderes devem cobrar o registro dos resultados em relatórios padronizados facilitando o compartilhamento do conhecimento.	Na MB, o Plano de Gerenciamento de Riscos registra formalmente os riscos. Especificamente na Aviação Naval diversos relatórios sobre riscos são emitidos periodicamente.
	Compartilhar conhecimento faz parte das boas práticas na Força.	Prática adotada na Aviação Naval com regularidade. Não observada em outras áreas da MB.
	Processo contínuo, elaborado por meio de "pilares" que estabelecem fundamentos da GRO, princípios básicos para sua implementação e níveis de decisão que diferenciam a variável de tempo disponível para o planejamento.	Em linhas gerais, com pequenas diferenças, todas as etapas do ciclo são abordadas pela MB, sendo o mesmo resultado final alcançado: riscos identificados e tratados. Porém, não é generalizado como na USNAVY, permanecendo um enfoque administrativo na MB ou, no caso da Aviação Naval, particularizado com as especificidades daquela atividade.
	Segurança cibernética deve estar integrada e deve ser garantida em todas as aquisições, desenvolvimentos ou modificações de sistemas de TI.	Não identificado nas publicações pesquisadas.
	Terceirizados devem adotar a mesma terminologia da USNAVY.	Não identificado nas publicações pesquisadas.
	Monitoramento da performance das tecnologias contratadas.	Não identificado nas publicações pesquisadas.
	Usa o *framework* do NIST como padrão.	Usa o *framework* da ABNT como padrão.
Tecnologias	A norma é definida como ferramenta essencial de apoio à decisão e deve ser utilizada por todos os níveis hierárquicos e todas as instituições que compõem a USNAVY.	Na MB, as normas são também referenciadas como ferramentas de apoio, porém estão mais relacionadas com processos administrativos das OM. Na Aviação Naval observa-se a única aplicação operacional da GRO na MB.
	Aplica-se a todas as tecnologias e ativos de informação, incluindo mas não se limitando a: Sistemas de Informação (SI); aplicativos; Tecnologia Operacional (OT); Plataforma de TI (PIT) para incluir sistemas de armas, controle de propulsão e sensores diversos, por exemplo; Sistemas de Controle Industrial (ICS); Sistema de Controle de Supervisão e Aquisição de Dados (SCADA); Sistemas de Casco, Mecânicos e Elétricos (HM&E); Laboratório de TI de Pesquisa, Desenvolvimento, Teste e Avaliação (RDT&E); Produtos de TI; Serviços de TI, Serviços de Nuvem; e qualquer outro ativo de TI.	Na MB a Gestão de Riscos possui um enfoque administrativo, sendo consideradas apenas as "bases de dados" e os "fluxos de informações" da MB para a gestão de riscos. Observa-se que os Sistemas Digitais Administrativos (SDA) possuem um processo de Gestão de Riscos, em contrapartida, os Sistemas Digitais Operativos (SDO) e as infraestruturas críticas não.
	Brainstorming deve ser adotado entre pessoal experiente e demais membros das equipes.	*Brainstorming* também é utilizado como ferramenta, sendo indicado tanto pelo MD na Doutrina de Operações Conjuntas quanto na MB pela SGM-107 e pela DGMM-3010.
	Fomenta o uso de tecnologias existentes e a pesquisa de novas, visando atender às necessidades específicas.	Não identificado nas publicações pesquisadas.
	Vide quadro 3 deste Apêndice para as ferramentas de apoio à GRO da USNAVY.	A Doutrina de Operações Conjuntas possui anexos que tratam de defesa cibernética e gerenciamento do risco operacional,

		assemelhando-se ao objetivo da GRO da USNAVY. Na MB, a principal ferramenta de Gestão de Riscos é o Plano de Gerenciamento de Riscos, porém com viés administrativo. A MB possui o Programa Netuno, em auxílio à tomada de decisão dos gestores. Na Aviação Naval são utilizados diagramas e ferramentas de análise, testes, ensaios, planilhas e históricos dos riscos específicos para aquela atividade.
	Matriz de Avaliação de Risco (*Risk Assessment Matrix*) como uma de suas principais ferramentas.	Várias matrizes como ferramentas de apoio à decisão: Matriz de Análise do GRO, segundo a Doutrina de Operações Conjuntas. Matriz de Probabilidade e Impacto, segundo a Portaria nº 110/EMA. Matriz de Gerenciamento do Risco, segundo a DGMM-3010.
Eventos Externos	Riscos decorrentes de eventos externos não são apresentados de forma taxativa. São inferidos nas publicações, podendo ser citados: condições meteorológicas adversas, ambientes desconhecidos ou hostis, ameaças externas imprevistas e eventos naturais ou técnicos fora do padrão.	Na Nota da CIDOC são apresentados os ataques cibernéticos a sistemas de armas de um navio, a múltiplos sistemas de comando e controle de uma Diretoria especializada e a um Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo, porém estes exemplos não foram considerados na Doutrina de Operações Conjuntas. Na Doutrina de Operações Conjuntas o ataque cibernético é considerado como um risco às operações, assim como a necessidade de identificar as forças inimigas. Na DGMM-3010 são mencionados os riscos relacionados aos equipamentos e sistemas de tecnologia da informação empregados no controle do espaço aéreo, porém sem referência direto aos riscos cibernéticos.
	Riscos associados a atividades pessoais fora do serviço.	Não identificado nas publicações pesquisadas.

