INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2016/2017

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

O PAPEL DA GESTÃO DO RISCO NO APOIO À DECISÃO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Paulo António Pires

Capitão-de-mar-e-guerra AN

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O PAPEL DA GESTÃO DO RISCO NO APOIO À DECISÃO

CMG AN Paulo António Pires

Trabalho de Investigação Individual do CPOG 2016/2017

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O PAPEL DA GESTÃO DO RISCO NO APOIO À DECISÃO

CMG AN Paulo António Pires

Trabalho de Investigação Individual do CPOG 2016/2017

Orientador: CMG M José Carlos Miguel Picoito

Pedrouços 2017

Declaração de Compromisso Anti plágio

Eu, **Paulo António Pires**, declaro por minha honra que o documento intitulado "**O papel da Gestão do Risco no apoio à decisão**" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial General 2016/2017** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.
Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, **02** de **maio** de **2017**

Paulo António Pires
CMG AN

Agradecimentos

Este espaço é dedicado a todos aqueles que de uma forma direta ou indireta contribuíram para a elaboração deste trabalho de investigação.

Assim, manifesto os meus sinceros agradecimentos aos oficiais generais e oficiais superiores da Marinha, do Exército e da Força Aérea com quem contatei e que, partilhando os seus conhecimentos e experiência profissional e pessoal, me ajudaram à realização da investigação.

Ao meu orientador, Capitão-de-mar-e-guerra M Miguel Picoito, agradeço igualmente os conselhos avisados, apoio e compreensão que sempre me disponibilizou e que em muito facilitaram o desenvolvimento do trabalho.

Aos auditores do Curso de Promoção a Oficial General 2016/2017, pela camaradagem, ânimo e partilha de experiências com que sempre me presentearam.

À minha família, pelo carinho, apoio incondicional e compreensão nas ausências.

A todos, bem hajam!

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A presente investigação tem como objetivo identificar contributos para uma gestão mais eficiente dos riscos nos Ramos das Forças Armadas, a fim de apoiar a tomada de decisão e contribuir para a prossecução dos objetivos organizacionais.

Em termos metodológicos seguiu-se uma abordagem de investigação hipotético-dedutiva, adotando-se para a pesquisa efetuada uma estratégia qualitativa e um desenho de pesquisa do tipo "Estudo de caso".

Como linhas de desenvolvimento, começou-se por caraterizar a importância estratégica da gestão do risco na gestão das organizações, concluindo-se que uma bem-sucedida gestão estratégica de riscos, alguns relacionados ou interdependentes, melhora a eficiência organizacional e contribui para o atingir dos objetivos.

Seguidamente analisou-se a cultura e a abrangência estratégica das práticas de gestão do risco existentes nos Ramos, concluindo-se que existe alguma cultura de risco e práticas em diferentes áreas e níveis organizacionais, havendo contudo lacunas na integração estratégica da informação de risco.

Por fim, analisou-se a aplicação aos Ramos de uma metodologia de gestão integrada de risco, tendo-se concluído ser uma solução que pode reforçar a cultura de risco e o apoio à decisão, permitindo assim melhorar os processos de planeamento estratégico e controlo de gestão, de planeamento e execução operacional e a afetação de recursos.

Palavras-chave

Cultura de Risco, Gestão Integrada do Risco, Gestão do Risco, Gestão de Risco Empresarial

Abstract

The present research aims to identify contributions to a more efficient risk management in the Armed Forces Branches, in order to support decision making and contribute to organizational objectives pursuit.

In methodological terms, a hypothetical-deductive research approach was followed, adopting a qualitative strategy and a case-study research design for the research.

As a development guideline, the strategic importance of risk management in the management of organizations was first introduced. It has been concluded that successful strategic management of risks, some related or interdependent, improves organizational efficiency and contributes to the achievement of goals.

Then, it was analyzed the culture and the strategic scope of risk management practices in the Branches, concluding that there is some culture of risk and practices in different areas and organizational levels, but there are gaps in the strategic integration of risk information.

Finally, the application of an integrated risk management methodology to the Branches was analyzed, and it was concluded that it is a solution that would reinforce risk culture and decision support, thus improving the processes of strategic planning and management control, of planning and operational execution and of allocation of resources.

Keywords

Risk Culture, Integrated Risk Management, Risk Management, Enterprise Risk Management

Lista de abreviaturas, siglas e acrónimos

ACA	Académica
ADMAER	Administração Aeronáutica
AIRMIC	*The Association of Insurance and Risk Managers*
ALARM	*The Public Risk Management Association*
AN	Administração Naval
BSC	*Balanced Scorecard*
CALM	Contra Almirante
CAS	*Casualty Actuarial Society*
CEMA	Chefe do Estado-Maior da Armada
CEME	Chefe de Estado-Maior do Exército
CEMFA	Chefe do Estado-Maior da Força Aérea
CMG	Capitão-de-mar-e-guerra
COR	Coronel
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
DACF	Direção de Auditoria e Controlo Financeiro
DAGI	Direção de Análise e Gestão da Informação
DN	Defesa Nacional
DPM	Diretiva de Planeamento da Marinha
EMA	Estado-Maior da Armada
EME	Estado-Maior do Exército
EMFA	Estado-Maior da Força Aérea
EMGFA	Estado-Maior General das Forças Armadas
EMQ	Engenheiro Maquinista Naval
EPM	*Enterprise Project Management*
ERM	*Enterprise Risk Management*
ERP	*Enterprise Resource Planning*
ES	Entidades Setoriais
FERMA	*Federation of European Risk Management Association*
FFAA	Forças Armadas
FND	Forças Nacionais Destacadas
GGIC	Gabinete de Gestão de Informação e do Conhecimento
GR	Gestão do Risco

GRC	*Governance, Risk and Compliance*
HIP	Hipótese
HST	Higiene e Segurança no Trabalho
IESM	Instituto de Ensino Superior Militar
IGDN	Inspeção-Geral da Defesa Nacional
IGE	Inspeção-Geral do Exército
IGFA	Inspeção-Geral da Força Aérea
IGM	Inspeção-Geral da Marinha
INF	Infantaria
INTOSAI	*International Organization of Supreme Audit Institutions*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
IUM	Instituto Universitário Militar
IRM	*Institute of Risk Management*
KPI	*Key Performance Indicator*
KRI	*Key Risk Indicator*
LPM	Lei de Programação Militar
M	Marinha
MDN	Ministério da Defesa Nacional
MGEN	Major General
NATO	*North Atlantic Treaty Organization*
NEP	Norma de Execução Permanente
OG	Objetivo Geral
OE	Objetivo Especifico
PA	Portal Administração
PESTLE	*Political, Economical, Social, Tecnological, Legal and Enviroment*
PILAV	Piloto Aviador
PMBOK	*Project Management Body of Knowledge*
PMI	*Projet Management Institute*
PGRCIC	Plano de Gestão de Riscos de Corrupção e Infrações Conexas
QC	Questão Central
QD	Questão Derivada
SIGDN	Sistema Integrado de Gestão da Defesa Nacional

SWOT	*Strengths, Weaknesses, Opportunities and Threats*
TCE	Tribunal de Contas Europeu
TIC	Tecnologias de Informação e de Comunicação
TIR	Tirocinado
UEO	Unidade, Estabelecimento ou Órgão

Introdução

Enquadramento e justificação do tema

É conhecida a variedade e a interação dos riscos nas organizações, resultante do ambiente complexo e em constante mudança em que operam, das escolhas estratégicas e da ocorrência de eventos imprevistos (CAS, 2003).

Para assegurar a continuidade das operações e o atingir dos objetivos, as organizações necessitam de controlar os efeitos da incerteza. Entramos, assim, no domínio da gestão do risco, que é um processo racional e estruturado de apoio à tomada de decisão nas organizações, usado nos vários níveis de gestão e atividades com a finalidade de controlar os riscos que afetam os objetivos, permitindo que estes possam ser alcançados com o mínimo de perdas (Collier, 2014).

Pela expressão do impacto dos riscos nos objetivos, a gestão do risco deve assim ser vista como um processo de criação e proteção de valor para as organizações (ISO, 2009a).

Num contexto de mudança constante do ambiente das organizações torna-se evidente, ao nível da gestão de topo, a necessidade de lidar com os riscos numa perspetiva mais abrangente, preditiva e proactiva, assumindo a gestão do risco uma perspetiva holística, com a organização considerada como um todo e requerendo um aperfeiçoamento das práticas de gestão existentes (CAS, 2003).

A gestão do risco é assim um processo contínuo, conduzido pela gestão de topo, que deve estar integrado na cultura da organização e ser transversal a todos os níveis e segmentos orgânicos com uma adequada atribuição de responsabilidades (FERMA, 2010). Deve ainda disponibilizar, de forma tempestiva e com qualidade, informação de gestão relevante para a tomada de decisão, que ajude a antecipar problemas e a aperfeiçoar continuamente os processos e o desempenho da organização (IGDN, 2013).

Com efeito, existem metodologias de gestão integrada e corporativa de riscos que procuram responder a estas necessidades crescentes das organizações através de novas abordagens, alinhando objetivos com mecanismos de identificação de riscos, procedendo à sua avaliação, gestão e acompanhamento, sempre procurando a sustentabilidade da organização e o aumento do seu valor no médio e longo prazo (CAS, 2003).

À semelhança de outras organizações públicas ou privadas, também as Forças Armadas (FFAA) estão sujeitas a vários tipos de risco, com origem em fatores internos e externos, pelo que a sua identificação, análise, avaliação, mitigação e controlo são essenciais tendo em vista uma melhor resposta para o atingir dos objetivos, procurando-se

sempre uma utilização eficiente dos escassos recursos colocados à disposição para o cumprimento da missão.

Entre outros, esses riscos podem ser genericamente classificados em riscos estratégicos, financeiros, operacionais, de gestão de recursos humanos, recursos materiais e informacionais, riscos de projetos, riscos de comunicação e riscos de conformidade (COSO, 2004; ISO, 2009a; FERMA, 2010).

Considerando o ajustamento estrutural e genético operado nas FFAA no âmbito da Reforma "Defesa 2020" (MDN, 2013), cujos impactos se refletem no tempo e constituem grandes desafios ao funcionamento dos Ramos, e tendo presente não só as restrições financeiras previsíveis a médio e longo prazo, como também o cenário de instabilidade e de ameaças internacionais à escala regional e global, determinantes para o estabelecimento das missões, dos meios e dos níveis de empenhamento operacional, importa dispor de adequados instrumentos que permitam gerir bem e maximizar a utilização dos recursos disponíveis para a prossecução dos objetivos.

Para cumprir a missão as FFAA têm de ter capacidade de se adaptarem às circunstâncias, num processo contínuo de transformação que as mantenham sempre relevantes e úteis, atuando com elevados padrões de eficiência e eficácia.

Em apoio aos ciclos de gestão estratégica e operacional, importa recordar que as FFAA têm vindo a adotar nas últimas décadas conceitos, instrumentos e processos associados às melhores práticas de gestão, com suporte em modernos sistemas e tecnologias de informação.

Também a gestão do risco, pela relevância no planeamento estratégico e controlo de gestão, nas operações, na gestão de recursos e na auditoria interna, deve integrar a cultura organizacional dos Ramos, com uma adequada arquitetura, estratégia e protocolos de risco, estando sempre presente nas decisões de gestão.

Objeto de estudo e sua delimitação

A presente investigação tem como objeto a Gestão do Risco (GR) nos Ramos das FFAA e as perspetivas de aperfeiçoamento de práticas que neste âmbito melhorem a gestão e a tomada de decisão.

A investigação incidiu sobre a gestão superior dos Ramos, sendo orientada à integração do risco na gestão estratégica.

Como linhas de desenvolvimento da investigação, é feita uma análise da relevância estratégica da GR nas organizações, analisa-se a cultura e as práticas de GR nos Ramos, e faz-se uma análise da aplicação aos Ramos de uma metodologia de gestão estratégica e integrada do risco, considerando a implementação da estrutura de GR e as fases de desenvolvimento do processo de GR.

Objetivos da investigação

O Objetivo Geral (OG) da investigação é identificar contributos para melhorar a eficiência da gestão do risco nos Ramos das FFAA, a fim de apoiar a tomada de decisão e contribuir para a prossecução dos objetivos organizacionais.

No sentido de cumprir com o OG, definiram-se os Objetivos Específicos (OE) constantes da Tabela 1:

Tabela 1 - Objetivo Geral e Objetivos Específicos

OG	Identificar contributos para melhorar a eficiência da gestão do risco nos Ramos das FFAA, a fim de apoiar a tomada de decisão e contribuir para a prossecução dos objetivos organizacionais.
OE1	Caraterizar a importância da gestão estratégica do risco na gestão das organizações.
OE2	Caraterizar a cultura de risco e a abrangência estratégica das práticas de gestão do risco existentes nos Ramos.
OE3	Explorar a aplicação aos Ramos de uma metodologia de gestão estratégica e integrada do risco.

Fonte: Autor (2017)

Questões da investigação e hipóteses

Tendo presente o objeto e os objetivos de investigação identificados, formularam-se, para orientação da investigação, a Questão Central (QC), as Questões Derivadas (QD) e as Hipóteses (HIP) constantes na Tabela 2:

Tabela 2 - Questão Central, Questões Derivadas e Hipóteses

QC	Como pode ser melhorada a eficiência da gestão do risco nos Ramos das FFAA em apoio às decisões estratégicas, operacionais e ao desempenho organizacional?
QD1	Qual a importância da gestão estratégica do risco para a gestão das organizações?
HIP1	Uma adequada gestão estratégica dos riscos, alguns relacionados ou interdependentes, melhora a eficiência organizacional e contribui para o atingir dos objetivos.
QD2	Qual o nível de cultura de risco e a abrangência estratégica das práticas de gestão do risco existentes nos Ramos?
HIP2	Os Ramos dispõem de alguma cultura de risco, bem como de práticas de gestão do risco de relevância estratégica em diferentes áreas e níveis organizacionais, existindo contudo lacunas no tratamento integrado da informação.
QD3	De que forma a aplicação nos Ramos de uma metodologia de gestão estratégica e integrada de riscos pode contribuir para apoiar as decisões estratégicas, operacionais e o desempenho organizacional?
HIP3	Uma abordagem mais estruturada, integrada e corporativa da gestão do risco nos Ramos, suportada por um modelo de Gestão de Risco Empresarial, melhora a capacidade de decisão e de tratamento dos riscos que afetam os objetivos.

Fonte: Autor (2017)

Breve síntese da metodologia da investigação

A presente investigação regeu-se metodologicamente pelo disposto nos documentos 010-NEP/ACA (IESM, 2015a), 018-NEP/ACA (IESM, 2015b) e Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (IUM, 2016), tendo sido seguido o percurso metodológico, descrito na Figura 1, assente em três fases: exploratória, analítica e conclusiva.

Figura 1 - Percurso metodológico

Fonte: Autor (2017)

Como método de investigação, foi utilizada uma abordagem hipotético-dedutiva com o intuito de encontrar uma resposta para a questão formulada através do teste a hipóteses levantadas, adotando-se para a pesquisa e análise efetuadas uma estratégia eminentemente qualitativa.

A investigação seguiu um desenho de pesquisa do tipo "Estudo de caso", uma vez que se estudam as práticas e modelos de GR a aplicar aos Ramos das FFAA.

Nessa conformidade, foi definida uma QC a partir de alguma pesquisa bibliográfica inicial e de entrevistas exploratórias informais.

De modo a facilitar a condução da investigação e a emprestar-lhe a ordem e o rigor indispensáveis, optou-se por organizá-la em torno de três QD, dando deste modo um fio condutor à investigação. Assim, foram propostas três hipóteses de investigação, que serviram de base à observação, recolha de dados e respetiva análise.

Deu-se então continuidade à pesquisa bibliográfica, tendo ainda sido realizadas entrevistas semiestruturadas, baseadas no guião geral constante do Apêndice C, a especialistas e a responsáveis em áreas da gestão superior dos Ramos das FFAA, com vista a recolher elementos relevantes para a análise.

Seguiu-se depois, na fase analítica, ao estudo da informação coligida, analisando-se a importância da gestão estratégica dos riscos na gestão das organizações e as práticas

seguidas pelos Ramos das FFAA neste domínio, o que permitiu, por fim, explorar como pode ser adaptada por estes uma metodologia de gestão estratégica e integrada de riscos.

Foi assim possível avançar para a fase conclusiva, no decurso da qual se procedeu ao teste das hipóteses e subsequente enunciação das respostas às interrogações formuladas, designadamente às questões derivadas e à questão central.

Organização do trabalho

Este trabalho, para além da presente introdução e das conclusões, está organizado em quatro capítulos.

No primeiro capítulo, faz-se uma breve referência à literatura consultada e aos principais conceitos subjacentes à investigação para enquadramento teórico do tema.

No segundo capítulo, analisa-se a importância da gestão estratégica dos riscos na gestão das organizações.

No terceiro capítulo, analisa-se a cultura de risco e as práticas de GR existentes nos Ramos das FFAA, considerando as áreas de aplicação, a abrangência estratégica dos processos e o nível de integração da informação.

No quarto e último capítulo, e tendo por base os elementos coligidos anteriormente, explora-se uma solução de aplicação aos Ramos de uma metodologia de gestão estratégica e integrada de riscos, considerando a implementação da estrutura de GR e as fases de desenvolvimento do processo de GR.

1. Revisão da literatura e metodologia

1.1. Revisão da literatura

A revisão da literatura incidiu na consulta a vasta bibliografia sobre a temática da GR em empresas e organizações públicas, complementada com a leitura de diversos trabalhos de autores e organizações onde o tema em apreço tem sido abordado em diferentes perspetivas.

Procedeu-se igualmente à leitura de normas *standard* sobre a gestão do risco, designadamente:

- As normas da *International Organization for Standardization* (ISO):
  - ISO 31000:2009[1] *Risk Management - Principles and Guidelines* (ISO, 2009a);
  - ISO 31010:2009 *Risk Management - Risk Assessment Techniques* (ISO, 2009b);
  - ISO *Guide 73 Risk Management – Vocabulary* (ISO, 2009c);
  - ISO/TR 31004:2013 *Risk management - Guidance for the Implementation of ISO 31000* (ISO, 2013).
- A metodologia do *Commitee of Sponsoring Organizations of the Tredway Commission*[2] (COSO) - *Enterprise Risk Management- Integrated Framework* (COSO, 2004).

1.2. Metodologia

A metodologia adotada foi a referida na introdução do presente trabalho, bem como o percurso metodológico seguido nas várias fases da investigação.

Os dados obtidos da pesquisa e análise documental e bibliográfica e das entrevistas semiestruturadas foram analisados criteriosamente e contribuíram significativamente para as respostas às questões da investigação.

1.3. Enquadramento conceptual

A presente investigação observou um conjunto de conceitos base sobre risco e GR, aqui apresentados, e conceitos complementares que constam do Apêndice A.

[1] Resultado do trabalho de organizações dedicadas à GR no Reino Unido.

[2] COSO é uma organização internacional, originária dos Estados Unidos da América, que divulga boas práticas de gestão, ajudando as organizações a aperfeiçoar as estruturas e procedimentos em matéria de Gestão do Risco Empresarial, sistema de controlo interno e combate à fraude (COSO, 2017).

1.3.1. Risco

Existem múltiplas definições do risco, todas associando o risco à possibilidade de ocorrência de eventos ou de situações que podem constituir oportunidades ou ameaças ao sucesso das organizações.

O risco integra três elementos chave: o evento, as causas e os impactos. Um evento decorre de fatores internos e externos à organização, afeta a realização dos objetivos e pode causar impacto negativo, positivo ou ambos (COSO, 2004).

No mesmo sentido, Collier refere o risco como a "combinação da probabilidade de um evento e das suas consequências, podendo estas serem positivas ou negativas." (Collier, 2014, p. 4).

De igual modo, para a ISO o risco é o " efeito da incerteza na consecução dos objetivos", e esse "efeito é um desvio, positivo ou negativo, relativamente ao esperado" afetando os ativos, as atividades e operações de uma dada entidade (ISO, 2009c; 2009a).

No âmbito da gestão de projetos, riscos são considerados eventos ou circunstâncias incertas que, se ocorrerem, tem efeitos positivos ou negativos nos objetivos dos projetos[3] (PMI, 2013).

Os riscos têm impacto nas organizações no curto, médio e longo prazo, estando relacionados com a tática, as operações e com a estratégia. Os riscos táticos estão em regra associados a projetos e à aquisição ou desenvolvimento de produtos ou serviços, os riscos operacionais estão associados ao funcionamento normal das organizações (à sua aptidão para executarem a estratégia) e os riscos estratégicos afetam a estratégia e os objetivos (FERMA, 2010).

1.3.2. Gestão do risco

Segundo a ISO, a GR é um conjunto de atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco (ISO, 2009c).

Numa perspetiva estratégica, a GR é um processo de identificação, de avaliação e tratamento de riscos e incertezas, com origem em eventos ou cenários internos e externos que podem afetar os objetivos estratégicos e, por conseguinte, a criação de valor para os vários *stakeholders*[4] (ISO, 2009a).

[3] Afetam normalmente condições de prazo, custo, âmbito e qualidade (PMI, 2013).
[4] *Stakeholder* é um conceito anglo-saxónico muito utilizado nas áreas da gestão e das tecnologias da informação, que designa as partes interessadas ou intervenientes nas organizações (PA, 2017) .

Uma adequada GR deve ser feita de forma continuada ao longo de todo o processo de negócio da organização, devendo existir envolvimento de todos, promovendo-se a eficiência nos vários níveis de gestão de modo a alcançar o sucesso da estratégia (Frigo & Anderson, 2011).

Uma bem-sucedida GR deve ainda ser adequada quanto ao nível de risco aceite pela organização (o apetite ao risco), desenvolver-se em função da dimensão, natureza e complexidade desta, estar alinhada com outras atividades corporativas e assegurar uma resposta dinâmica às alterações da envolvente (ISO, 2009a).

1.3.3. Cultura de risco

A implementação de modelos e atividades de GR não chega para proteger as organizações das falhas de funcionamento. É imperativo que a GR esteja integrada na cultura da organização e inclua o apetite e a tolerância aos riscos, e isso pressupõe compromisso e liderança. O pensamento estratégico deve ter em consideração o risco (FERMA, 2010).

Conforme ilustrado na Figura 2, para o desenvolvimento de uma boa cultura de risco é necessário dispor de uma adequada arquitetura de risco, definir uma estratégia e elaborar protocolos de risco (FERMA, 2010).

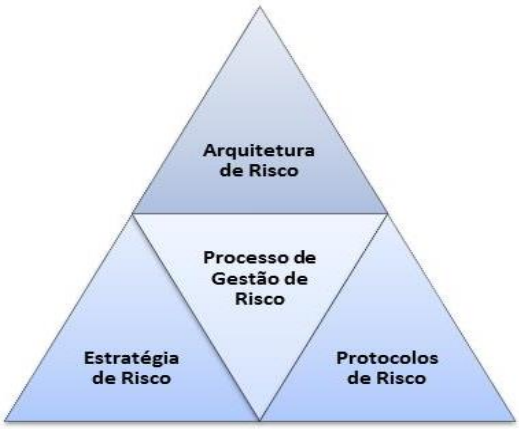

Figura 2 – Componentes da cultura de risco

Fonte: Autor, adaptado de (FERMA, 2010)

A arquitetura de risco compreende a organização, a definição e atribuição de responsabilidades e as regras de comunicação e de reporte de riscos. A estratégia de risco contém os objetivos orientadores das atividades de GR, o apetite e a tolerância ao risco, que decorrem da política de GR. Os protocolos de risco abrangem as normas e os procedimentos de GR, sendo especificadas metodologias, técnicas e instrumentos a aplicar (FERMA, 2010).

2. A importância estratégica do risco nas organizações

O presente capítulo procura caraterizar a importância estratégica do risco na gestão das organizações, considerando a evolução havida nos modelos de GR, o risco no âmbito da gestão estratégica e as potencialidades evidenciadas pelos modelos de Gestão de Risco Empresarial (*Enterprise Risk Management* – ERM).

2.1. Evolução da gestão do risco

Tradicionalmente, os riscos eram tratados de forma isolada, apenas como ameaças e numa perspetiva de transferência ou cobertura de prejuízos, recorrendo-se para tal a seguros ou outros instrumentos. Procurava-se apenas proteger os ativos da organização contra riscos naturais e outros incidentes físicos (Oliveira, 2013).

Gradualmente, as organizações passaram a considerar a GR como um processo mais prioritário à gestão, deixando os riscos de ser tratados de forma isolada, assumindo natureza estratégica e sendo suportada por estruturas próprias e instrumentos de apoio à tomada de decisão (Hardy, 2010).

As empresas foram assim evoluindo na GR acrescentando às dimensões física e operacional da GR outras dimensões, como a financeira (em contextos de instabilidade económica e de resultados desfavoráveis) e a conformidade face a normas e regulamentos em vigor (Oliveira, 2013).

Contudo a GR continua ainda muito informal e descentralizada na maioria das organizações. Essa descentralização, apesar da vantagem conferida pela consciencialização para o risco nas áreas onde estes são geridos, não permite que se obtenha uma visão global dos diferentes riscos e suas interdependências, pelo que importa evoluir no sentido de uma maior centralização da função e adotar uma gestão integrada do risco (Castanheira & Rodrigues, 2006).

Para este autor, “mais do que se concentrar em riscos ao acaso, a abordagem integrada procura implementar processos consistentes que considerem todos os eventos que podem afetar adversamente as empresas.” (Castanheira & Rodrigues, 2006, p. 5).

Neste contexto, surge então a Gestão de Risco Empresarial (ERM) como um novo paradigma à GR, focada na criação de valor e cuja perspetiva é a coordenação integrada do risco por toda a organização, em vez de cada área gerir os seus próprios riscos (Oliveira, 2013).

A ERM veio transformar a GR tradicional, vista numa ótica de “silos”, fragmentada e funcional, numa abordagem moderna e mais completa, adaptável à mudança,

multifuncional, colaborativa, holística, integrada e coordenada ao mais alto nível na organização (Pickett, 2006).

A Figura 3 contém as principais diferenças entre a gestão de risco tradicional e a ERM.

Figura 3 - Gestão de risco. Modelo tradicional versus ERM

Fonte: (Castanheira & Rodrigues, 2006)

2.2. O risco e a gestão estratégica

A gestão estratégica é definida como a "arte e ciência que formula, implementa e avalia um conjunto de decisões interfuncionais que permitem a uma organização alcançar os seus objetivos" (David, 2003, p. 5).

O risco é considerado um *driver* das decisões estratégicas das organizações, embora nem sempre estas o considerem no planeamento estratégico (Maia & Chaves, 2016).

Um estudo da consultora Deloitte (2014, cit. por Maia & Chaves, 2016), referente aos anos de 2003 e 2012, diz-nos que 73% dos principais prejuízos das empresas têm origem em riscos estratégicos, seguido do risco financeiro com 17% e os restantes 10% em riscos operacionais.

Oliveira (2013) considera o risco estratégico como o efeito das incertezas nos objetivos estratégicos e nas metas definidas, pelo que importa identificar e avaliar os riscos estratégicos de forma a evitar e a prevenir os efeitos das ameaças e a alavancar as oportunidades, no sentido da prossecução dos objetivos estratégicos.

A gestão eficaz dos riscos estratégicos só é possível no contexto da formulação, implementação e controlo da estratégia, interligando assim a GR com o planeamento e o controlo de gestão[5] (COSO, 2004).

Durante a fase de formulação da estratégia de uma organização faz-se um diagnóstico do ambiente interno e externo, avaliando-se os pontos fortes e as fraquezas, as ameaças e as oportunidades, através de uma análise SWOT (*Strengths, Weaknesses, Opportunities and Threats*[6]*)*, a fim de determinar onde concentrar as iniciativas estratégicas (Maia & Chaves, 2016).

Para Maia & Chaves (2016), as ameaças e as oportunidades identificadas nesta fase constituem riscos "pré-estratégicos" que devem ser avaliados. Para tal, podem ser usadas diferentes técnicas de avaliação do risco, por nível organizacional, por departamento, por projeto, por atividade ou por risco específico, transversal ou correlacionado.

Depois de identificados e mapeados estes riscos escolhem-se apenas os que podem afetar o negócio da organização ao nível da missão, da visão e dos objetivos, e procede-se à sua análise quanto à probabilidade de ocorrência e impacto estratégico, não esquecendo de considerar outros impactos ao nível da reputação, impactos financeiros e de conformidade (Maia & Chaves, 2016).

As organizações têm no entanto dificuldade em definir e quantificar os riscos estratégicos (Oliveira, 2013). Para auxiliar no processo, há que mapear esses riscos classificando-os por categorias e proceder a uma análise de cenários, que deverá ser apresentada e discutida com a gestão superior da organização (Maia & Chaves, 2016).

Já na fase de implementação da estratégia, as iniciativas a desenvolver para serem bem-sucedidas, devem ter presente a influencia positiva ou negativa dos riscos identificados anteriormente, assim como outras eventuais limitações de ordem regulamentar ou associadas à disponibilidade de recursos (Maia & Chaves, 2016).

Depois de implementadas as iniciativas mais adequadas à prossecução dos objetivos estratégicos, importa proceder à sua monitorização e revisão periódica. Neste âmbito, o acompanhamento preventivo e sistemático dos fatores associados aos eventos geradores de

[5] O controlo de gestão compreende "um conjunto de instrumentos que motivam os responsáveis descentralizados a atingirem os objetivos estratégicos, privilegiando a ação e a tomada de decisão em tempo útil e favorecendo a delegação de autoridade e a responsabilização" (Jordan, H.; Neves, J.C. e Rodrigues, J.A., 2011, p. 21).

[6] Forças, fraquezas, oportunidades e ameaças.

risco estratégico permitem à organização preparar-se para responder de forma adequada a esses mesmos riscos (ISO, 2009a).

Para Maia & Chaves (2016), uma boa gestão dos riscos estratégicos permite reagir desenvolvendo ações que aumentem a probabilidade de sucesso dos objetivos e dos resultados previstos, sendo essencial proceder à sua monitorização através de indicadores de performance de risco (*Key Risk Indicator* - KRI*).*

A revisão dos riscos estratégicos deve ser efetuada periodicamente de forma a acompanhar as mudanças no ambiente da organização, conferindo assim a oportunidade de decidir sobre a continuidade ou a mudança da estratégia, ou a eliminação do risco (ISO, 2009a).

Quando uma organização implementa iniciativas estratégias orientadas aos riscos estratégicos, está a convertê-las em objetivos operacionais e a atribuir responsabilidades não só à área responsável pela GR como também a outras áreas dentro da organização, possibilitando a avaliação da performance do risco e a melhoria da eficiência operacional nos vários níveis (Maia & Chaves, 2016) .

2.3. A Gestão de Risco Empresarial

Segundo COSO, a ERM é "um processo, desenvolvido pela gestão de topo, órgãos de gestão e demais colaboradores, aplicado na definição da estratégia e abrangendo toda a organização, que tem como objetivo a identificação dos eventos potenciais que podem afetar a organização e gerir os riscos de forma alinhada com o apetite pelo risco pretendido, com vista a fornecer segurança aceitável relativamente ao cumprimento dos objetivos definidos pela organização." (COSO, 2004).

Para Hardy (2010), entre outras vantagens, a ERM é um instrumento de gestão estratégica que permite aumentar o conhecimento e a compreensão do risco dentro da organização, alinhando os riscos das atividades e projetos às metas e objetivos e estimulando a cultura de risco e o desenvolvimento de competências que proporcionam maior eficiência no diagnóstico, avaliação e GR.

Ainda para este autor, nesta abordagem não há espaço para discutir o risco de uma área funcional específica, o que é requerido é uma perspetiva transversal de análise face à missão e aos objetivos estratégicos, focada nas áreas chave de risco (Hardy, 2010).

Com a crise financeira de 2008, a ERM sobressai como processo de gestão crítico em vários sectores de atividade, assumindo os departamentos de risco e os seus profissionais maior notoriedade e reconhecimento, pelo seu contributo para mitigar os riscos críticos que

afetam o crescimento sustentável das suas organizações no longo prazo (Maia & Chaves, 2016). Muitas empresas passaram, por exemplo, a incluir nos seus planos de comunicação (relatórios de gestão e portais institucionais) informação sobre a gestão dos seus riscos (Oliveira, 2013).

Segundo Hardy (2010), a ERM providencia um ciclo completo em torno da GR.

Como ilustrado na Figura 4, o ciclo inicia-se com o conhecimento dos objetivos estratégicos e respetivas metas, a que se segue a identificação das áreas chave de potencial risco e depois a avaliação, implementação e monitorização das ações destinadas a prevenir, reduzir ou mitigar esses riscos, num processo dinâmico de adaptação permanente às mudanças de contexto (Hardy, 2010).

Figura 4 - Ciclo de Gestão do Risco

Fonte: Autor, adaptado de (Hardy, 2010)

Para que a ERM seja eficaz, é necessário que a organização se focalize nos eventos internos e externos geradores de risco, na utilização de métodos de avaliação simples, na identificação dos responsáveis pela GR e na utilização de sistemas informacionais de suporte (Castanheira & Rodrigues, 2006).

A ERM é assim uma metodologia que resulta da estratégia da organização, dos seus objetivos, da cultura, do apetite ao risco e dos recursos disponíveis, não existindo uma abordagem única para a sua aplicação (Deloach, 2000).

Caraterizaremos seguidamente os principais modelos de ERM.

2.3.1. Modelo COSO – *Enterprise Risk Management*

O modelo COSO–ERM providencia uma solução de implementação da metodologia ERM (COSO, 2004).

Criado em 2004, é um modelo estruturado e formal de GR integrado, aplicado à estratégia e transversal à organização, que permite identificar os potenciais riscos que podem afetar a organização, gerindo-os em função do respetivo perfil e dos objetivos organizacionais. Permite identificar e avaliar todos os riscos da organização gerindo-os de forma holística e coordenada (COSO, 2004).

O modelo COSO–ERM ajuda as organizações a atingirem as suas metas de performance, minimizando a perda de recursos, assegurando uma comunicação eficaz e o cumprimento de leis e regulamentos que evitem riscos de reputação (COSO, 2014).

Este modelo corporativo e integrado de GR permite alinhar o apetite ao risco da organização com a estratégia, gerir e fortalecer as decisões de resposta a múltiplos riscos, aproveitar as oportunidades e reduzir as surpresas e os custos operacionais (COSO, 2014).

Para a COSO (2014), um modelo de GR eficiente e um bom sistema de auditoria e controlo interno[7] são essenciais para o sucesso de longo prazo das organizações, pois permitem, numa perspetiva holística, integrar a governança e a gestão dos processos.

O COSO-ERM responde a este novo paradigma, sendo hoje em dia utilizado por entidades com responsabilidades nas áreas da auditoria e do controlo interno.

É o caso da Inspeção Geral da Defesa Nacional (IGDN), onde as atividades seguem o modelo de avaliação dos riscos do COSO "centrando-se na antecipação e na prevenção dos principais riscos das entidades auditadas, através da identificação, avaliação e controlo dos riscos, não se limitando apenas à análise de factos históricos ou de legalidade" (IGDN, 2013).

Detalhando um pouco mais o modelo COSO-ERM, conforme ilustrado na Figura 5, este proporciona um bom nível de GR, com uma abordagem tridimensional que considera as seguintes perspetivas: objetivos organizacionais; componentes de ação, a desenvolver em torno da GR para atingir aqueles objetivos, e níveis organizacionais que executam essas ações (COSO, 2004).

[7] O controlo interno corresponde à organização, métodos e medidas a adotar com vista a salvaguardar os ativos, a verificar a exatidão e a fidedignidade dos dados contabilísticos, a promover a eficácia operacional e a estimular o cumprimento das políticas determinadas pela gestão (COSO, 1992).

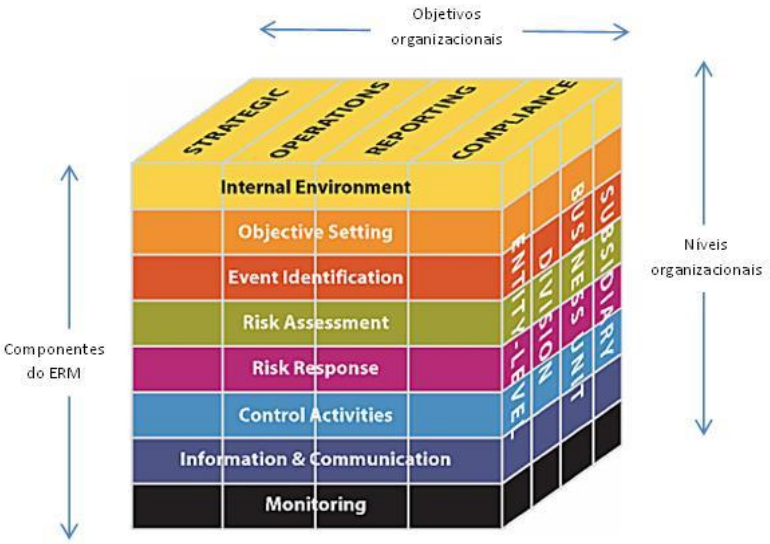

Figura 5 – Cubo COSO - ERM

Fonte: Autor, adaptado de (COSO, 2017)

Quanto aos objetivos, o modelo COSO-ERM identifica quatro tipos, que se interrelacionam: (COSO, 2004)

- Estratégicos *(strategic)*: são os objetivos de nível mais elevado, alinhados com a missão. Os riscos a eles associados podem colocar em causa a estratégia como um todo e a própria missão da organização;
- Operacionais *(operations)*: são objetivos relacionados com a eficiência e eficácia na gestão dos recursos da organização e no desenvolvimento das operações. Os riscos a eles associados têm impacto nas atividades das diversas áreas;
- Comunicação *(reporting)*: são objetivos associados à fiabilidade do reporte interno e externo da organização;
- Conformidade *(compliance):* são objetivos associados ao cumprimento das leis, regulamentos e procedimentos em vigor.

Os riscos associados aos objetivos estratégicos e operacionais, por estarem também sujeitos a fatores externos, são mais difíceis de controlar, já os riscos de comunicação e de conformidade, estando mais dependentes de eventos internos, podem mais facilmente ser controlados pela organização (COSO, 2004).

Para alcançar estes objetivos o modelo prevê um processo de GR com oito componentes de ação, descritos no Apêndice B, relacionados entre si e estruturados em função da dimensão da organização, designadamente: “Ambiente Interno”; “Fixação de Objetivos”; “Identificação de Eventos”; “Avaliação dos Riscos”; “Resposta aos Riscos”;

"Atividades de Controlo"; "Informação e Comunicação" e "Monitorização" (COSO, 2004).

O grau de eficácia da GR baseada neste modelo estruturado decorre da avaliação destas componentes de ação, do enquadramento dos riscos no apetite ao risco, na garantia de que os objetivos estratégicos e operacionais são alcançados, e que a comunicação é credível e as leis e regulamentos estão a ser cumpridos (COSO, 2004).

Importa no entanto realçar que o modelo COSO-ERM não garante que os objetivos sejam alcançados de forma absoluta. De facto, apesar de conferir algum grau de segurança aceitável para que possam ser atingidos, a ação cognitiva dos decisores pode facilmente conduzir a avaliações e a decisões incorretas (COSO, 2004).

2.3.2. Modelo ISO – *Enterprise Risk Management*

Como referido, a crise financeira de 2008 veio reforçar a importância de uma adequada GR nas organizações. Novos *standards* internacionais foram publicados neste âmbito, entre eles a norma ISO 31000:2009 – *"Risk Management – principles and guidelines"*, dedicada também à implementação de um *framework* ERM (ISO, 2009a).

Esta norma disponibiliza um modelo de estrutura de GR para utilização pelas organizações públicas e privadas, recomendando que estas desenvolvam, implementem e aperfeiçoem continuamente as suas práticas de GR integrando-as no modelo de governança, nas políticas, valores e cultura organizacional, no planeamento estratégico, no controlo de gestão e no *reporting* (ISO, 2009a).

Trata-se de um modelo potenciador da GR nas organizações que considera a articulação dos objetivos dos vários níveis organizacionais, fortalece a comunicação estratégica e a *accountability*[8] (ISO, 2009a).

Para a ISO, a GR deve obedecer aos seguintes princípios (ISO, 2009a):

- Criar e proteger o valor das organizações;
- Ser parte integrante de todos os processos, incluindo a tomada de decisão;
- Considerar explicitamente a incerteza;
- Ser sistemática, estruturada e atempada;
- Basear-se na melhor informação disponível;
- Ser feita à medida;

[8] Aplicado às organizações públicas, é o processo pelo qual estas e os seus gestores são responsáveis pelas suas decisões e ações, incluindo a gestão de fundos públicos, a equidade e todos os aspetos do desempenho (INTOSAI, 2016).