Fontes: Compilação das fontes: ABNT, 2018; Brasil, 2015; Brasil, 2017a; Brasil, 2017b; Brasil, 2018a; Brasil, 2019c; Brasil, 2020b; Brasil, 2023b; Brasil, 2024b; NPS, 2025; USA, 2022a; USA, 2025; USA, 2025; e USA, 2018.

ANEXO A – Figuras Explicativas da Pesquisa

Figura 1 – Processo de gestão de riscos.



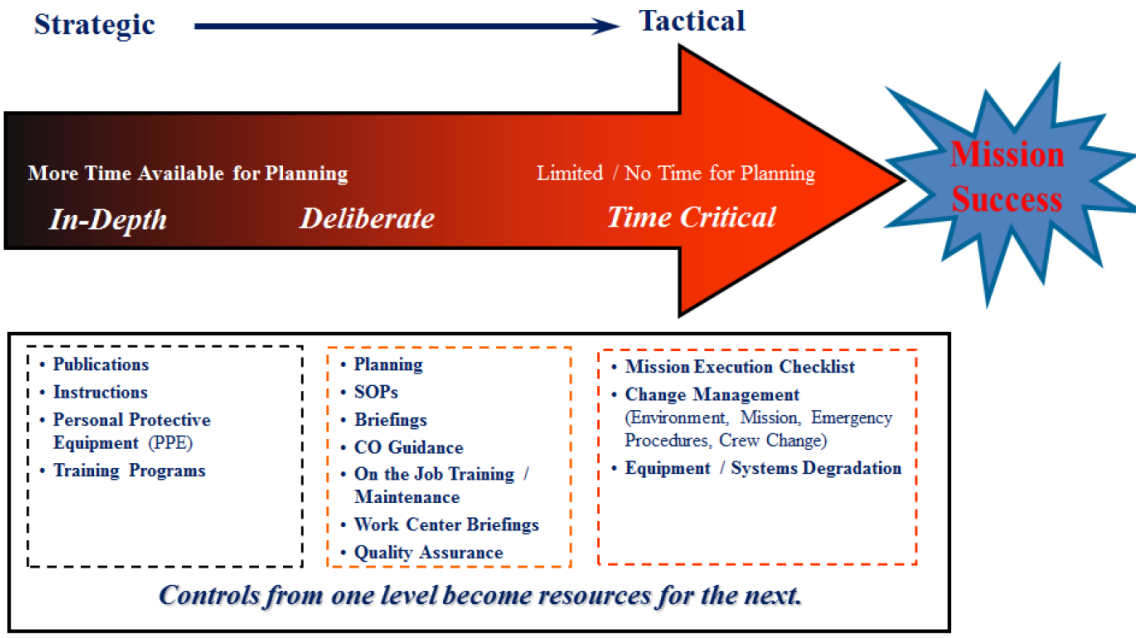
Fonte: Associação Brasileira de Normas Técnicas (ABNT), 2018.

Figura 2 – Taxonomia do risco cibernético operacional.

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
1.2 Deliberate	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2.1 Fraud	**2.2 Software**	3.1.5 Information flow	4.1.5 Unrest
1.2.2 Sabotage	2.2.1 Compatibility	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.3 Theft	2.2.2 Configuration management	3.1.7 Service level agreements	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control	3.1.8 Task hand-off	4.2.1 Regulatory compliance
1.3 Inaction	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3.1 Skills	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.2 Knowledge	2.2.6 Testing	3.2.2 Metrics	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.3 Periodic review	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design	3.2.4 Process ownership	4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	**4.4 Service dependencies**
	2.3.4 Complexity	3.3.2 Funding	4.4.1 Utilities
		3.3.3 Training and development	4.4.2 Emergency services
		3.3.4 Procurement	4.4.3 Fuel
			4.4.4 Transportation