- Ter em conta os fatores humanos e culturais;
- Ser transparente e participada;
- Ser dinâmica, iterativa e reativa à mudança;
- Facilitar a melhoria contínua da organização.

Tal como o COSO-ERM também a ISO-ERM, não contrariando aquele modelo, apresenta um *standard* internacional que proporciona uma visão holística da GR com processos e conceitos comuns, proporcionado uma estrutura de implementação e de suporte do processo de GR, conforme ilustrado na Figura 6.

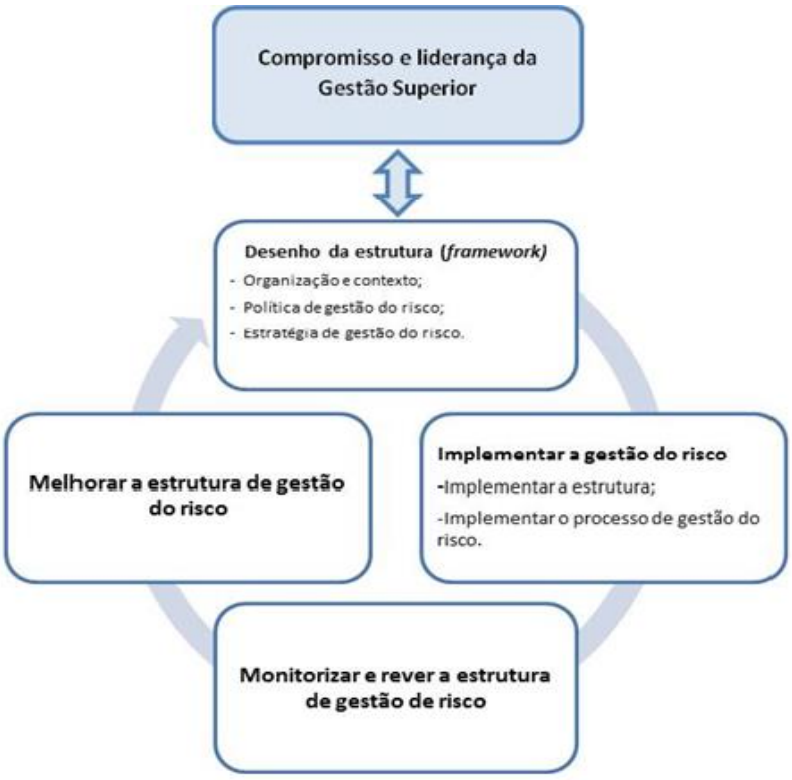

Figura 6 - Estrutura de Gestão do Risco – ISO 31000:2009

Fonte: Autor, adaptado de (ISO, 2009a)

Como fator crítico de sucesso, a implementação de uma estrutura de GR na organização pressupõe uma liderança e um compromisso da gestão superior para que seja possível um envolvimento de todos e em todas as áreas (Jorge, 2013).

Ao desenhar uma estrutura de GR, importa avaliar e compreender o contexto externo e interno da organização, analisando a envolvente em várias perspetivas. No plano externo, analisar, entre outras, a envolvente legal, regulamentar, social, económica e cultural, identificar os fatores chave e as tendências que tenham impacto sobre os objetivos da organização e identificar as relações com os *stakeholders.* No plano interno, há que avaliar

entre outros aspetos, o modelo de governança, a estrutura organizacional, as funções e responsabilidades, as políticas, os objetivos e estratégias implementadas, as capacidades em recursos e informação, os sistemas de informação, os processos de apoio à tomada de decisão (formais e informais) e a cultura da organização (Jorge, 2013).

Outro aspeto relevante para o desenho da estrutura é a existência de uma política de GR que estabeleça os objetivos e os compromissos neste domínio. Esta política é essencial para a integração da GR no sistema de gestão da organização e para o estabelecimento de prioridades. A gestão superior deve assegurar que os objetivos estratégicos estão alinhados com os objetivos da GR e que são disponibilizados os recursos necessários e atribuídas as responsabilidades neste âmbito pelos diferentes níveis organizacionais (ISO, 2009a).

A integração da GR em todos os processos organizacionais vai promover a eficiência e eficácia destes e facilitar a tomada de decisão (ISO, 2009a).

O processo de GR do modelo ISO-ERM desenvolve-se num conjunto de atividades coordenadas, que respeitam a terminologia do Guia 73 "*Risk Management – vocabulary-guidelines for use of standards*", conforme ilustrado na Figura 7.

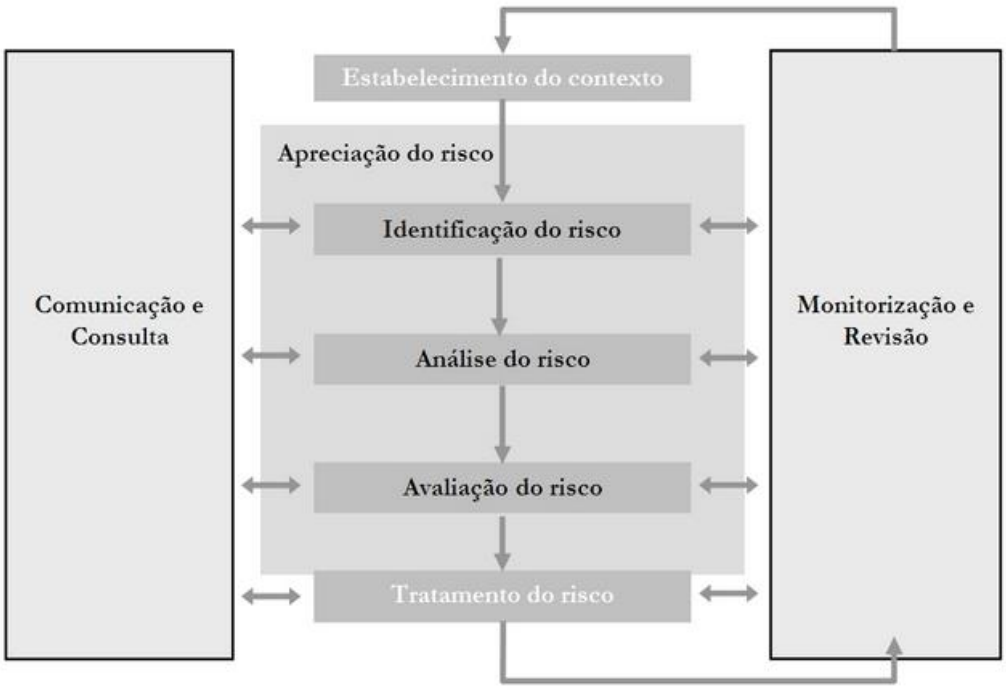

Figura 7 - Processo de Gestão do Risco - ISO 31000:2009

Fonte: Autor, adaptado de (ISO, 2009a; ISO, 2009c)

Os pontos críticos do processo de GR são a "Apreciação do risco" e o "Tratamento do risco" (ISO, 2009a).

A "Apreciação do risco" requer um conhecimento da organização e do ambiente legal, social, político e cultural em que opera, bem como a compreensão dos objetivos estratégicos e operacionais. Inclui o conhecimento dos fatores críticos de sucesso, as ameaças e as oportunidades relativas aos vários objetivos e pressupõe que as atividades de valor acrescentado (as iniciativas estratégicas) são identificadas assim como os riscos a elas associados (ISO, 2009a).

O resultado da "Análise de risco" deve ser usado para definir o perfil de risco e a tolerância a cada um dos riscos, de modo a priorizar o seu tratamento. Os riscos são mapeados e identificadas as áreas afetadas, o que permite definir os mecanismos de controlo que é necessário ajustar. A "Análise de risco" identifica assim os riscos que requerem atenção da gestão (ISO, 2009a).

O "Tratamento do risco" compreende a seleção e implementação das medidas de controlo do risco (ISO, 2009a). À semelhança do modelo COSO–ERM (componente de "Resposta ao risco") (COSO, 2004), e de outras normas, designadamente as aplicadas à gestão de projetos (PMI, 2013), podem ser seguidas várias estratégias de tratamento dos riscos.:

Perante ameaças ou riscos negativos:

- Evitar, eliminando completamente a probabilidade da ocorrência do risco, mediante decisão de não iniciar ou continuar a atividade portadora de risco;
- Transferir, total ou parcialmente, o impacto e a responsabilidade do risco para terceiros;
- Mitigar, reduzindo a probabilidade e/ou o impacto do risco para níveis aceitáveis, ou
- Aceitar, estabelecendo ou não planos de contingência para tratar os riscos caso ocorram (COSO, 2004; ISO, 2009a; PMI, 2013).

E perante oportunidades ou riscos positivos:

- Explorar, garantindo a ocorrência do risco para tirar vantagem ou beneficio;
- Partilhar, transferindo total ou parcialmente, a propriedade do risco para um terceiro que tenha mais capacidade para o explorar;
- Potenciar, aumentando a probabilidade e/ou o impacto do risco, ou
- Aceitar, tirando vantagem da ocorrência do risco (COSO, 2004; ISO, 2009a; PMI, 2013).

As estratégias de evitar ou prevenir e de mitigar são boas perante riscos críticos negativos de grande impacto. Aceitar ou transferir são estratégias mais adequadas para riscos menos críticos e de baixo impacto (ISO, 2009a) .

Tal como referido para o modelo COSO-ERM, o processo de GR da ISO exige um eficiente e eficaz sistema de controlo interno, no entanto há sempre que avaliar o custo-benefício da decisão de implementação das medidas de controlo à luz da redução de riscos que é pretendida (COSO, 2004; ISO, 2009a).

A "Monitorização e revisão" e a "Comunicação e consulta" são instrumentos que se revestem de particular importância no suporte ao processo de GR, devendo ocorrer de forma contínua. Garantem que a organização monitoriza a performance do risco e aprende com a experiência, privilegia a comunicação e o relato interno e externo, e a credibilização destes instrumentos de modo a criar confiança na organização e nos *stakeholders* (ISO, 2009a).

2.4. Síntese conclusiva

As práticas de GR têm evoluído para ir ao encontro das necessidades de gestão das organizações, adotando-se modelos estruturados de GR que tornam os processos mais consistentes que permitem que o risco seja gerido de forma mais coerente.

No entanto, muitas das perdas nas organizações ainda são causadas por falhas de integração do risco no planeamento estratégico, por não existir ou existir de forma ineficaz uma gestão de riscos estratégicos e porque a estratégia não é orientada para o risco.

Assim, é importante que as organizações identifiquem, analisem e priorizem os riscos críticos mais significativos, assim como as fragilidades do seu controlo.

Os modelos apresentados de gestão corporativa e integrada de riscos do tipo ERM, aplicam-se às organizações em contexto de gestão estratégica, num processo contínuo que envolve todos os níveis organizacionais, integra uma visão de portfólio dos riscos mais significativos permitindo identificar, analisar e tratar aqueles que podem afetar a organização e a sua estratégia, e administrar o risco de acordo com o apetite e tolerância definidos.

Considera-se assim que o resultado de uma bem-sucedida gestão integrada dos riscos, alguns relacionados ou interdependentes, expressa-se em termos de conformidade, de segurança e em melhores tomadas de decisão, favorecendo a eficiência das operações e a eficácia da gestão estratégica.

3. A gestão dos riscos nos Ramos das Forças Armadas

No presente capítulo analisa-se a cultura e procedimentos de GR existentes nos Ramos das FFAA, tendo por base um conjunto de entrevistas realizadas a várias entidades dos Ramos (Apêndice I).

As questões formuladas, contidas no guião geral (questões 1 a 7 do Apêndice B) incidiram sobre a cultura de risco, designadamente quanto à existência de políticas, estratégias, organização e normas para a GR, sobre a GR nos processos de gestão estratégica e de edificação das capacidades militares, a ligação e o tratamento dos riscos operacionais (operações e gestão dos recursos financeiros, humanos, materiais e informacionais) relevantes para a estratégia, e o contributo da análise dos riscos nas atividades de auditoria e controlo interno.

A síntese das respostas obtidas a estas questões consta do Apêndice D.

3.1. Marinha

A Marinha não dispõe de uma política formal de GR. Existem práticas casuísticas de análise de risco ao nível da gestão estratégica, na gestão dos projetos de investimento, no planeamento e execução de algumas missões operacionais e no âmbito da função auditoria e controlo interno para os processos das áreas de gestão de recursos financeiros, humanos, materiais e informacionais (Marques, 2017).

Não havendo um departamento especializado para a área da GR, é o Estado-Maior da Armada (EMA), através da Divisão de Planeamento, que procede à avaliação dos riscos estratégicos. Por sua vez, os sectores funcionais procedem igualmente à avaliação dos riscos operacionais subjacentes à formulação dos seus objetivos (alinhados com os objetivos estratégicos), e no âmbito da auditoria interna, a Inspeção Geral da Marinha (IGM) e a Direção de Auditoria e Controlo Financeiro (DACF) realizam-se análises de risco aos processos das unidades auditadas (Marques; Daniel, 2017).

Não existindo normativo geral e específico sobre risco e GR, encontram-se no entanto referências a estes conceitos em algumas publicações, sendo de realçar a doutrina da Gestão Estratégica, no capítulo dedicado ao controlo da estratégia[9] (Marinha, 2015, pp.

[9] "O controlo é a fase em que se comparam os resultados obtidos com aqueles que se desejavam e que tinham sido planeados, apurando-se e analisando-se os desvios, de forma a detetar as suas causas e a introduzir medidas corretivas" (Marinha, 2015, p. 5.5).

5.1-5.15), as normas da Atividade Inspetiva, no capítulo dedicado à gestão do risco[10] (Marinha, 2011, pp. 5.1-5.7), a doutrina de Gestão de Projetos (Marinha, 2013) e o Plano de Gestão de Riscos de Corrupção e Infrações Conexas (PGRCIC) (Marinha, 2014) (Marques; Monteiro; Daniel, 2017).

A Marinha não tem uma estratégia para a GR e, por conseguinte, não tem portfólio de riscos nem uma matriz única de riscos. No entanto, apesar de não existirem objetivos estratégicos específicos que visem esta área, entende-se ser possível definir objetivos de nível operacional que visem a melhoria destas práticas e que estejam alinhados com objetivos estratégicos da perspetiva estrutural (processos internos) da atual Diretiva de Planeamento da Marinha (DPM) (Marinha, 2017) (Marques, 2017).

A Marinha dispõe de um instrumento dinâmico de análise estratégica de longo prazo, "A Marinha a 20 anos", que permite projetar e orientar para este período a evolução das suas componentes genética, estrutural e operacional, realizando-se neste âmbito análises de risco às ameaças identificadas ao ambiente estratégico, avaliando a probabilidade de ocorrência e o impacto para cenários prováveis da sua verificação e de acordo com critérios de risco definidos (Marques, 2017).

Para o mandato do Chefe do Estado-Maior da Armada, a Marinha adota o *Balanced Scorecard* (BSC) seguindo a inerente metodologia de planeamento estratégico. Os fatores de risco associados às ameaças e às oportunidades do ambiente estratégico são também identificados e analisados pelo EMA na fase de formulação da estratégia através de uma análise SWOT, sendo depois definidas estratégias para explorar as oportunidades e para eliminar, reduzir ou mitigar as ameaças. A execução das iniciativas estratégicas é acompanhada através de uma ferramenta aplicacional de gestão de projetos, o *Entreprise Project Management* (EPM), que contém funcionalidades de análise de risco (Marques, 2017).

A identificação pelo EMA dos riscos inerentes à execução da estratégia faz-se pela análise aos resultados que vão sendo reportados nos vários indicadores de gestão estratégica *(Key Performance Indicators* - KPI*)*, interpretando-se os eventuais desvios face às metas planeadas, e agindo-se em função disso (Marques, 2017).

[10] Apesar de serem normas que incidem sobre o processo e a matriz de GR a aplicar à atividade inspetiva, facilmente podem ser aproveitadas para um âmbito de aplicação geral e como tal ser integradas em doutrina específica do ramo na área da GR (Daniel, 2017).

Os riscos operacionais associados às operações e às atividades de gestão de recursos são geridos pelos respetivos sectores funcionais. A este nível, se existirem riscos que afetam a estratégia da Marinha, estes são identificados por via da monitorização periódica dos KPI sectoriais que estão alinhados com objetivos estratégicos. Não existem no entanto mecanismos expeditos de alerta caso se verifiquem desvios significativos face às metas, i.e. não há integração imediata da informação de risco (Marques, 2017) .

Na edificação das capacidades militares, a execução material e financeira dos vários projetos de investimento da Lei de Programação Militar (LPM) aprovada é acompanhada de processos de análise de risco. Utiliza-se o EPM para a gestão destes projetos, cujas normas seguem a doutrina da Gestão de Projetos da Marinha (Marinha, 2013), baseada nos guias *Project Management Body of Knowledge* (PMBOK) (PMI, 2013) e *NATO Risk Management* (NATO, 2010) (Marques, 2017).

A auditoria e controlo interno são essenciais para avaliar os processos, em especial os críticos que fazem parte da cadeia de valor. Neste âmbito, são efetuadas análises de risco durante as inspeções aos processos e às recomendações para prevenção e mitigação dos riscos de conformidade (Daniel, 2017).

Apesar das boas práticas apontarem para que o planeamento e a realização das auditorias e das inspeções tenham em conta os riscos existentes, alguns já avaliados, nem sempre tal tem sido aplicado (Daniel, 2017).

Fazem-se igualmente auditorias de acompanhamento à execução do PGRCIC, que contém, para os riscos nele identificados, um conjunto de ações a desenvolver pelos sectores funcionais com vista a reduzir ou a prevenir aquele tipo de riscos considerados de relevância estratégica por poderem lesar financeira e patrimonialmente a Marinha e afetar a sua reputação (Daniel, 2017).

Ao nível das responsabilidades financeiras, procura-se igualmente, através da DACF e dos serviços administrativos e financeiros dos sectores funcionais, prevenir os riscos associados à gestão dos recursos financeiros e patrimoniais, o que perante situações de incumprimento de normativo legal ou regulamentar aplicável, ou de incorreto registo contabilístico, podem degradar a qualidade do relato financeiro e de gestão, e prejudicar igualmente a imagem da Marinha.

3.2. Exército

O Chefe de Estado-Maior do Exército (CEME), na diretiva de planeamento estabelece como orientação específica juntar a GR às atuais ferramentas de gestão

estratégica de forma a "…ampliar a capacidade de verificação da consecução dos objetivos, do melhor apoio à sua realização, ou da reafectação de recursos ou prioridades para a sua finalização" (CEME, 2016, p. 27).

Estabelece-se ainda na mesma diretiva, que o conceito de risco "…é indissociável da atividade do Exército e afigura-se como crucial, face a um contexto de elevado dinamismo e mutabilidade, como se carateriza a realidade atual", acrescentando que "… a gestão de risco no Exército é informal e descentralizada, onde cada entidade gere os seus próprios riscos e, a descentralização da GR em cada uma das Entidades Sectoriais (ES) ajudou a criar uma consciência de prevenção de riscos no Exército. Contudo, num prazo mais alargado, a centralização e formalização de um processo de gestão de risco facilita uma visão global dos diferentes riscos e suas interdependências, pelo que o caminho natural do processo de gestão de risco é aquele que leva a uma maior centralização da função, até chegar à gestão integrada dos riscos" (CEME, 2016, p. 29).

Além das práticas contidas no processo de gestão estratégica, o Exército faz análise de riscos nas operações militares, na gestão de projetos de investimento e nas auditorias e inspeções às atividades e processos de gestão de recursos financeiros, pessoal, material e informação (Ribeiro; Rosa, 2017).

O Exército dispõe de um departamento especializado no Estado-Maior do Exército (EME), o Gabinete de Gestão de Informação e Conhecimento (GGIC), com responsabilidades na gestão centralizada dos riscos associados às várias fases do ciclo da gestão estratégica (Ribeiro, 2017).

Além das orientações específicas e conceitos relativos à GR constantes do capítulo já referido da diretiva de planeamento do CEME, inerente às fases de implementação, acompanhamento e controlo da estratégia (CEME, 2016, pp. 27-31), existem ainda referências normativas de procedimentos nesta matéria, designadamente a Norma de Gestão de Projetos (Exército, 2015), e a publicação doutrinária da componente operacional relativa ao Planeamento Tático e Tomada de Decisão[11] (Exército, 2007, pp. E1-E18).

A diretiva de planeamento do CEME estabelece uma linha de ação (na perspetiva dos recursos) que visa melhorar os processos de gestão de risco, fixando objetivos específicos

[11] Neste âmbito, a GR é integrada no planeamento de cada operação, na preparação e na condução das mesmas, sendo um "processo de identificação e controle das situações com vista á manutenção do potencial de combate e preservação dos recursos humanos, materiais e temporais" (Costa, 2017).

de natureza operacional e estratégica neste âmbito (CEMA, 2017, p. 24), pelo que se entende existir estratégia de GR.

O Exército tem um portfólio de riscos, considerando que este identifica todos os riscos com relevância para a estratégia, com "…a designação dos responsáveis pela sua gestão e as respostas adotadas para cada um e, o mapa dos riscos como representação gráfica dos riscos em função da probabilidade e impacto" (CEME, 2016, p. 30).

O Exército utiliza também a metodologia BSC e o EPM como ferramentas de gestão estratégica, querendo no entanto melhorar as práticas introduzindo a gestão da comunicação e a GR. Dispõem ainda de *dashboards* específicos, construídos a partir do EPM, que permitem acompanhar e balancear a performance e o risco (Ribeiro, 2017).

Os objetivos estratégicos e os objetivos operacionais das ES são definidos centralmente e constam da diretiva de planeamento do CEME (Ribeiro, 2017) .

A análise dos riscos estratégicos faz-se inicialmente aquando da formulação estratégica com base numa análise SWOT, sendo definidas estratégias para explorar as oportunidades e para eliminar, reduzir ou mitigar as ameaças. O produto final são os planos de ação ou planos de contingência que derivam da análise conjunta dos objetivos estratégicos e da identificação e avaliação dos riscos associados (Ribeiro, 2017).

Durante a execução da estratégia, os riscos são monitorizados de forma contínua pelo EME/GGIC através dos resultados dos indicadores e análise de desvios em relação às metas definidas, habilitando assim a adoção de eventuais medidas corretivas (Ribeiro, 2017).

Os riscos que não têm impacto estratégico são da responsabilidade das ES, no âmbito das suas atividades correntes, que os analisam e estabelecem para o efeito medidas de controlo e mitigação (Ribeiro, 2017).

No que respeita às capacidades militares, o procedimento é comum nos Ramos. Existem procedimentos de GR a montante, no planeamento de defesa, relacionando cenários, riscos e lacunas existentes, sustentados na doutrina do ciclo de planeamento de defesa nacional e da NATO, sendo depois materializada em planos de implementação de projetos de investimento. A execução material e financeira desses projetos pelo Exército é acompanhada em EPM, que contém funcionalidades específicas de análise de risco (Ribeiro, 2017).

No âmbito da auditoria e controlo interno, as atividades não são planeadas em função dos riscos existentes. No entanto, é possível identificar, com base em estatísticas de não

conformidades comuns a várias unidades, tendências de anomalias ou incidentes que podem constituir vulnerabilidades com relevância estratégica, o que pode levar ao reforço dos mecanismos de controlo para este tipo de riscos (Rosa, 2017).

A Inspeção-Geral do Exército (IGE) realiza inspeções gerais (no âmbito da segurança física das instalações e a processos logísticos, financeiros e de pessoal) e inspeções operacionais (conforme padrões NATO) orientadas para o treino operacional e certificação das Forças Nacionais Destacadas (FND). As recomendações identificadas para as não conformidades são objeto de análise de risco e de estimativa de custo de resolução. Fazem-se igualmente inspeções técnicas (p. ex.: Higiene e Segurança no Trabalho (HST)) e inspeções a processos transversais (p. ex.: alimentação, aquisições e saúde operacional). É entendimento que muitos dos riscos aqui identificados têm relevância estratégica (Rosa, 2017).

Sobre os riscos de corrupção e infrações conexas, o EME elabora o PGRCIC (Exército, 2016) e a IGE o relatório anual de execução (Rosa, 2017).

3.3. Força Aérea

A Força Aérea não dispõe de uma política formal de GR. Existem práticas consolidadas e formais específicas de GR nas áreas da segurança de voo, segurança física das instalações, do armamento e de proteção ambiental, e práticas casuísticas e informais de análise de risco no apoio à formulação estratégica, na gestão de projetos de investimento e em sede de auditoria e controlo interno aos processos das áreas de gestão de recursos financeiros, humanos, materiais e informacionais, numa ótica de conformidade face à legislação e aos procedimentos instituídos (Ferreira, 2017).

A Força Aérea não tem um portfólio de riscos, nem uma matriz única de risco. Não havendo um departamento especializado na GR, compete à Divisão de Planeamento do Estado-Maior da Força Aérea (EMFA), área responsável pelo processo de planeamento, a identificação e análise das ameaças e riscos relativos ao processo de formulação da estratégia, embora sem uma avaliação estruturada de cenários de impacto e de probabilidade de ocorrência de riscos, de priorização e de interligação destes (Ferreira, 2017).

A diretiva de planeamento da Força Aérea (CEMFA, 2016a) estabelece os objetivos estratégicos e define os objetivos operacionais e as atividades associadas. Em sede de planeamento, considera-se que os riscos são avaliados aquando da definição das atividades

que concorrem para a execução de cada um dos objetivos operacionais (que por sua vez estão alinhados com os objetivos estratégicos) (Ferreira, 2017).

Anualmente são definidos, em diretiva do CEMFA, os objetivos dessas atividades, os KPI e as respetivas metas (CEMFA, 2016b). Apesar de não existir uma estratégia de GR, entende-se que há atividades específicas que procuram eliminar e mitigar riscos (Ferreira, 2017).

Para planeamento e controlo de execução da estratégia, utiliza-se uma ferramenta própria (em folha de cálculo), o "Cockpit Organizacional", que relaciona objetivos (estratégicos e operacionais), atividades, ações, KPI, metas e recursos, para um regime de esforço anual planeado, em horas de voo. Esta ferramenta permite a monitorização e controlo da execução, analisando-se o reporte periódico de resultados dos indicadores de todas as áreas de atividade de modo a identificar desvios face às metas estabelecidas. Dessa avaliação, podem ser tomadas medidas corretivas e de controlo de forma a mitigar desvios (riscos) de planeamento. O "Cockpit organizacional" permite acompanhar e balancear a performance e o risco dos objetivos e das atividades através dos resultados dos vários KPI (Ferreira, 2017).

Na edificação das capacidades militares, a GR é materializada e acompanhada durante a execução material e financeira dos vários projetos da LPM aprovada. Utiliza-se igualmente o EPM para a gestão destes projetos, que contém funcionalidades de análise de risco (Ferreira, 2017).

A Força Aérea considera as funções auditoria e controlo relevantes para melhorar os processos e corrigir as não conformidades com vista a uma utilização mais eficiente dos recursos. A prevenção dos riscos associados à gestão e aplicação dos recursos financeiros e patrimoniais, que se refletem na qualidade do relato financeiro e de gestão, na conformidade e na imagem da instituição, é igualmente importante (Vasconcelos, 2017).

O planeamento das auditorias e das inspeções não é efetuado com base na informação de risco. São efetuadas inspeções de conformidade pela Inspeção-Geral da Força Aérea (IGFA) incidindo, entre outros, em processos das áreas financeira, logística e recursos humanos, a segurança de voo e a segurança física de uma forma geral. As não conformidades identificadas dão origem a recomendações, definidas em função das normas e riscos percecionados, e ao eventual reforço dos mecanismos de controlo. A IGFA pretende evoluir as suas práticas inspetivas diferenciando dois tipos de inspeções: as de

gestão, com um carácter geral e transversal, e as de execução, de âmbito mais temático (Vasconcelos, 2017).

A IGFA faz igualmente auditorias de acompanhamento à execução do PGRCIC (Força Aérea, 2014) que contém, para os riscos nele identificados, um conjunto de ações a desenvolver a nível operacional para redução ou prevenção daqueles riscos, que consideram de relevância estratégica por poderem lesar financeira e patrimonialmente a Força Aérea e por em causa a sua imagem (Vasconcelos, 2017).

3.4. Síntese conclusiva

Analisadas as componentes da cultura de risco nos Ramos conclui-se que, não obstante a sensibilidade e o interesse evidenciados durante as entrevistas sobre esta matéria, a cultura de risco é ainda insuficiente, em especial na Marinha e na Força Aérea, dada a ausência de politicas formais e de organização próprias para a GR, de estratégias especificas nesta área, e da existência de incipiente e disperso normativo sobre risco e GR.

O Exército apresenta um quadro de evolução mais favorável neste domínio, identificando-se na diretiva de planeamento do CEME uma estratégia para a GR que visa a centralização da função e a adoção da gestão integrada de riscos. Dispõe ainda de um núcleo específico no EME que trata a GR ao nível estratégico e de normas técnicas de GR aplicadas a áreas específicas (p. ex.: operações).

Ao nível estratégico e ao nível operacional, os Ramos estão a aplicar casuisticamente práticas de GR no planeamento estratégico, na gestão de projetos de investimento, nas operações militares, na gestão de recursos financeiros, humanos, materiais e informacionais, e ainda no âmbito das auditorias e inspeções. Tratam-se em regra de práticas não estruturadas, informais, conduzidas a nível descentralizado e sem integração da informação de risco.

Os Ramos revelam contudo uma boa consolidação dos instrumentos e práticas no domínio da gestão estratégica. A identificação e análise dos riscos estratégicos associados a ameaças e oportunidades são tidos em conta na formulação das estratégias, influenciando a sua implementação, sendo que na fase de execução o controlo desses riscos (os iniciais e os novos) e dos riscos operacionais com relevância para os objetivos estratégicos, fazem-se através da monitorização dos vários KPI, analisando-se os desvios face às metas estabelecidas.

Não existem instrumentos que permitam aos Ramos gerir de forma sistemática e integrada todos riscos com relevância estratégica.

Além da estratégia para a GR identificada no Exército, as estratégias em curso nos restantes Ramos preveem objetivos de melhoria da eficiência organizacional, podendo daí serem derivadas iniciativas (estratégicas) que incrementem a cultura de risco e as respetivas práticas.

4. A aplicação da gestão estratégica e integrada de riscos aos Ramos das Forças Armadas

O presente capítulo é dedicado à implementação de uma metodologia ERM nos Ramos das FFAA que permitirá a gestão estratégica e integrada de riscos.

A adequabilidade desta iniciativa decorre da avaliação efetuada às práticas de GR identificadas no capítulo anterior, assim como da análise às respostas obtidas para as questões 8 a 10 do guião geral para entrevistas (Apêndice C) cuja síntese consta do Apêndice E.

No quadro das estratégias em curso nos Ramos, procurar-se-á também avaliar da aceitabilidade desta iniciativa alinhando-a com objetivos que visam a melhoria da eficiência organizacional e dos processos.

4.1. Enquadramento

Colocada a questão quanto à forma de melhorar a GR, a Marinha entende ser necessário aumentar a cultura de risco na instituição, através da definição de uma política e de uma estratégia específicas, orientadas superiormente, e operacionalizar a implementação de metodologias de gestão integrada de riscos, adiantando poder ser adequada a edificação de uma "capacidade de gestão de risco" em processo semelhante à atual "capacidade de gestão de projetos" (Marques; Daniel; Monteiro, 2017).

Com referência às normas da Atividade Inspetiva, a Marinha considera que "a adoção de um modelo de gestão do risco irá contribuir para uma utilização mais eficiente dos recursos dentro da organização e para a melhoria do processo de planeamento, de estabelecimento de prioridades e de tomada de decisão nos diferentes níveis hierárquicos e em todas as áreas funcionais da Marinha, permitindo desta forma melhorar a eficiência na gestão dos recursos e agilizar o rastreio e a resolução das situações irregulares detetadas". (Marinha, 2011, p. 5.1; Daniel, 2017).

Considera ainda que "para além da identificação dos principais fatores de risco, este modelo de gestão permitirá ainda conhecer e priorizar os riscos já existentes, estimar os custos associados à sua resolução ou mitigação e implementar as medidas de controlo que se venham a revelar mais adequadas em cada situação." (Marinha, 2011, pp. 5.1 cit. por Daniel,2017).

No caso do Exército, a atual diretiva de planeamento do CEME estabelece que "… a centralização e formalização de um processo de gestão de risco facilita uma visão global dos diferentes riscos e suas interdependências, pelo que o caminho natural do processo de

gestão do risco é aquele que leva a uma maior centralização da função, até chegar à gestão integrada dos riscos" (CEME, 2016, p. 29 cit. por Ribeiro,2017).

Os riscos estratégicos podem ser identificados tanto na definição como na implementação da estratégia, sendo que no primeiro caso podem limitar as estratégias a ser seguidas e no segundo inviabilizar a própria estratégia definida (Ribeiro, 2017).

Ainda segundo Ribeiro, uma avaliação de desempenho e uma monitorização contínua dos riscos estratégicos que antecipe acontecimentos relevantes, confere mais eficiência e flexibilidade à ação do Exército caso as alterações ambientais venham a afetar de forma muito significativa os objetivos estratégicos, podendo determinar a adoção de medidas corretivas, a reafectação de recursos ou a alteração de prioridades (Ribeiro, 2017).

Quanto à Força Aérea, foi manifestada igualmente a ideia de que a GR deve ser integrada na cultura do Ramo com uma política eficaz e um programa conduzido pela gestão de topo, e que a melhoria destas práticas pode passar pela implementação de metodologias de gestão integrada de riscos (Ferreira; Vasconcelos, 2017)

Assim, com base na análise à cultura de risco e às práticas seguidas no âmbito da GR, e considerando ainda as respostas obtidas, procurou-se através de uma análise SWOT identificar as principais potencialidades, vulnerabilidades, oportunidades e ameaças, determinantes para a definição de uma iniciativa de implementação da metodologia ERM no Ramos.

Esta análise simples, ilustrada na Figura 8, salienta como potencialidades dos Ramos, entre outras: a consolidação das práticas de gestão estratégica; as prioridades da gestão na melhoria da eficiência organizacional; a sensibilidade da gestão superior para as matérias do risco e GR, e ainda a existência de áreas específicas dedicadas às funções de auditoria e controlo interno que têm um papel decisivo no aperfeiçoamento dos processos.

Como vulnerabilidades, é salientada a insuficiente cultura de risco na gestão (mais evidente na Marinha e na Força Aérea) e a falta de integração da informação de risco.

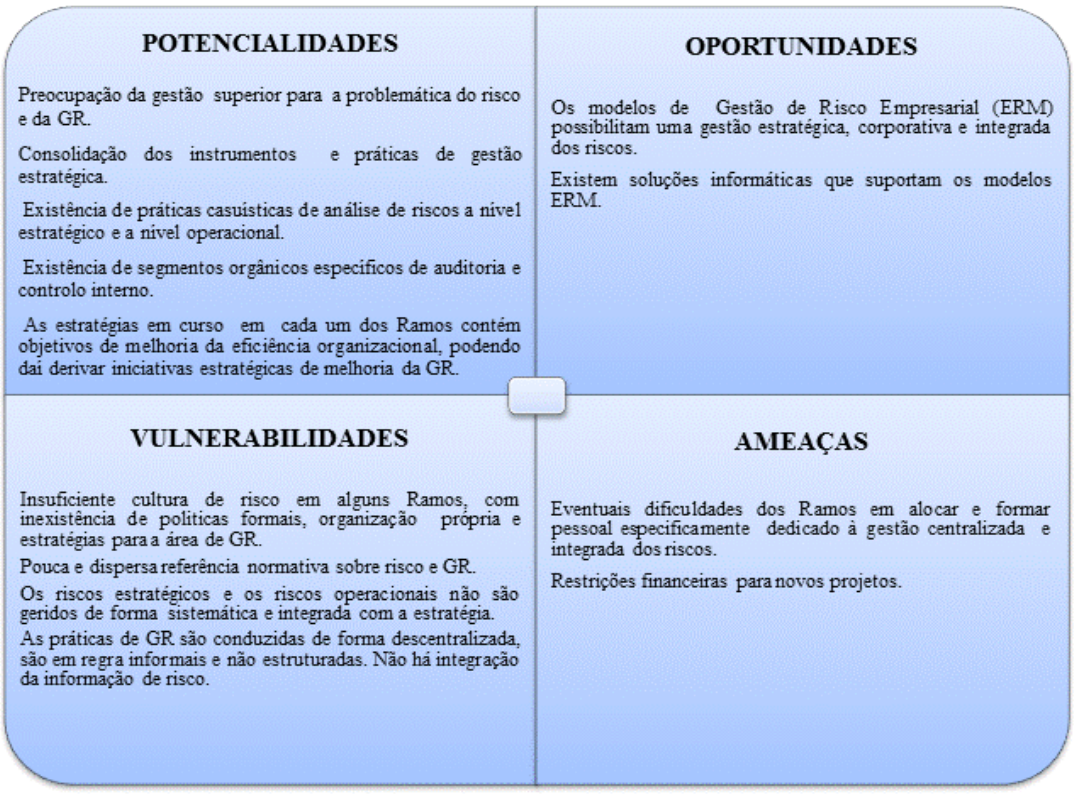

Figura 8 - SWOT da Gestão do Risco nos Ramos das FFAA

Fonte: Autor (2017)

Assim, considerando a oportunidade (e vantagens) conferidas pelos modelos e sistemas aplicacionais de ERM, afigura-se adequado e aceitável formular uma iniciativa comum aos Ramos, que vise a implementação da gestão estratégica, integrada e corporativa de riscos, a suportar por uma solução organizativa e tecnológica exequível no contexto das atuais limitações em matéria de recursos humanos e financeiros.

O alinhamento estratégico desta iniciativa obter-se-ia da seguinte forma:

- Na Marinha, alinhada com o objetivo estratégico da DPM 2017, "OE5 – Aperfeiçoar a eficiência nos processos e na gestão de recursos" (Marinha, 2017);
- No Exército, alinhada com o objetivo estratégico da diretiva de planeamento do CEME, "OE8-Melhorar a obtenção e gestão dos recursos do Exército", objetivo operacional "OO84- Consolidar as metodologias, as ferramentas e o processo de decisão", e correspondente linha de ação: "LA841 – Consolidar os processos de planeamento e gestão estratégica de forma a melhorar o controlo da execução das atividades, antever riscos e decidir com oportunidade" (CEME, 2016);
- Na Força Aérea, com um alinhamento distribuído pelos seguintes objetivos operacionais e atividades da Diretiva de Planeamento da Força Aérea de 2016: objetivo operacional "OB3 – Proporcionar um apoio logístico com qualidade e

eficiência" para as atividades "A3.4 – Gestão de comunicações, sistemas e tecnologias de informação" e "A3.5 – Proteção ambiental"; objetivo operacional "OB6 – Assegurar o controlo e a segurança das atividades" para as atividades "A6.1 - Controlo e Inspeção", "A6.2 -Prevenção e investigação de acidentes" e "A6.3 – Segurança militar"; e objetivo "OB10 – Administrar com eficiência, eficácia e economia os recursos financeiros" para a atividade "A10.3 – Auditoria financeira e patrimonial" (CEMFA, 2016b).

Como visto anteriormente (capítulo 2), um processo de gestão integrada de riscos suportado por uma metodologia ERM ajudará no processo de decisão estratégico, no planeamento e na afetação de recursos.

O ERM vai assim permitir aos Ramos a identificação dos riscos e a partilha interna dessa informação, a aplicação de estratégias combinadas de GR, a determinação de prioridades de ação estratégica e operacional, a discussão dos tipos e níveis de risco aceitáveis (tendo em conta o apetite e tolerância definidos para cada risco) e um suporte para o planeamento de médio e longo prazo.

Assim, para esta iniciativa descrevem-se seguidamente as fases de implementação de uma metodologia ISO-ERM, cuja síntese se apresenta no Apêndice H.

4.2. Planeamento da metodologia ERM

Como ponto prévio, importa referir que a implementação da metodologia ERM tem de ser compreensiva pois trata-se de um processo progressivo cujos resultados não se obtém no imediato.

Em primeiro lugar, é necessário que os Ramos definam os objetivos a atingir com o modelo e que são influenciados obviamente pelas várias expectativas de gestão.