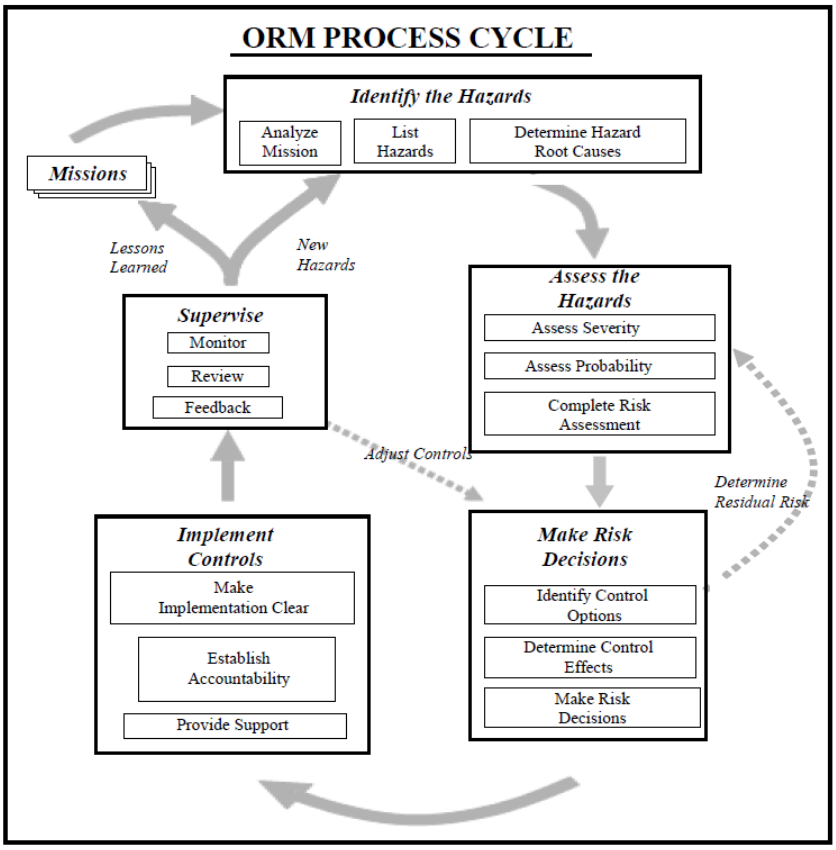
Fonte: *Software Engineering Institute* (SEI), 2014.

Figura 3 – Relação entre os níveis da GRO na USNAVY.



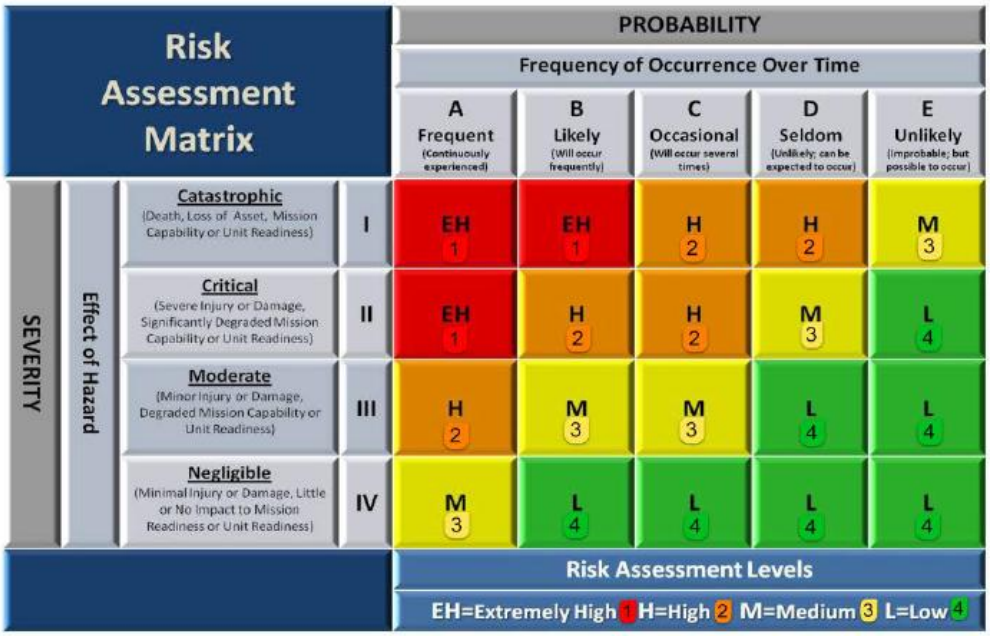
Fonte: *Department of the Navy. Office of the Chief of Naval Operations*, 2018.

Figura 4 – Processo de Gestão do Risco Operacional em cinco passos (USA, 2018).



Fonte: *Department of the Navy. Office of the Chief of Naval Operations*, 2018.

Figura 5 – Matriz de risco.