Podem-se assim definir os objetivos da GR da seguinte forma:

- Proporcionar à gestão superior do Ramo um processo de decisão e de planeamento que seja informado por uma adequada avaliação dos riscos estratégicos;
- Proporcionar à gestão intermédia (Sectores Funcionais da Marinha e Entidades Sectoriais/Comandos Funcionais do Exército e Força Aérea) e à gestão operacional (Unidades, Estabelecimentos e Órgãos (UEO)) um processo de decisão informado por uma adequada avaliação dos riscos operacionais que tenham impacto estratégico;

- Aderir aos princípios e às melhores práticas de GR que reforcem a cultura de risco nos Ramos, estimulem a inovação e o pensamento baseado no risco.

Estes objetivos, assim como outras orientações associadas à arquitetura, estratégia e protocolos/normas sobre risco, seriam incluídos numa política de GR do Ramo, contendo: (FERMA, 2010)

- Os objetivos da GR e do correspondente controlo interno (governança);
- Uma avaliação da cultura de risco existente e do sistema de controlo interno;
- Uma declaração quanto à atitude do Ramo face ao risco (estratégia de risco);
- O nível e a natureza do risco que é considerado aceitável (apetite ao risco);
- A definição da organização para a GR (arquitetura de risco);
- A alocação de recursos financeiros, humanos, materiais e informacionais à GR;
- A atribuição de regras e responsabilidades pela GR;
- Os procedimentos para a identificação e análise de riscos (avaliação do risco);
- A lista de documentos para a análise e relato de riscos (protocolos de risco);
- Os requisitos para a mitigação de riscos e os mecanismos de controlo (resposta ao risco);
- Os critérios de monitorização e de revisão de riscos;
- A identificação das áreas chave de risco e dos riscos prioritários para a gestão.

Os recursos necessários para implementar uma política de GR seriam definidos para cada nível de gestão, o que obrigaria a considerar as atividades de GR em sede de planeamento estratégico, planos de atividades e processo orçamental (FERMA, 2010).

Apesar das áreas específicas de risco operacional (p. ex.: financeira, tecnologias de informação, segurança física, continuidade do negócio, gestão ambiental, HST) serem guiadas por políticas, normas e procedimentos próprios, considera-se que as mesmas devem fazer parte do modelo de gestão integrada de riscos (FERMA, 2010).

Considerando a dimensão dos Ramos e a existência de vários níveis de gestão, as responsabilidades em torno da GR poderiam ser atribuídas conforme modelo descrito na Tabela 3.

Tabela 3 - Matriz de responsabilidades pela gestão do risco nos Ramos das FFAA

Níveis	Responsabilidades
Chefe do Estado-Maior	– Aprovar a política de GR; – Definir o nível e tipo de risco aceitável (o "apetite ao risco"); – Estabelecer a organização para a GR; – Compreender os riscos mais significativos e prioritários para a gestão; – Gerir o Ramo em situações de crise.
Estado-Maior	– Elaborar a política de GR e mantê-la atualizada; – Documentar a política interna de riscos e a organização para a GR; – Compilar a informação de risco para apoio à decisão.
Sectores Funcionais / Entidades Sectoriais e UEO dependentes	– Desenvolver uma cultura de risco dentro do sector e nas UEO; – Colaborar com o Estado-Maior no estabelecimento específico de políticas de risco; – Desenvolver planos especificos de contingência e de recuperação; – Aceitar as metas de GR que decorrem da estratégia de risco do Ramo; – Garantir a implementação das recomendações de melhoria dos processos que têm riscos identificados; – Identificar e reportar alterações de circunstância na envolvente de risco; – Participar nas investigações a incidentes ou quase incidentes.
Inspeção-Geral e outras UEO com responsaabilidades de auditoria e controlo interno	– Desenvolver programas de auditoria interna baseados no risco; – Auditar os processos de risco do Ramo; – Coordenar as medidas de GR e controlo interno; – Reportar a eficiência e eficácia do controlo interno
As pessoas individualmente	– Compreender, aceitar e ajudar a implementar os processos de GR; – Reportar ineficiências e controlos desnecessários; – Reportar os incidentes e os quase incidentes; – Cooperar na gestão e investigação de incidentes.

Fonte: Autor, adaptado de (FERMA, 2010)

Ainda atendendo à natureza, dimensão[12] e estrutura organizativa dos Ramos, entende-se que a coordenação da gestão do risco deverá ser atribuída a um departamento específico.

[12] Em organizações de menor dimensão esta função de GR acaba pode ser atribuída apenas a um gestor em regime de tempo parcial, ou total.

Para a Marinha, a área considerada mais adequada para assumir essa coordenação seria o órgão de governação da "capacidade de gestão do risco", a criar conforme anteriormente sugerido, podendo a decisão recair no EMA[13] (ou na IGM) que contaria necessariamente, face às limitações em pessoal, com o apoio de especialistas, colocados em várias UEO, para atividades e processos internos comuns (Daniel, 2017).

Para o Exército, a coordenação seria do EME através da estrutura já existente, o GGIC (Ribeiro; Rosa, 2017).

Para a Força Aérea, a coordenação e o controlo poderia ser da IGFA, envolvendo-se sempre o EMFA em termos de produção e validação de normativo (Vasconcelos, 2017).

4.3. Implementação da metodologia ERM

O processo de GR da metodologia ISO-ERM, representado na Figura 7 (capítulo 2.3.2), pode ser aplicado no planeamento estratégico e controlo de gestão, na gestão dos projetos de investimento e nas decisões correntes de funcionamento dos Ramos.

O processo de GR deve assim integrar a gestão dos Ramos, beneficiando os processos, clarificando os objetivos e as metas. Os riscos seriam avaliados e mitigados para alcançar objetivos operacionais e de projeto, e alinhar as prioridades estratégicas (FERMA, 2010).

4.3.1. Estabelecimento do contexto

De acordo com a ISO, o contexto confirma o objeto da gestão integrada de risco, os seus objetivos e metas e os objetivos e metas de avaliação do risco propriamente dita. Identifica os *stakeholders*[14], os constrangimentos e limitações impostas à execução da estratégia (ISO, 2013).

Segundo a ISO, estabelecendo o contexto "...a organização articula os seus objetivos, define os parâmetros internos e externos que têm de ser tidos em conta quando se gere o risco, e fixa um nível e critério de risco para o restante processo" (ISO, 2009a, p. 15).

Assim, importa antes de mais definir qual o objeto de análise de risco em cada um dos Ramos. Se incide apenas sobre o plano estratégico, ou se abrange também os planos operacionais/sectoriais, os projetos e os processos. Independentemente desta definição, é essencial garantir que os objetivos operacionais e metas estejam sempre alinhados com a estratégia (ISO, 2013).

[13] O EMA é o atual órgão de governação da gestão estratégica e da capacidade de gestão de projetos.
[14] Podem ser fonte de risco pelo que importa proceder à sua análise.

No estabelecimento do contexto, a missão, a visão e os valores, como conceitos estruturantes das estratégias dos Ramos, devem também estar presentes como pontos de referência para focalizar e ajudar a resolver eventuais divergências (ISO, 2013).

As disposições legais, regulamentares e as políticas são também parte do contexto em que o risco tem lugar, não servindo só para identificar riscos (como limitações com prazos, riscos processuais, de conformidade e de gestão de recursos), servem também como guião para a implementação de estratégias de mitigação (ISO, 2013).

Os contextos das áreas específicas de risco operacional exigem análises separadas e especializadas, no entanto, como referido anteriormente, estes planos de gestão de riscos devem integrar o modelo de gestão integrada.

4.3.2. Identificação do risco

A apreciação dos riscos numa organização envolve quase sempre a identificação, a avaliação e a priorização destes riscos (ISO, 2009a).

A identificação dos riscos é uma das partes mais importantes do processo de GR, podendo ser utilizadas pelos Ramos diversas técnicas para o efeito, conforme exemplos da Tabela 4.

Tabela 4 - Técnicas para identificação de riscos

Técnicas	Descrição
Questionários ou entrevistas	Fazer questionários ou entrevistas para recolha de informação que permita identificar os riscos mais significativos.
Workshops* e/ou *brainstormings	Discutir e partilhar ideias sobre os eventos de risco que podem afetar os objetivos e a relação de dependências do risco.
Inspeções e auditorias	Inspeções a instalações e a atividades e auditorias de conformidade sobre sistemas e procedimentos.
Análise de processos (Fluxogramas)	Análise dos processos a fim de identificar etapas e componentes críticos do sucesso destes.
Análises SWOT e PESTLE	Análise SWOT; Análise PESTLE (*Political, Economical, Social, Tecnological, Legal and Enviroment*) são, entre outras, técnicas de aproximação mais estruturadas e de identificação dos riscos.

Fonte: Autor, adaptado de (FERMA, 2010)

Embora a simples caraterização do risco seja por vezes suficiente para a sua identificação, circunstâncias há em que é necessária uma descrição mais detalhada para melhor compreensão no processo de apreciação e para registo.

A Tabela 5 lista alguns atributos úteis que ajudam os Ramos nessa caraterização.

Tabela 5 - Descrição detalhada do risco

Atributo	Descrição
Nome do risco	Identificador do risco.
Âmbito do risco	Âmbito do risco com indicação de possíveis eventos associados.
Natureza do risco	Classificação do risco. Descrição como ameaça, oportunidade ou incerteza.
Stakeholders	Expetativas dos *stakeholders* internos e externos.
Avaliação do risco	Probabilidade e gravidade do evento. Possível impacto ou consequências.
Histórico	Histórico de incidentes associados ao tipo de risco.
Apetite ao risco e tolerância ao risco	Atitude perante o risco (apetite ao risco, tolerância ou limites ao risco). Fixação de metas de controlo tendo em conta o efeito de potenciais perdas.
Resposta ao risco/ controlo	Existência de mecanismos e atividades de controlo. Procedimentos de monitorização (e revisão) da performance do risco.
Potencial de melhoria do risco	Análise custo/ benefício de eventuais melhorias de controlo. Recomendação e prazo para implementação dessas melhorias. Responsabilidade pela implementação.
Estratégia de desenvolvimento	Responsabilidade no desenvolvimento da estratégia para o risco. Responsabilidade pela auditoria de conformidade.

Fonte: Autor, adaptado de (ISO, 2009a)

Como referido ao longo desta investigação, os riscos podem ser gerados por fatores internos e externos. Na Tabela 6 identificam-se alguns exemplos de fatores geradores de riscos operacionais, riscos financeiros e riscos de reputação aplicáveis aos Ramos.

Tabela 6 - Fatores de risco nos Ramos das FFAA - exemplos

Tipo de Risco	Fatores	
	Internos	Externos
Riscos operacionais	– Recrutamento do pessoal – Formação do pessoal – Gestão do pessoal – Apoio sanitário – Manutenção dos meios operacionais; – Manutenção de infraestruturas – Gestão dos contratos – Segurança nas operações – Segurança no trabalho – Segurança das instalações – Segurança da informação – Tecnologias informação	– Alterações ao ambiente de segurança e defesa – Rotura cadeia logística – Evolução tecnológica – Desastres ambientais ou catástrofes naturais
Riscos financeiros	– Controlo interno – Corrupção e riscos conexos – Registos contabilísticos	– Orçamento e níveis de financiamento – Normas legais – Regras orçamentais ou contabilísticas
Riscos de reputação	– Diagnóstico do ambiente – Qualidade da informação – Corrupção e riscos conexos – Comunicação estratégica – *Accountability*	– Opinião pública – Entidades de regulação – Entidades de fiscalização

Fonte: Autor, adaptado de (COSO, 2004; FERMA, 2010)

A classificação destes riscos deve ser complementada com os riscos estratégicos que embora possam ter tratamento separado, estão interligados com os riscos identificados (COSO, 2004; FERMA, 2010).

4.3.3. Análise do risco

Identificados os riscos, importa proceder à sua análise.

Recordando a ISO, a análise dos riscos é um processo de cálculo da probabilidade e do seu impacto. A probabilidade é a possibilidade do risco identificado poder ocorrer. A consequência é o nível de gravidade dos seus efeitos nos objetivos e metas (ISO, 2009a).

A priorização dos riscos decorre da análise em termos da probabilidade de ocorrência e possível impacto, podendo ser feita de forma quantitativa ou qualitativa[15] (ISO, 2013).

A probabilidade e o impacto podem ser analisados de forma qualitativa utilizando escalas gradativas e matrizes de avaliação do risco, conforme o modelo que se exemplifica na Figura 9, de configuração dupla (ameaças e oportunidades).

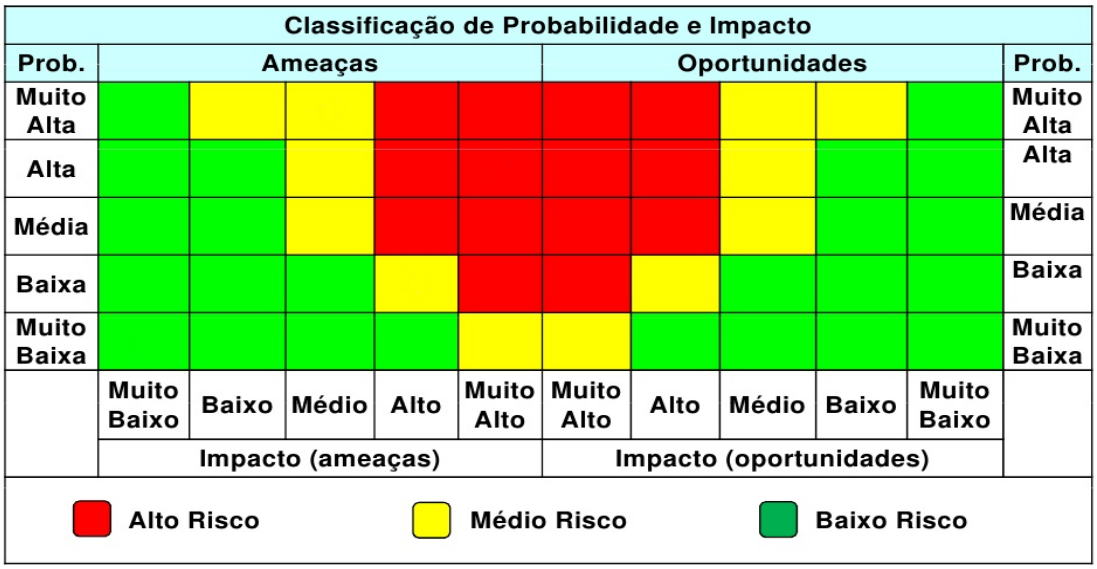

Figura 9 - Matriz de análise do risco

Fonte: (PMI, 2013, p. 331)

O resultado da análise é a classificação do risco, que pode ser: "Alto", "Médio" ou "Baixo".

Para os Ramos, à semelhança das restantes organizações, a importância da análise de risco inerente a cada objetivo, atividade ou processo, será determinar a natureza do evento, as causas e os impactos (ISO, 2013).

Não deixa contudo de ser um processo complexo, pelos fatores subjetivos que envolve, como o julgamento de quem avalia, a influência do ambiente interno e externo e a incerteza do futuro (ISO, 2013).

Os Ramos podem ainda dispor de registos de riscos já classificados baseados em histórico de eventos, que ajudam a identificar as melhores estratégias de resposta perante eventos similares. Um catálogo prévio é um instrumento expedito muito usado em auditoria e que visa a eficiência dos processos (ISO, 2013).

[15] Raramente se exige a aplicação de modelos matemáticos, em vez disso fazem-se estimativas subjetivas.

4.3.4. Avaliação do risco

A avaliação do risco terá de ser sempre exigida a nível estratégico como parte do processo de tomada de decisão estratégica[16] para explorar oportunidades e mitigar as ameaças, e a nível operacional, referida às operações, atividades e projetos a desenvolver (ISO, 2013).

Avaliar os riscos em cada Ramo é verificar a existência de mecanismos de controlo, definir a tolerância aos riscos e as ações de resposta. O objetivo é chegar a uma decisão de como responder aos riscos, considerando sempre análises e critérios de racionalidade custo/ benefício (ISO, 2013).

É caraterizar em termos qualitativos se existem mecanismos de controlo que ajudem a mitigar o risco em questão (p. ex.: "Não existente", "Inadequado", "Adequado", "Robusto" ou "Excessivo") (ISO, 2013).

É também caraterizar o risco em relação ao nível de tolerância (p. ex.: "Inaceitável", "Aceitável com tratamento" ou "Aceitável")[17]. A tolerância é inaceitável quando se assume que o risco deve ser evitado. É aceitável, se for inevitável, proibitivo ou impossível de tratar (ISO, 2013).

O apetite e a tolerância ao risco servem os objetivos, as atividades, os processos e a auxiliam na alocação de recursos, orientando a organização e os meios necessários para responder e monitorizar os riscos de forma eficaz (ISO, 2013).

4.3.5. Tratamento do risco

Tratar o risco é identificar a resposta a tomar em conjunto com a capacidade do Ramo em suportar esse risco, vista numa ótica de resiliência organizacional[18].

As cores assinaladas na matriz da Figura 10 ajudam a indicar as prioridades a dar no tratamento do risco.

[16] Como forma de garantir que a avaliação dos riscos é feita deverá figurar (como anexo) na documentação estruturante da estratégica do Ramo.

[17] Para classificar os riscos quanto aos níveis de tolerância, podem-se desenvolver estudos comparativos para determinar a significância dos riscos, sendo que a natureza desses estudos depende do tipo de risco.

[18] Referindo-se à norma *British Standard for Organizational Resilience* (BS 65000), Kerr (2017) define a resiliência organizacional como " a capacidade de uma organização para antecipar, preparar-se, responder e se adaptar a mudanças incrementais e ruturas súbitas, a fim de sobreviver e prosperar".

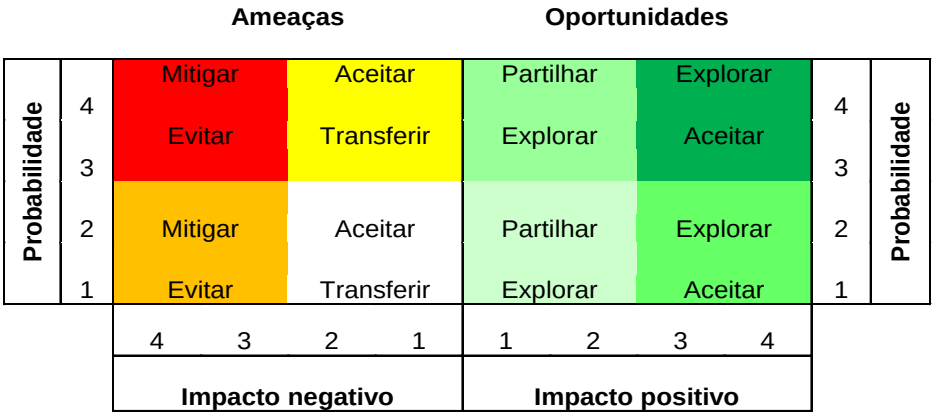

Figura 10 – Matriz de tratamento do risco

Fonte: Autor, adaptado de (Maia & Chaves, 2016)

Se o impacto do risco afetar a estratégia da organização, ou seja a missão, a visão ou os objetivos estratégicos, é sugerido mitigar ou evitar os riscos negativos (ameaças) e partilhar, aceitar ou potenciar os riscos positivos (oportunidades) (Maia & Chaves, 2016).

Se o risco é inaceitável ou aceitável com tratamento, é recomendável uma estratégia de mitigação. Evitar o risco, se inaceitável, é eliminá-lo não fazendo por exemplo a ação onde este ia ocorrer primariamente, no entanto há que avaliar se essa decisão vai originar outro tipo de risco (p. ex.: risco de reputação) (ISO, 2013).

Para uma melhor avaliação do nível de risco associado a uma iniciativa que concorre para um dado objetivo estratégico e assim serem determinadas ações que procurem reduzir o nível de incerteza na sua concretização, é útil verificar o alinhamento estratégico da iniciativa e a sua probabilidade de sucesso, podendo para tal serem aplicadas matrizes de decisão como a exemplificada na Figura 11.

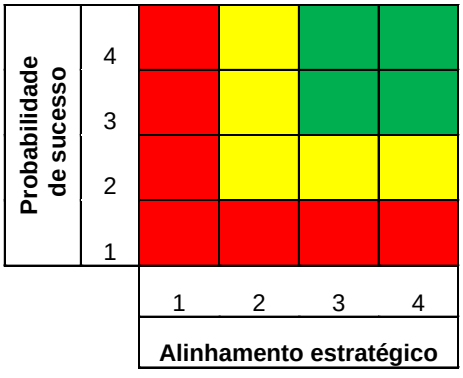

Figura 11 - Matriz de decisão estratégica

Fonte: Autor, adaptado de (Maia & Chaves, 2016)

Este alinhamento permitirá ao decisor escolher quais as iniciativas que melhor servem os objetivos e que têm possibilidade de serem bem-sucedidas (Maia & Chaves, 2016).

Pôr em prática estratégias de prevenção e mitigação do risco é combater as causas, diminuindo os impactos ou preparando planos de contingência. Há que estar preparado para responder a questões do tipo:

- Como podemos prevenir um evento de acontecer?
- E se acontecer, como podemos limitar os danos retomando a atividade e prosseguindo os objetivos? (ISO, 2013)

Há assim que estimular a discussão, ter uma boa caraterização e documentação do risco e chamar a atenção do decisor para o mesmo, procurando que sejam ajustadas as políticas de afetação de recursos (Maia & Chaves, 2016).

Como referido anteriormente, as ações de tratamento do risco devem ser objeto de avaliação custo/ beneficio. Por vezes, soluções simples baseadas em controlos legais, administrativos, regulamentos e políticas podem ajudar os Ramos a mitigar muitos riscos associados a atividades correntes, reduzindo-os para níveis toleráveis (ISO, 2013).

Deste modo, há que manter atualizados estes mecanismos de controlo e pôr em prática ações corretivas sempre que necessário, procurando a conformidade. Neste âmbito, fica uma vez mais evidente o importante papel da função auditoria e controlo interno para a verificação e validação dos níveis de conformidade da organização face a normas e políticas em vigor (ISO, 2013).

Além dos objetivos estratégicos e de conformidade, o tratamento dos riscos nos Ramos deve ainda abranger ações de prevenção e mitigação associadas a outros fatores que de uma forma direta ou indireta têm relevância na execução das estratégias, de que são exemplos os fatores geradores de riscos operacionais, financeiros e de reputação, identificados anteriormente na Tabela 6.

Para estes, são apresentados, no Apêndice F, alguns exemplos de ações que auxiliam na prevenção e mitigação de potenciais riscos associados.

4.4. Monitorização e revisão

Para que haja compromisso para uma adequada gestão integrada de riscos, há que rever regularmente a estratégia, avaliar os atuais e potenciais riscos e implementar mecanismos de controlo para reduzir esses riscos (FERMA, 2010).

A informação de risco deve ser gerida regularmente, para isso há que monitorizar.

Sabe-se que os riscos podem mudar, podendo ser necessário rever a sua classificação e apreciação, e novos riscos podem aparecer. Recomenda-se assim que haja uma atualização periódica da informação de risco e do seu registo (FERMA, 2010).

De facto, esse registo não pode ser um registo estático dos riscos mais significativos dos Ramos. Ele tem de ser visto como um plano de ação que inclui detalhes dos controlos correntes e das ações complementares que vão sendo planeadas e executadas (FERMA, 2010).

Além de monitorizar a eficiência dos controlos existentes, há que avaliar o mérito da implementação das ações adicionais através de adequadas análises custo-benefício (FERMA, 2010).

Tal como os sistemas de controlo correntes, também as ações adicionais devem ser auditáveis permitindo às várias entidades dos Ramos com responsabilidades de auditoria e controlo interno, monitorizar todos os mecanismos de controlo e planear as próprias auditorias e inspeções com base na avaliação dos riscos.

Monitorizar o risco de continuidade do negócio é essencial para evitar disrupção, pelo que importa manter sempre atualizados os planos de continuidade de negócio e os planos de *disaster recovery* (FERMA, 2010).

As mudanças operadas na organização e no seu ambiente de funcionamento devem ser igualmente identificadas e originar as correspondentes modificações nos protocolos e procedimentos (FERMA, 2010).

A monotorização deve incidir também sobre a evolução da cultura de risco e sobre a estrutura de GR existentes, verificando o nível de alinhamento das atividades de GR com as restantes atividades corporativas de gestão da organização. Deve apurar-se se as medidas adotadas alcançaram o resultado pretendido, se os protocolos adotados foram eficientes, se houve suficiente informação disponível para a avaliação do risco, se a melhoria do conhecimento está a ajudar a obter melhores decisões, e se há lições aprendidas para futuras avaliações e mecanismos de controlo (FERMA, 2010).

4.5. Aprendizagem e comunicação

A GR exige um ambiente de grande liderança, um envolvimento de todos os níveis organizacionais e uma cultura de aprendizagem, de responsabilidade pelas ações e uma boa comunicação dos assuntos de risco (FERMA, 2010).

Uma experiência de ERM nos Ramos envolverá também a necessária revisão de indicadores de performance e a medição do contributo da GR para o sucesso das estratégias.

Como dispõe a ISO, comunicar e consultar com os *stakeholders* internos e externos deve verificar-se em todas as fases do processo de GR. Esta é proactiva e inclusiva se envolver todos aqueles que compreendem os riscos e são capazes de os gerir (ISO, 2009a).

A "Comunicação e consulta" devem ser usadas para reportar riscos para os níveis de decisão superior (interno ou externo ao Ramo), mas também para passar informação descendente sobre as decisões de execução respeitantes à tolerância ao risco e às prioridades de ação (ISO, 2009a).

Segundo Hopkin, a informação sobre os riscos não deve ser analisada isoladamente mas integrada com a restante informação de gestão. A inclusão no mesmo relatório de gestão da performance, de indicadores de gestão estratégica e de monitorização dos riscos (estratégicos), fornece uma visão de grande latitude sobre os objetivos, os riscos associados e a sua gestão (Hopkin, 2012).

4.6. Sistemas de *Governance, Risk and Compliance*

A GR e o planeamento estratégico apresentam diferenças que tornam difícil a sua integração no mesmo sistema de controlo (Oliveira, 2013).

Segundo este autor, as ferramentas de gestão estratégica do tipo BSC apesar de apropriadas para traduzir a estratégia em ação e focar a atenção nos KPI, têm limitações a lidar com a incerteza devido à natureza difusa e não quantificável dos riscos estratégicos. A avaliação da performance preocupa-se com os resultados de curto prazo da estratégia, enquanto a GR tem uma perspetiva mais alargada focando a atenção nos riscos estratégicos de longo prazo (Oliveira, 2013).

Assim, utilizar ferramentas como o BSC[19] para ligar o processo de GR a correspondentes medidas de gestão de performance pode não ser a solução mais adequada. Contudo, as práticas formais de planeamento e controlo de gestão, de avaliação da performance e de GR podem levar ao uso de outros sistemas complementares de que são exemplo os atuais sistemas de *Governance, Risk and Compliance* (GRC).

Estes sistemas aplicacionais suportam as metodologias ERM aqui descritas (COSO - ERM e ISO-ERM), abrangem os processos da GR e dispõem de funcionalidades de identificação inicial de riscos e do subsequente *workflow* que permite a análise, avaliação, mitigação e monitorização dos riscos e a gestão de incidentes (BWise, 2017).

[19] Em exploração na Marinha e Exército.

Segundo a Consultora Bwise (2017) estes sistemas servem para integrar políticas, processos e controlos, e para criar estruturas colaborativas para ajudar no processo de apoio à decisão.

Na Figura 12 identificam-se as principais funcionalidades associadas às componentes de *Governance, Risk and Compliance*.

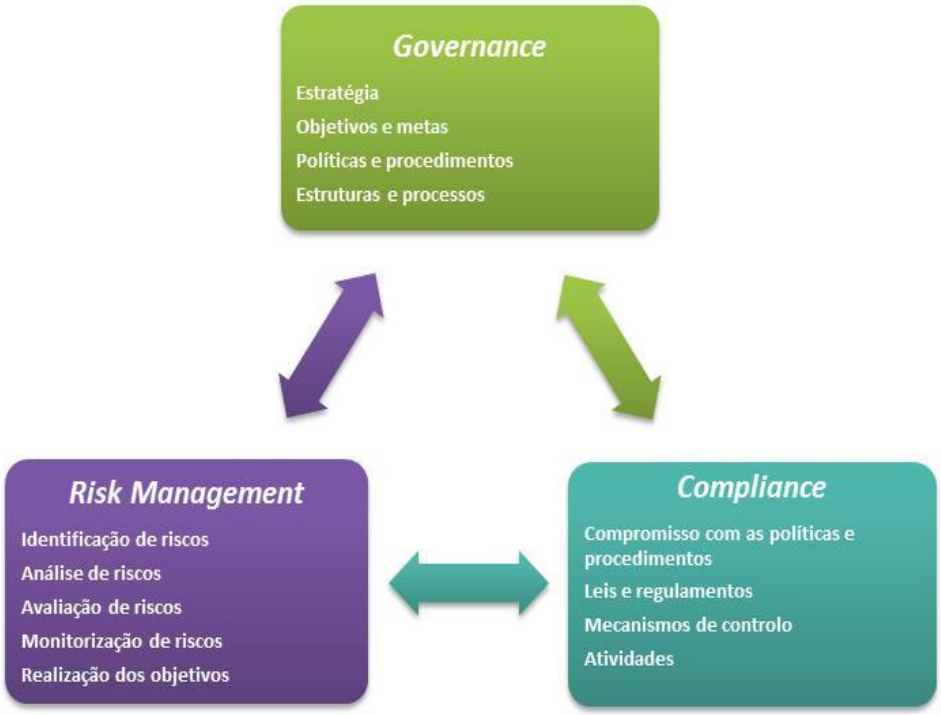

Figura 12 - *Governance, Risk and Compliance*

Fonte: Autor, adaptado de (Deloitte & ISACA, 2013)

As soluções GRC estão disponíveis em várias plataformas tecnológicas, como é o caso do *Enterprise Resource Planning* (ERP) da SAP (Deloitte & ISACA, 2013), plataforma que suporta atualmente o Sistema Integrado de Gestão da Defesa Nacional (SIGDN)[20].

No Apêndice G procede-se a uma melhor caraterização destes sistemas GRC.

4.7. Síntese conclusiva

A gestão estratégica e integrada de riscos nos Ramos, suportada por uma metodologia ERM, ajuda no processo de decisão estratégica, no planeamento e na afetação de recursos.

[20] Sistema aplicacional modular, comum aos Ramos, gerido pela Secretaria-Geral do MDN, que contém funcionalidades para os processos comuns de gestão financeira, logística e recursos humanos.

Tendo presente as estratégias dos Ramos, é possível definir uma iniciativa que visa a implementação deste tipo de metodologia, alinhada com objetivos estratégicos e operacionais de melhoria da eficiência organizacional e dos processos.

Com base na estrutura de GR do modelo ISO-ERM, foram descritos os aspetos mais relevantes das etapas de planeamento, implementação, monitorização e revisão e de aprendizagem e comunicação.

No planeamento da estrutura de GR foi-se ao encontro dos principais componentes de uma cultura de risco, tendo sido definidos os objetivos da GR, a estrutura de conteúdos para a política de GR e os níveis e responsabilidades organizacionais.

Quanto à implementação do processo de GR do modelo ISO-ERM, percorreram-se as fases de estabelecimento do contexto, identificação, análise, avaliação e tratamento do risco.

No estabelecimento do contexto, os Ramos devem confirmar o objeto de análise de risco e os objetivos e metas da avaliação tendo presente os interesses dos *stakeholders* e os constrangimentos e limitações existentes.

Na identificação do risco podem ser aplicadas várias técnicas, devendo os riscos serem caraterizados e registados. Nesse sentido, foram exemplificados para os Ramos um conjunto de fatores internos e externos geradores de riscos operacionais, riscos financeiros e riscos de reputação, suscetíveis de interligação com os riscos estratégicos.

Recorrendo a matrizes de avaliação de risco os Ramos podem analisar a probabilidade dos eventos e do seu impacto se ocorrerem, classificando os riscos quanto à sua gravidade. Tal permitirá verificar os respetivos mecanismos de controlo, que conjugados com os níveis de apetite e tolerância aceites para cada um dos riscos, orientam as estratégias de resposta.

Todo o processo de GR requer permanente liderança, envolvimento e cultura de aprendizagem e comunicação, sendo igualmente relevante a monitorização e revisão das atividades e dos respetivos indicadores de performance, essenciais para confirmar a eficácia dos mecanismos de controlo, aperfeiçoar os próprios processos e evoluir na cultura de risco.

Finalmente, e porque uma metodologia abrangente como a descrita requer sistemas de informação de suporte, identificaram-se os sistemas GRC como solução possível para implementar o ERM nos Ramos, tendo sido ainda referenciada a plataforma SAP do SIGDN para servir aquele propósito.

Conclusões

Num contexto de mudança permanente do ambiente das organizações e de grande incerteza, torna-se necessário lidar com os riscos numa perspetiva abrangente, preditiva e proactiva, assumindo a GR uma dimensão holística, envolvendo toda a organização.

Existem presentemente metodologias de gestão estratégica, integrada e corporativa de riscos que procuram responder a essa necessidade, através de novas abordagens que alinham objetivos organizacionais com mecanismos de identificação, análise, avaliação, mitigação e controlo dos riscos, sempre com o propósito de criar e proteger o valor da organização.

A presente investigação teve como objetivo geral, identificar contributos para uma gestão mais eficiente dos riscos nos Ramos das FFAA, a fim de apoiar a tomada de decisão e contribuir para a prossecução dos objetivos organizacionais.

Como método de investigação foi utilizada uma abordagem hipotético-dedutiva, com o intuito de responder à questão formulada através do teste a hipóteses indicativas, adotando-se para a pesquisa efetuada uma estratégia eminentemente qualitativa e um desenho de pesquisa do tipo "Estudo de caso".

Efetuada a sistematização do quadro conceptual em torno dos conceitos de Risco, Gestão do Risco e Cultura de Risco, a pesquisa foi direcionada para a caraterização da importância da gestão estratégica dos riscos nas organizações, seguindo-se uma análise à cultura e à abrangência estratégica das práticas de gestão de risco existentes nos Ramos. Por fim, perspetivaram-se os contributos para a aplicação de uma metodologia de gestão estratégica e integrada de riscos aos Ramos.

Assim, num primeiro momento procurou-se a resposta para a QD1 "Qual a importância da gestão estratégica do risco para a gestão das organizações?" pelo que houve necessidade de estudar a evolução da GR, o risco na gestão estratégica e os modelos de ERM da COSO e da ISO.

A análise desenvolvida permitiu concluir que as práticas de GR têm evoluído para ir ao encontro das necessidades de gestão das organizações, com a adoção de processos consistentes e modelos estruturados que têm permitido que o risco seja gerido de forma mais coerente.

De facto, muitas das perdas nas organizações são causadas por falhas na gestão dos riscos estratégicos, por não integração da GR no planeamento estratégico, por não existir

ou existir de forma ineficaz uma gestão de riscos estratégicos e porque a estratégia não é orientada para o risco.

As organizações devem tomar consciência que, sendo o risco uma variável incerta, a informação recolhida sobre este durante os processos de planeamento estratégico, pode sofrer alterações à medida que a estratégia progride, pelo que se torna necessário um controlo e monitorização permanentes.

Confirmaram-se igualmente as vantagens dos modelos ERM para uma gestão estratégica, corporativa e integrada de riscos, por serem aplicados à definição das estratégias e envolverem a organização como um todo, por pressuporem uma visão de portfólio dos riscos mais significativos, e por permitirem a identificação dos eventos cuja ocorrência pode afetar os objetivos, bem como a administração dos mesmos de acordo com o apetite e tolerância definidos.

Deste modo, conclui-se que uma bem-sucedida gestão estratégica de riscos, alguns relacionados ou interdependentes, melhora a eficiência organizacional e contribui para o atingir dos objetivos, pelo que se valida a Hip1 de resposta à QD1.

Num segundo momento procurou-se responder à QD2 “Qual o nível de cultura de risco e a abrangência estratégica das práticas de gestão do risco existentes nos Ramos? “ tendo-se recorrido à análise da informação obtidas das entrevistas realizadas na Marinha, Exército e Força Aérea, designadamente para os itens de análise respeitantes à “Avaliação da cultura de risco”, “Riscos Estratégicos”, “Riscos associados às capacidades militares”, “Riscos operacionais” e “Auditoria e Controlo Interno”.

Assim, para as componentes que enformam uma cultura de risco, não obstante a sensibilidade e o interesse evidenciados sobre a importância da GR, em especial na área das operações, verificou-se que a cultura de risco na gestão é insuficiente, em especial na Marinha e na Força Aérea, pela ausência de políticas formais de GR, organização própria, incipiente e disperso normativo assim como ausência de estratégias específicas para esta área. O Exército apresenta uma situação mais favorável neste domínio, essencialmente porque existe estratégia para a GR, que decorre da atual diretiva de planeamento do CEME, há um núcleo específico no EME que trata a GR ao nível estratégico, e existem normas técnicas mais abrangentes neste domínio.

Verificou-se ainda que existem a nível estratégico e a nível operacional práticas casuísticas de análise do risco, que abrangem a gestão estratégica, a gestão de projetos, as operações, as áreas de gestão de recursos financeiros, humanos, materiais e informacionais

e as áreas de auditoria e controlo interno. No entanto, são práticas em regra informais e não estruturadas, conduzidas a nível descentralizado e sem integração da informação de risco.

Conclui-se ainda que, não obstante os Ramos revelarem uma boa consolidação dos instrumentos e práticas no âmbito da gestão estratégica, não dispõem contudo de instrumentos que permitam gerir de forma sistemática e integrada todos os riscos com relevância estratégica.

Do exposto, considera-se que os Ramos dispõem de alguma cultura de risco, bem como de práticas de GR de relevância estratégica em diferentes áreas e níveis organizacionais, existindo contudo lacunas no tratamento integrado da informação de risco, pelo que se valida a Hip2 de resposta à QD2.

Na terceira fase da investigação procurou-se responder à QD3 "De que forma a aplicação de uma metodologia de gestão estratégica e integrada de riscos nos Ramos pode contribuir para apoiar as decisões estratégicas, operacionais e o desempenho organizacional?".

Para tal procedeu-se ao enquadramento avaliativo de uma solução de implementação da metodologia ERM da ISO, considerando os resultados do diagnóstico efetuado à cultura de risco e às práticas de GR dos Ramos, à informação obtida das entrevistas quanto ao item "Gestão Integrada de Riscos", e à possibilidade da iniciativa ficar alinhada com os objetivos estratégicos e operacionais de melhoria da eficiência organizacional das atuais diretivas de planeamento dos Ramos.

Seguidamente procedeu-se à análise dos aspetos mais relevantes da aplicação das etapas da estrutura de ERM da ISO tendo sido definidos, em sede de planeamento da metodologia, os objetivos da GR para os Ramos, a estrutura de informação da política formal de GR e a matriz de responsabilidades.

Na implementação do processo de GR da ISO foram abordados os aspetos mais relevantes das fases de estabelecimento do contexto, identificação do risco, análise do risco, avaliação do risco e tratamento do risco. Releva-se, neste âmbito, a identificação de um conjunto de fatores internos e externos geradores de riscos operacionais, riscos financeiros e riscos de reputação, suscetíveis de interligação com os riscos estratégicos, para os quais foram indicadas algumas ações de prevenção e mitigação.

Por fim, identificaram-se os sistemas de *Governance, Risk and Compliance* para possível suporte informacional da metodologia ERM da ISO, tendo igualmente sido referida a possibilidade da plataforma SAP do SIGDN servir esse propósito.

Ficou assim demonstrado que uma abordagem mais estruturada, integrada e corporativa da gestão de riscos nos Ramos, suportada por um modelo de Gestão de Risco Empresarial, melhora a capacidade de decisão e de tratamento dos riscos que afetam os objetivos, pelo que se valida a Hip3 de resposta à QD3.

Do exposto, conclui-se que a gestão estratégica e integrada de riscos aplicada aos Ramos e suportada por uma metodologia ERM, reforça a cultura de risco e ajuda nos processos de planeamento estratégico e controlo de gestão, no planeamento e execução operacional e na afetação de recursos, pelo que se considera respondida a QC "Como pode ser melhorada a eficiência da gestão do risco nos Ramos das FFAA em apoio às decisões estratégicas, operacionais e ao desempenho organizacional?", e cumprido assim o objetivo geral da investigação.

O contributo deste trabalho para o conhecimento decorreu da análise realizada, tendo sido possível avaliar a integração da GR na gestão estratégica dos Ramos e demonstrar a possibilidade de ser aplicado um mecanismo de melhoria que permitirá reforçar a cultura de risco e auxiliar a gestão.