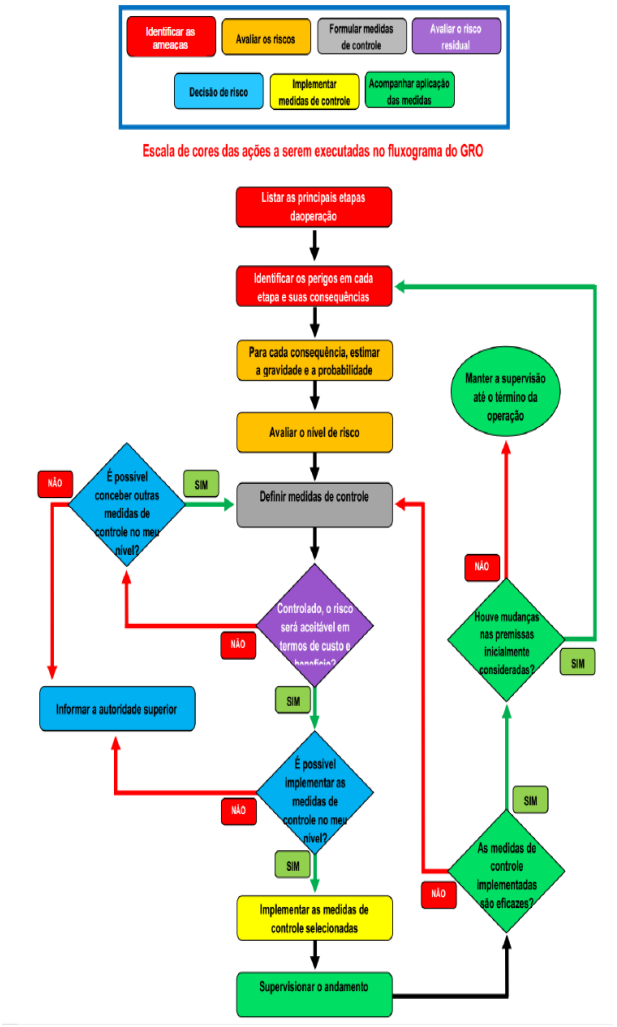
Fonte: *Department of the Navy. Office of the Chief of Naval Operations*, 2018.

Figura 6 – Matriz Probabilidade X Gravidade.

		PROBABILIDADE DE OCORRÊNCIA (Pbld)			
		Muito provável (M Provl)	**Provável** (Provl)	**Pouco provável** (P Provl)	**Improvável** (Iprovl)
GRAVIDADE (Gv)	**Catastrófica (Cat)** (Inviabiliza a missão)	CRÍTICO (Ctc)	CRÍTICO (Ctc)	ALTO (Alt)	MODERADO
	Severa (Sev) (Grande impacto na missão)	CRÍTICO (Ctc)	ALTO (Alt)	MODERADO (Mod)	BAIXO (Bai)
	Média (Med) (Dificulta a missão)	ALTO (Alt)	MODERADO (Mod)	BAIXO (Bai)	DESPREZÍVEL (Des)
	Leve (Lev) (Pouco impacto na missão)	MODERADO (Mod)	BAIXO (Bai)	DESPREZÍVEL (Des)	DESPREZÍVEL (Des)

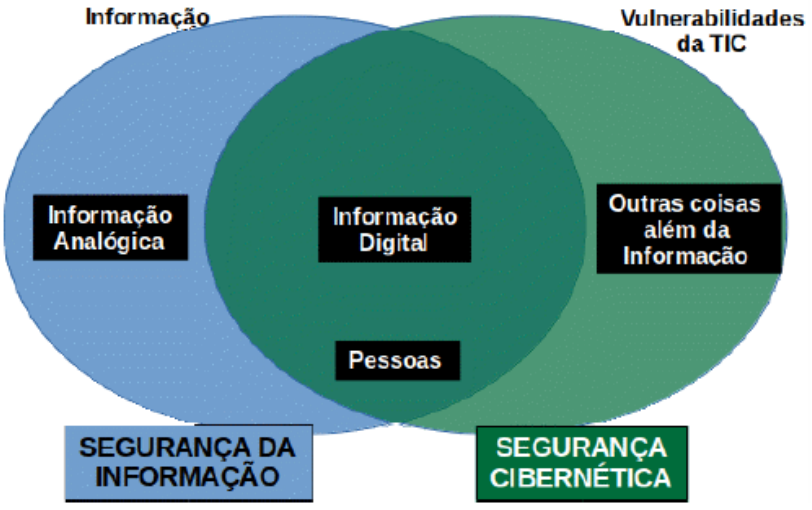
Fonte: Doutrina de Operações Conjuntas (MD30-M-01), 2020b.

Figura 7 – Fluxograma do processo de gestão do risco operacional.



Fonte: Doutrina de Operações Conjuntas (MD30-M-01), 2020b.

Figura 8 – Interseção da Segurança da Informação e da Segurança Cibernética.



Fonte: Doutrina Cibernética da Marinha (2021).