De facto, não existindo nenhum referencial normativo, nem nenhuma metodologia específica para a GR aplicável de forma transversal à administração pública, considera-se que a metodologia descrita de aplicação da ISO-ERM aos Ramos, concebida com base no conhecimento implícito das normas referenciadas e na análise da informação recolhida, pode servir como guia para eventual implementação e apoio à produção de normativo.

Nesse sentido, como recomendações para futuros trabalhos propõe-se:

- Estudos práticos de integração do processo de GR nas futuras estratégias dos Ramos;
- Estudo de adequabilidade e aceitabilidade da criação de uma "capacidade de gestão de risco", a gerir pelo órgão de governação responsável pela gestão estratégica de cada Ramo e a edificar em moldes semelhantes à "capacidade de gestão de projetos" da Marinha. Não obstante tratar-se de uma capacidade gestionária, entende-se que a análise seria facilitada incorporando as conhecidas vertentes da edificação das capacidades militares, designadamente: Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade;
- Um estudo ao módulo de GRC/ ERM da plataforma tecnológica ERP da SAP que suporta o SIGDN, a fim de avaliar da possibilidade de ser utilizado para a gestão

integrada do risco nos Ramos. Esta solução, se viável, permitiria aperfeiçoar, expandir e otimizar um sistema de informação conhecido e em ampla exploração nos Ramos, o que facilitaria a exploração e desenvolvimento da própria "capacidade de gestão do risco".

Por fim, salienta-se que uma implementação do ERM conforme às fases descritas, a suportar por um adequado sistema de informação de gestão e acompanhada da sensibilização e formação dos decisores para a GR, fortalecem a gestão estratégica e operacional dos Ramos, melhorando a performance e o apoio à tomada de decisão.

Bibliografia

Andrade, J., 2016. *As ferramentas de gestão estratégica na avaliação de desempenho organizacional das Forças Armadas.* Lisboa: IUM.

BWise, 2017. *Solução inovadora de Governance, Risk Management and Compliance.* [Em linha] Disponível em: http://www.bwise.com/solutions [Acedido em 8 abril 2017].

CAS, 2003. *Overview of Entreprise Risk Management.* [Em linha] Disponível em: https://www.casact.org/area/erm/overview.pdf [Acedido em 5 dezembro 2016].

Castanheira, N e Rodrigues, LL, 2006. Gestão de risco - Da abordagem tradicional à gestão de risco empresarial (ERM). *Boletim: Revisores&Empresas*, julho/setembro, pp. 58-61.

CEMA, 2017. *Diretiva de Planeamento da Marinha 2017.* Lisboa: Marinha - Gabinete do Chefe do Estado-Maior da Armada.

CEME, 2016. *Diretiva do Comandante do Exército 2017-2019.* Lisboa: Exército Português - Estado-Maior do Exército.

CEMFA, 2016a. *Diretiva nº 1/CEMFA/2016 - Diretiva de Planeamento da Força Aérea.* Alfragide: Força Aérea - Chefe do Estado-Maior.da Força Aérea

CEMFA, 2016b. *Diretiva nº 4/CEMFA/2016 - Objetivos e Indicadores de Gestão para 2016.* Alfragide: Força Aérea - Chefe do Estado-Maior da Força Aérea.

Collier, P. M., 2014. *Fundamentals of Risk Management for Accountants and Managers Tools & Techniques.* New York: Routledge.

COSO, 1992. *COSO I - Internal Control - Integrated Framework.* New York: American Institute Of Certified Public Accountants.

COSO, 2004. *COSO II - Enterprise Risk Management – Integrated Framework.* New York: American Institute Of Certified Public Accountants.

COSO, 2014. *Governance and Operational Performance - Improving Organizational Performance and Governance - How the COSO Frameworks Can Help.* [Em linha] Disponível em: https:// www.coso.org/ Documents/ 2014-2-10-COSO-Thought-Paper.pdf [Acedido em 2 2017 fevereiro].

COSO, 2017. *Committee of Sponsoring Organizations of the Treadway Commission.* [Em linha] Disponível em: https://www.coso.org/Pages/default.aspx [Acedido em 14 janeiro 2017].

Costa, D., 2017. *Gestão do risco e de proteção da força. Conferência CPOG em 3 abril.* Lisboa, IUM.

Costa, S. R. R. d. & Fajardo, J. d. M., 2011. *Um estudo acerca do uso da gestão de riscos estratégicos na auditoria de gestão da Marinha do Brasil.* [Em linha] Disponível em: http://dx.doi.org/10.16930/2237-7662/rccc.v10n28p73-89 [Acedido em 16 fevereiro 2017].

Daniel, M., 2017. *As práticas de gestão do risco na Marinha* [Entrevista], Lisboa (20 janeiro 2017).

David, F. R., 2003. *Strategic Management - Concepts.* 9ª ed. New Jersey: Pearson Education International.

Deloach, J. W., 2000. *Enterprise-Wide Risk Management - Strategies foi Linking Risk & Opportunity*. Harlow: Financial Times - Person Education Limited.

Deloitte, 2014. *O estágio atual da gestão de riscos. Estratégias e ações para o crescimento sustentável.* [Em linha] Disponível em: https://www2.deloitte.com /content/dam/Deloitte/br/Documents/risk/Pesquisa-InteligenciaGestaoRiscos2014 .pdf [Acedido em 4 dezembro 2016].

Deloitte & ISACA, 2013. *Governance, Risk and Compliance - ISACA Monterrey.* [Em linha] Disponível em: http://m.isaca.org/chapters7/Monterrey/ Events/Documents/ 201323_05%_20Governance,%20Risk%20and%20Compliance.pdf [Acedido em 3 abril 2017].

Exército, 2007. *PDE 5-00 Planeamento Táctico e Tomada de Decisão.* Lisboa: Exército - Estado-Maior do Exército.

Exército, 2015. *Normas de Gestão de Projetos no Exército.* Lisboa: Exército - Estado-Maior do Exército.

Exército, 2016. *Plano de Gestão de Riscos de Corrupção e Infrações Conexas.* [Em linha] Disponível em: http://assets.exercito.pt/ SiteAssets/ GabCEME/ RCRPP/ documentos/ano%20de%20Gest%c3%a3o%20de%20Riscos%20de%20Corrup%

c3%_a7_%c3%a_3o%_20e%20Infra%c3%a7%c3%b5es%20Conexas_%20Assinado.pdf [Acedido em 3 abril 2017].

FERMA, 2003. *Norma de gestão de riscos.* [Em linha] Disponível em: https://www.theirm.org/media/886340/rm_standard_portugais_15_11_04.pdf [Acedido em 12 fevereiro 2017].

FERMA, 2010. *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.* [Em linha] Disponível em: http://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf [Acedido em 5 fevereiro 2017].

Ferreira, B., 2017. *As práticas de gestão de risco na Força Aérea* [Entrevista], Lisboa (24 janeiro 2017).

Ferreira, H., 2014. *A auditoria financeira como ferramenta de gestão na Marinha.* Lisboa: IESM.

Força Aérea, 2014. *Plano de Gestão de Riscos de Corrupção e Infrações Conexas.* [Em linha] Disponível em: http://www.emfa.pt/www/conteudos/informacaofap/plano_gestao_riscos.pdf [Acedido em 3 abril 2017].

Frigo, M. L. & Anderson, R. J., 2011. *What Is Strategic Risk Management.* s.l.:s.n.

Hardy, K., 2010. *Managing Risk in Government: An Introduction to Enterprise Risk Management 2ª ed.*. Washington: IBM Center For the Business of Govermment.

Henriques, S., 2013. *Maturidade da Gestão do Risco. Uma análise exploratória da sua divulgação nas empresas cotadas na Euronext Lisbon. Tese de Dissertação de Mestrado em Auditoria Empresarial Pública.* Coimbra: IPC-ISCAC.

Hopkin, P., 2012. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. 2ª ed.*. London: Kogan Page.

IESM, 2015a. *Trabalhos de Investigação (NEP / ACA - 010).* Lisboa: IESM.

IESM, 2015b. *Regras de Apresentação e Referenciação para os Trabalhos Escritos a realizar no IESM - NEP/ACA018.* Lisboa: IESM.

IGDN, 2013. *Manual de Procedimentos de Auditoria e Inspeção da IGDN.* Lisboa: IGDN.

INTOSAI, 2016. *INTOSAI GOV 9100 - Guidelines for Internal Control Standards for the Public Sector.* [Em linha] Disponível em: http://www.issai.org/en_us/site-issai/issai-framework/intosai-gov.htm [Acedido em 8 março 2017].

IRM, 2017. *Institute of Risk Management.* [Em linha] Disponível em: https:// www.theirm.org /the-risk-profession/ risk-management /irms-risk-management-standard.aspx [Acedido em 6 janeiro 2017].

Isac, F. L., 2015. Influence of Culture on the Process of Managing Decisions Adoption. *Journal of Economics and Business Research. Volume XXI, No. 2*, pp. 99-105.

ISO, 2009a. *ISO 31000:2009 - Risk Management - Principles and Guidelines.* Geneve: ISO.

ISO, 2009b. *IEC/ISO 31010:2009 Risk management -- Risk assessment techniques.* Geneve: ISO.

ISO, 2009c. *DNP ISO Guide 73 Risk management -- Vocabulary.* Geneve: ISO.

ISO, 2013. *ISO/TR 31004:2013 Risk management -- Guidance for the implementation of ISO 31000.* Geneve: ISO.

IUM, 2016. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação. Caderno N.º 8.* Lisboa: IESM.

Jordan, H.; Neves, J.C. e Rodrigues, J.A., 2011. *O Controlo de Gestão ao Serviço da Estratégia e dos Gestores.* 8ª ed. Lisboa: Áreas Editora.

Jorge, A. M., 2013. *Principios da gestão de risco da NP ISO 31000. Tese de Dissertação de Mestrado em Qualidade, Ambiente e Segurança.* Lisboa: Instituto Superior de Educação e Ciências.

Kaplan, R., 2009. *Risk Management and the Strategy Execution System.* s.l.: s.n.

Kerr, H., 2017. *Resiliência Organizacional: Aproveitando experiências, abraçando oportunidades.* [Em linha] Disponível em: https://www.bsigroup.com/LocalFiles/pt-BR/ Whitepapers/Resili%C3%AAncia%20Organizacional.pdf [Acedido em 6 abril 2017].

KPMG, 2013. *Gestão do Risco em Portugal Desafios para as Empresas.* [Em linha] Disponível em: https://www.kpmg.com/PT/pt/ IssuesAndInsights/ Documents/ survey ERM2013.pdf [Acedido em 06 dezembro 2016].

Lopes, T., 2017. *As práticas de gestão de risco na Força Aérea* [Entrevista], Lisboa (24 janeiro 2017).

Maia, I. e Chaves, G., 2016. *Integration of Risk Management into Strategic Planning: A New Comprehensive Approach. 2016 Enterprise Risk Management Symposium.*. [Em linha] Disponível em: http://www.ermsymposium.org/ 2016/ ERM_ Additional_Papers/Chaves-Maia.pdf [Acedido em 01 dezembro 2016].

Marinha, 2011. *Atividades de Inspeção.* Lisboa: Marinha - Inspeção-Geral da Marinha.

Marinha, 2013. *PAA 1002 - Doutrina de Gestão de Projeto na Marinha.* Lisboa: Marinha - Estado-Maior da Armada.

Marinha, 2014. *IAA 4 - Plano de Gestão de Riscos de Corrupção e Infrações Conexas.* Lisboa: Marinha - Inspeção Geral da Marinha.

Marinha, 2015. *PAA 1003 - Gestão Estratégica da Marinha.* Lisboa: Marinha - Estado-Maior da Armada.

Marinha, 2017. *Diretiva de Planeamento da Marinha 2017.* Lisboa: Marinha - Gabinete do Chefe do Estado-Maior da Armada.

Marques, S., 2017. *As práticas de gestão de risco na Marinha* [Entrevista], Lisboa (21 fevereiro 2017).

McKinsey&Company, 2011. *Strengthening risk management in the US public sector. McKinsey Working Papers on Risk, Number 28.*. [Em linha] Disponível em: http://www.mckinsey.com/business-functions/risk/our-insights/strengthening-risk-management-in-the-us-public-sector [Acedido em 06 dezembro 2016].

McPhee, I., 2005. *Public Sector Governance and Risk Forum. Risk and Risk Management in the Public Sector.* Australia: Australian National Audit Office.

MDN, 2013. *Diretiva Ministerial para a Reforma Estrutural na Defesa Nacional e nas Forças Armadas (Despacho nº 7527 - A/2013, de 31MAI).* Lisboa: Diário da República.

Monteiro, S., 2017. *As práticas de gestão de risco na Marinha* [Entrevista], Lisboa (3 fevereiro 2017).

NATO, 2010. *NATO Risk Management Guide (Draft).* Bruxelas: NATO HQ.

Nogueira, N., 2007. *A Gestão de Risco no Processo de Planeamento Estratégico.* [Em linha] Disponível em: http://www.occ.pt/ downloads/ files/ 1196447705_51a55_gestao.pdf [Acedido em 01 dezembro 2016].

Nutt, P. & Wilson, D., 2010. *Handbook of Decision Making.* United Kingdom: Wiley.

Oliveira, L., 2013. *Gestão de Riscos Estratégicos – Action Research numa empresa de tecnologias de informação. Tese de Dissertação de Mestrado em Gestão e Estratégia Industrial.* Lisboa: ISEG.

PA, 2017. *Stakeholders - Do significado à classsificação.* [Em linha] Disponível em: http://www.portal-administracao.com/2014/07/stakeholders-significado-classificacao .html [Acedido em 2 abril 2017].

Pickett, S. K., 2006. *Enterprise Risk Management: A Manager's Journey.*. Hoboken, NJ: John Wiley & Son.

PMI, 2013. *A Guide to the Project Management Body of Knowledge (PMBOK Guide).* Pennsylvania: PMI.

Province of British Columbia, 2012. *Risk Management Guideline for the BC Public Sector.* Canadá: Province of British Columbia.

Rasmussen, J. & Svedung, I., 2000. *Proactive Risk Management in a Dynamic Society.* Karlstad,Sweden: Swedish Rescue Services Agency.

Raymond, Q. & Luc, C. V., 2013. *Manual de Investigação em Ciências Sociais.* 6ª ed. Lisboa: Gradiva Publicações, S. A..

Ribeiro, B., 2017. *As práticas de gestão de risco no Exército* [Entrevista], Lisboa (6 fevereiro 2017).

Rosa, M., 2003. *Análise de Risco: Uma ferramenta de apoio à decisão.* Lisboa: IAEM.

Rosa, P. L., 2017. *As práticas de gestão de risco no Exército* [Entrevista], Lisboa (4 abril 2017).

SAP, 2017. *SAP Risk Management - Preserve and grow business value – with our enterprise risk management (ERM) software.* [Em linha] Disponível em: https://www.sap.com/product/ analytics/ risk-management.product-capabilities .html [Acedido em 9 abril 2017].

TCE, 2012. *Manual de Auditoria Financeira e de Conformidade.* Bruxelas: TCE- Unidade Metodologia de Auditoria e Apoio.

Vasconcelos, M. A., 2017. *As práticas de gestão de risco na Força Aérea* [Entrevista], Lisboa (8 fevereiro 2017).

Apêndice A – Conceitos associados ao risco e gestão do risco

Análise do risco: Processo destinado a compreender a natureza do risco e a determinar a probabilidade da sua ocorrência e o nível de impacto. Fornece a base para a avaliação do risco e as decisões para o seu tratamento (ISO, 2009c).

Apetite ao risco: Quantidade e tipo de risco que uma organização está disposta a aceitar na definição da sua estratégia e no desenvolvimento da atividade (ISO, 2009c).

Apreciação do risco: Processo global de identificação do risco, de análise do risco e de avaliação do risco (ISO, 2009c).

Avaliação do risco: Processo de comparação dos resultados da análise do risco com os critérios do risco para determinar se o risco e/ou a respetiva magnitude é aceitável ou tolerável (ISO, 2009c).

Critérios do risco: Termos de referência em relação aos quais a significância de um risco é avaliada (ISO, 2009c).

Estrutura de gestão de risco: Conjunto de componentes que servem de base para a organização, desenho, implementação, monitorização, revisão e contínuo aperfeiçoamento da GR de uma organização (ISO, 2009c).

Fonte de risco: Elemento que, por si só ou em combinação com outros, tem o potencial intrínseco de originar um risco (ISO, 2009c).

Identificação do risco: Processo de pesquisa, de reconhecimento e de descrição dos riscos. Envolve a identificação das fontes do risco, dos eventos, respetivas causas e potenciais impactos (ISO, 2009c).

Impacto: Resultado ou efeito de um evento (COSO, 2004).

Incerteza: Incapacidade de conhecer antecipadamente a probabilidade exata ou os impactos de eventos futuros (COSO, 2004).

Mitigação do risco: "Processo que visa diminuir o impacto do risco assumindo que este já ocorreu ou que a probabilidade de ocorrência é muito elevada" (IGDN, 2013, p. 21).

Nível de risco: Magnitude de um risco ou combinação de riscos, expressa em termos da combinação de impacto e respetiva probabilidade (ISO, 2009c).

Perfil de risco: Descrição de um conjunto de riscos de uma organização ou de um dos seus segmentos (ISO, 2009c).

Prevenção do risco: "Medidas adotadas no sentido de reduzir a probabilidade de ocorrência de um evento indesejado" (IGDN, 2013, p. 22)

Responsável pelo risco: Pessoa ou entidade com responsabilidade e autoridade para gerir o risco (ISO, 2009c).

Risco aceite: Risco reduzido a um nível que pode ser aceite. (IGDN, 2013).

Risco inerente: Risco que a organização terá de enfrentar na falta de medidas para alterar a probabilidade ou o impacto do evento (COSO, 2004).

Risco residual: Remanescente do risco depois do seu tratamento. Pode conter riscos não identificados ou riscos aceites (COSO, 2004).

Tolerância ao risco: Representa o nível aceitável de variação em relação à meta fixada para a realização de um objetivo específico (COSO, 2004)**.**

Tratamento do risco: "Processo de selecionar e implementar medidas para modificar o risco" (ISO, 2009c).

Apêndice B - Modelo COSO ERM - Componentes de ação

Tabela 7 - Modelo COSO - ERM – Componentes

Componentes	Descrição
Ambiente Interno *(Internal Environment)*	É a base de todos os restantes componentes. Compreende a avaliação ao ambiente em que a organização opera, a sua cultura de risco, o apetite ao risco, a supervisão da gestão superior, a integridade, os valores éticos e as competências do pessoal.
Fixação de Objetivos *(Objetive Setting)*	Os objetivos são fixados a nível estratégico, estabelecendo a base para os objetivos operacionais, de comunicação e de conformidade. A fixação de objetivos é um pré-requisito da identificação dos eventos internos e externos potenciadores de riscos. Os objetivos são alinhados com a missão da organização e são compatíveis com o apetite e a tolerância ao risco.
Identificação de Eventos *(Event Identification)*	Identifica os fatores internos e externos que podem dar origem a riscos e oportunidades que podem afetar a estratégia e a consecução dos objetivos.
Avaliação dos Riscos *(Risk Assessment)*	Permite que a organização avalie os efeitos dos potenciais riscos na realização dos objetivos. A avaliação é feita de acordo com a sua probabilidade e o impacto, utilizando para tal uma combinação de métodos qualitativos e quantitativos.
Resposta aos Riscos *(Risk Response)*	Após a avaliação dos riscos relevantes, a organização escolhe a resposta aos riscos - evitar, reduzir, partilhar ou aceitar, desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite ao risco.
Atividades de Controlo *(Control Activities)*	São políticas e procedimentos que contribuem para assegurar que as respostas aos riscos sejam executadas com eficácia.
Informação e Comunicação *(Information e Comunication)*	As informações relevantes sobre os riscos são identificadas, recolhidas e comunicadas, com eficácia e em tempo, em todos os níveis da organização, de modo a permitir que as pessoas envolvidas cumpram as suas responsabilidades.
Monitorização *(Monitoring)*	A GR é monitorizada para que sejam feitas modificações quando necessário. Realiza-se através de avaliações periódicas por parte da organização ou de entidades independentes.

Fonte: Autor, adaptado de COSO (2004)

Apêndice C - Guião geral das entrevistas

INSTITUTO UNIVERSITÁRIO MILITAR

Curso de Promoção a Oficial General 2016-2017 – Trabalho de Investigação Individual

Tema: "O papel da Gestão do Risco no apoio à decisão"

Auditor: 26485 CMG AN Paulo António Pires

Contactos: pires.pa@ium.pt; antonio.pires@marinha.pt; TM: 914515227

Guião para Entrevista com S. Exa. _____

Apresentação do trabalho

Justificação do tema

A importância crescente da gestão do risco nas organizações tem levado a um aperfeiçoamento das respetivas práticas, evoluindo essa gestão para um nível mais preditivo e proactivo dos riscos, tratados de forma holística pela gestão superior, e considerando a organização como um todo.

Com efeito, existem metodologias de gestão integrada de riscos, que procuram responder às necessidades crescentes das organizações, através de novas abordagens que alinham objetivos com mecanismos de identificação de riscos, procedem à sua avaliação, gestão e acompanhamento, com a finalidade de aumentar o valor da organização no médio e longo prazo.

À semelhança de outras organizações, também as FFAA estão sujeitas a vários tipos de risco, com origem em fatores internos e externos, pelo que a identificação destes e a consequente avaliação, mitigação e controlo são essenciais tendo em vista uma melhor resposta para o atingir dos objetivos, procurando sempre uma utilização eficiente dos escassos recursos colocados à disposição para o cumprimento da missão. Entre outros, os riscos podem ser genericamente classificados em riscos estratégicos, financeiros, operacionais, de gestão de recursos humanos, de gestão do investimento, de gestão da informação, de comunicação e de conformidade.

Do exposto, entende-se que o conceito de risco e a sua gestão, pela relevância no planeamento estratégico e controlo de gestão, nos processos operacionais, na gestão de recursos e nos sistemas de controlo interno, deve integrar a cultura organizacional dos Ramos das FFAA, estando sempre presente nas decisões de gestão.

Objetivo da investigação

A investigação visa a Gestão do Risco nos Ramos das FFAA e as perspetivas de aperfeiçoamento de práticas que, neste âmbito, melhorem a gestão e a tomada de decisão.

Como linhas de desenvolvimento da investigação, é feita uma análise da relevância estratégica da gestão do risco nas organizações, analisa-se a cultura de risco e as práticas de gestão do risco nos Ramos, e faz-se uma análise da aplicação aos Ramos de uma metodologia de gestão estratégica e integrada do risco, considerando a implementação da estrutura e do processo de gestão do risco.

Questão central

Decorrente da fase de exploração e da delimitação do tema, identifica-se a seguinte questão central:

Como pode ser melhorada a eficiência da gestão do risco nos Ramos das FFAA, em apoio às decisões estratégicas, operacionais e ao desempenho organizacional?

Tabela 8 – Tabela de questões das entrevistas

Itens em análise	Questões	Informação Pretendida
Avaliação da cultura de risco	1) O Ramo dispõe de uma política de gestão do risco?	Sobre as áreas funcionais abrangidas e a documentação de suporte à política.
	2) O Ramo está organizado para a gestão do risco?	a. Se existe algum departamento especializado para a gestão de riscos. b. Se existem normas especificas com procedimentos sobre o risco.
	3) O Ramo dispõe de alguma estratégia de gestão de riscos?	a. Se existe portfólio de riscos e matriz única de riscos. b. Se existem objetivos estratégicos específicos para melhorar a área de gestão de riscos.
Riscos estratégicos	4) Como são tratados os riscos no âmbito da gestão estratégica, considerando as fases de formulação, de implementação e de execução da estratégia?	a. Como são identificados os riscos estratégicos. b. Se há análise formal e estruturada destes riscos, e quem a faz. c. Na implementação da estratégia: se são aplicadas medidas para prevenir, reduzir ou mitigar os riscos e se existem planos de contingência (para os riscos aceites); ainda se são tomadas medidas perante os "riscos positivos" associados às oportunidades. d. Na implementação e controlo da estratégia que instrumentos de monitorização de riscos existem para aumentar a probabilidade de sucesso das iniciativas em curso. e. Se existem indicadores de gestão que permitem acompanhar e balancear a performance com o risco.
Riscos associados às capacidades militares	5) Como são geridos os riscos na edificação das capacidades militares?	a. Se a escolha de projetos considera alguma análise de risco. b. Se são identificados e analisados os riscos dos projetos em execução e se são acionadas medidas preventivas, de mitigação ou de contingência. c. Os instrumentos utilizados na execução dos projetos que ajudem a minimizar os riscos.

Itens em análise	Questões	Informação Pretendida
Riscos operacionais	6) Como são geridos os riscos de relevância para a estratégia inerentes aos sectores/ comandos funcionais (atividade operacional, gestão de recursos financeiros, humanos, materiais, informação)	a. Como são tratados os riscos que nos respetivos âmbitos têm relevância na estratégia; b. Como é feita a interligação destas relações causa/ efeito.
Auditoria e Controlo Interno	7) Qual o contributo da auditoria/controlo interno para a gestão dos riscos do Ramo?	a. Se as atividades de auditoria/controlo interno (incluindo as inspeções) são planeadas em função dos riscos existentes. b. Qual a natureza dos riscos analisados (estratégicos, operacionais, conformidade…). c. Da relevância da função auditoria e controlo para a estratégia do Ramo.
Gestão integrada dos riscos	8) Como melhorar a gestão do risco no Ramo?	Saber da importância de existir uma política, uma estratégia e processos de gestão do risco.
	9) Existem vantagens na implementação de uma metodologia de gestão integrada e corporativa de riscos no Ramo?	Saber da adequabilidade de implementação de uma metodologia desta natureza, tendo em conta a necessidade de integrar e alinhar os vários riscos com os objetivos estratégicos.
	10) Como configurar no Ramo uma organização adequada e eficiente neste âmbito e como suportar a gestão dos riscos com impacto estratégico?	a. Identificar a entidade que deve coordenar e acompanhar a execução de uma estratégia de gestão de riscos. b. Identificar outros requisitos para suporte à gestão integrada e corporativa de riscos.

Fonte: Autor (2017)

As perguntas incluídas nestes tópicos são exclusivas para as entrevistas com os oficiais generais e oficiais superiores dos Ramos.

Notas:

a) Solicita-se autorização para a gravação da entrevista, a fim de facilitar a posterior redução a escrito;

b) O resultado da entrevista será submetido à aprovação e autorização de V. Exa.

c) Este guião da entrevista será integrado num dos apêndices ao estudo, sendo a entrevista mencionada na bibliografia e podendo constituir fonte para citações ao longo do texto da investigação, devidamente referenciadas.

Muito obrigado pela atenção dispensada.

Apêndice D - Resumo das respostas às questões 1-7 (apoio ao capítulo 3)

Tabela 9 - Resumo das respostas às questões 1-7

Questões	Marinha	Exército	Força Aérea
(1) O Ramo dispõe de uma política de gestão do risco?	Não há uma política formal de gestão de risco. Existem práticas casuísticas de gestão de risco, ao nível da gestão estratégica, gestão de projetos da LPM, em algumas missões operacionais, na função de auditoria e controlo das atividades e processos das áreas de gestão de recursos (financeiros, pessoal e material) e no combate à corrupção e infrações conexas (Marques, 2017).	Não há uma política formal de gestão de risco, contudo o CEME, através da diretiva de planeamento do Exército, estabelece como orientações específicas juntar às atuais ferramentas de gestão estratégica a GR. Para além da gestão estratégica, existem práticas de análise de risco na gestão de projetos e na área de auditoria e controlo das atividades e processos no âmbito da gestão de recursos (financeiros, pessoal e material). O Exército tem também um plano de prevenção de gestão de risco de corrupção e infrações conexas, e elabora relatórios anuais da respetiva execução (Ribeiro, 2017).	Não há política formal de gestão de risco. Existem no entanto práticas consolidadas de gestão do risco na segurança de voo e segurança física de uma forma geral (Ferreira, 2017). Ao nível da gestão existem práticas informais de análise de risco no apoio à formulação estratégica, na gestão de projetos da LPM, e na auditoria interna às atividades e processos das áreas de gestão de recursos (financeiros, pessoal e material), no âmbito da conformidade legal e de procedimentos (Ferreira, 2017; Vasconcelos, 2017). A Força Aérea tem também um plano de gestão de risco de corrupção e infrações conexas, e elabora relatórios anuais da respetiva execução (Vasconcelos, 2017).
(2) O Ramo está organizado para a gestão do risco?	a. Não há um departamento especializado na GR na Marinha. O EMA, através da Divisão de Planeamento identifica os riscos estratégicos na fase de formulação da estratégia. Por sua vez, os sectores funcionais, na elaboração	a. Dispõem de um departamento especializado, o GGIC (no EME), que tem responsabilidades na gestão centralizada dos riscos associados à estratégia. O GGIC procede avaliação do risco estratégico no processo de formulação estratégica. Os objetivos	a. Não há um departamento especializado na GR na Força Aérea. O EMFA, através da Divisão de Planeamento, é responsável pela identificação de riscos para apoio à formulação da estratégia (Ferreira, 2017).

Questões	Marinha	Exército	Força Aérea
	das suas diretivas, identificam os riscos subjacentes à formulação dos objetivos operacionais (Marques, 2017). A IGM faz análise de risco aos processos e recomendações das entidades auditadas (Daniel, 2017). b. Existem referências à gestão do risco nas publicações PAA 1003 da gestão estratégica e PAA 1002 da gestão de projetos, e na publicação da Atividade Inspetiva (Marques, 2017; Monteiro, 2017; Daniel, 2017).	estratégicos e os operacionais, a atribuir à Entidades Sectoriais, são definidos centralmente (constam da diretiva do CEME), sendo que os riscos operacionais são depois monitorizados pelo GGIC e pelos responsáveis sectoriais (Ribeiro, 2017). b. Existe um Manual de Gestão de Risco. A diretiva de planeamento do Exército, contém algumas orientações específicas e conceitos relativos à GR para a fase de implementação, acompanhamento e controlo da estratégia (Ribeiro, 2017).	b. Existe organização e doutrina sobre a GR no âmbito da segurança de voo, segurança das instalações, do armamento e proteção ambiental (Ferreira, 2017).
(3) O Ramo dispõe de alguma estratégia de gestão de riscos?	a. Não há portfólios de riscos, nem são elaboradas matrizes únicas de risco. (Marques, 2017) b. Não existem objetivos específicos na DPM para a área de gestão de riscos, entendendo-se no entanto que podem ser definidos a nível operacional (área das TIC) objetivos que fiquem alinhados com objetivos estratégicos dos processos internos/estrutural daquela diretiva. (Marques, 2017).	a. O Exército tem portfólio de riscos, considerando que este inclui todos os riscos com relevância para os objetivos estratégicos e operacionais. O ramo tem também uma matriz única desses riscos (Ribeiro, 2017). b. A atual diretiva de planeamento na perspetiva dos recursos, prevê linhas de ação que visam melhorar a área de gestão de risco prosseguindo assim neste âmbito objetivos específicos quer de natureza operacional quer estratégica (Ribeiro, 2017).	a. A Força Aérea não tem um portfólio de riscos, nem uma matriz única de risco (Ferreira, 2017). b. A atual diretiva de planeamento prevê atividades que concorrem para o objetivo operacional de assegurar o controlo e a segurança das atividades, designadamente, o controlo e inspeção de conformidade, de eficiência e eficácia das atividades no domínio das operações, pessoal, logística, finanças e segurança militar, áreas que podem acolher iniciativas estratégicas em torno da GR (Ferreira, 2017).

Questões	Marinha	Exército	Força Aérea
(4) Como são tratados os riscos no processo de gestão estratégica?	a. A Marinha utiliza o *Balanced Scorecard* (BSC) como ferramenta de gestão estratégica seguindo a respetiva metodologia de planeamento estratégico. Os riscos associados a ameaças ou oportunidades são identificados na análise SWOT ao ambiente estratégico (interno e externo). Para um horizonte temporal superior ao mandato do CEMA, é feita uma análise prospetiva da evolução da Marinha a 20 anos na vertente genética, estrutural e operacional. Na análise ao ambiente estratégico, é realizada uma análise de risco e uma cenarização das ameaças (Marques, 2017). b. A Divisão de Planeamento do EMA é responsável pelo processo, mas não elabora um documento de análise formal e estruturada de riscos (Marques, 2017). c. Na fase de implementação são definidas estratégias para explorar as oportunidades e para eliminar, reduzir ou mitigar as ameaças/riscos identificados no diagnóstico	a. O Exército considera que os riscos estratégicos podem ocorrer tanto na definição como na implementação da gestão estratégica podendo condicionar seriamente a sua missão. Utilizam o BSC e a plataforma EPM como ferramentas de apoio à gestão estratégica, querendo integrar também a gestão da comunicações e a GR. A identificação dos riscos estratégicos é feita com base em análises SWOT (Ribeiro, 2017) b. A Divisão de Planeamento do EME conduz o processo e elabora um mapa, com a representação gráfica dos riscos em função da sua probabilidade e impacto. São identificados os vários riscos estratégicos, com a designação dos responsáveis pela sua gestão, e as respostas a dar para cada risco (Ribeiro, 2017) c. Na implementação são definidas estratégias para explorar as oportunidades e para eliminar, reduzir ou mitigar as ameaças/riscos. O produto final são os planos de ação ou planos de contingência, que derivam da análise conjunta dos objetivos estratégicos e da	a. A diretiva de planeamento da Força Aérea define e estrutura de objectivos estratégicos, objetivos operacionais e atividades. (Ferreira, 2017) b. A Divisão de Planeamento do EMFA é responsável pelo processo, mas não há avaliação estruturada de cenários de impacto e de probabilidade de ocorrência de eventos de risco, de priorização e de interligação (Ferreira, 2017). c. Em sede de planeamento, os riscos são considerados na definição das ações que concorrem para a execução de cada um dos objetivos operacionais (alinhados com os objetivos estratégicos). Existem ações específicas que procuram eliminar e mitigar riscos (Ferreira, 2017). d. É utilizada uma ferramenta em *Excel* (“Cockpit Organizacional”) que alinha objetivos, planos de ação e indicadores (KPI), de onde se podem identificar riscos pela análise do executado face ao planeado. Existem reportes trimestrais de indicadores, com a avaliação de todas as áreas de atividade para identificar desvios face

Questões	Marinha	Exército	Força Aérea
	estratégico (Marques, 2017). d. A execução da estratégia, ao nível das iniciativas é acompanhada por uma ferramenta de gestão de projetos, o EPM. A gestão de riscos nesta fase faz-se com base na análise aos resultados obtidos dos vários KPI face às metas fixadas para os respetivos objetivos (Marques, 2017). e. Os KPI podem assumir essa função (Marques, 2017).	identificação e avaliação dos riscos associados (Ribeiro, 2017) d. A execução da estratégia é apoiada pelo EPM (gestão de projetos). É feita a monitorização de indicadores de gestão (KPI) dos vários objetivos, e dispõem de *dashboards* específicos que permitem acompanhar e balancear o desempenho e o risco, construídos a partir do EPM (Ribeiro, 2017). e. Os KPI assumem-se como *Key Risk Indicators* (KRI) uma vez que podem refletir desvios e como tal eventuais riscos à execução (Ribeiro, 2017).	às metas estabelecidas. Dessa avaliação, podem ser tomadas medidas corretivas ou se tal não for possível, identificam-se ações por forma a mitigar os desvios de planeamento (Ferreira, 2017). e. O "Cockpit organizacional" permite acompanhar e balancear o desempenho e o risco através do registo dos vários KPI dos objetivos/atividades (Ferreira, 2017).
(5) Como são geridos os riscos na edificação das capacidades militares?	a. A escolha de projetos decorre da LPM aprovada, que foi elaborada a montante (MDN e EMGFA) com base na criação de cenários, análise de risco e identificação de lacunas nas capacidades, seguindo a doutrina do ciclo de planeamento de defesa nacional e da NATO (Marques, 2017). b. Na fase de edificação de capacidades, a execução material e financeira dos vários projetos incorpora análise de risco (Marques, 2017).	a. Existem procedimentos de GR a montante no planeamento de defesa, relacionando cenários, riscos e lacunas existentes, sustentados na doutrina do ciclo de planeamento de defesa nacional e NATO, que por sua vez estão relacionados com a edificação de capacidades, onde a GR é materializada através dos respetivos planos de implementação, que são sustentados na doutrina do ramo relativa às normas de gestão de projetos (Ribeiro, 2017). b. Na fase de edificação de capacidades, a GR é materializada e acompanhada	a. Em sede da documentação estruturante, em concreto na LPM, a análise de risco é efetuada a montante na fase de planeamento. É a Divisão de Planeamento do EMGFA que faz esse estudo no qual se entra em consideração com os riscos, as capacidades, a tipologia de meios e as lacunas (Ferreira, 2017). b. Na fase de edificação de capacidades, faz-se análise de risco através da execução material e financeira dos projetos (Ferreira, 2017).

Questões	Marinha	Exército	Força Aérea
	c. É usado o EPM como ferramenta de gestão de projetos, que contém funcionalidades de análise de risco. A gestão de projetos segue a doutrina do PMBOK *Guide*, (PMI, 2013), da NATO *Risk Management* (NATO, 2010) e do PAA1002 (Marinha, 2013) (Marques, 2017).	através da execução material e financeira dos projetos (Ribeiro, 2017). c. É usado o EPM como ferramenta de gestão de projetos, que contém funcionalidades de análise de risco. (Ribeiro, 2017)	c. A Força Aérea utiliza o EPM para gestão de projetos/contratos, que contém funcionalidade de análise de riscos (Ferreira, 2017).
(6) Como são geridos os riscos de relevância para a estratégia inerentes aos sectores/ comandos funcionais (atividade operacional, gestão de recursos financeiros, humanos, materiais, informação)	a. Os riscos operacionais são geridos pelos sectores funcionais. Existe alinhamento estratégico dos objetivos operacionais com os objetivos estratégicos, e relações de causa efeito entre eles, representados nos vários mapas de objetivos (da Marinha e dos sectores funcionais) (Marques, 2017). b. Os riscos com relevância estratégica são acompanhados pelos sectores através da monitorização dos KPI operacionais, reportados periodicamente, não havendo contudo alertas imediatos caso estejam a ocorrer desvios significativos face às metas. (Marques, 2017)	a. A estratégia é monitorizada e avaliada para aferir o grau de prossecução dos objetivos, sendo elaborados relatórios mensais e trimestrais para avaliar se a execução está de acordo com o planeamento, habilitando assim a adopção de eventuais medidas corretivas face aos desvios identificados, e relatórios anuais para avaliar se a estratégia está a produzir os efeitos desejados, ou seja, se os recursos utilizados para atingir os fins são os mais adequados. (Ribeiro, 2017) b. A monitorização dos resultados e a análise dos desvios em relação às metas são contínuas, questionando-se constantemente a validade dos pressupostos que foram assumidos na definição da estratégia. É uma atividade de largo espectro, monitorizada	a. Os objetivos operacionais são objetivos de 2º nível e estão definidos em consonância com os objetivos estratégicos através da diretiva de planeamento, estruturando a forma como se planeia alcançar os resultados e dirigindo as áreas de atividade (Lopes, 2017). b. Dispõem de uma ferramenta de acompanhamento da gestão e execução (da atividade operacional, e dos recursos humanos, financeiros e materiais) designada por " Cockpit Organizacional". Esta ferramenta é carregada com a informação das horas de voo anuais (regime de esforço), informação financeira, logística, de pessoal e materiais. Ao longo do ano averigua-se o cumprimento dos objetivos e das

Questões	Marinha	Exército	Força Aérea
		mensalmente pelo GGIC envolvendo as várias divisões do EME. A gestão dos outros riscos que não os estratégicos, são da responsabilidade das Entidades Sectoriais, que analisam, de forma metódica, os riscos inerentes às atividades e projetos e os fatores que lhes estão associados, estabelecendo para o efeito medidas de controlo e mitigação (Ribeiro, 2017).	qualificações do pessoal para cumprir as missões. Com esta ferramenta faz-se a monitorização de riscos de execução face ao planeado. Através de reportes trimestrais faz-se uma avaliação das áreas de atividade para identificar desvios face às metas, podendo ser tomadas ações para correção de desvios ou para mitigar os desvios (riscos) ao planeamento (Lopes, 2017).
(7) Qual o contributo da auditoria interna na gestão de riscos do Ramo?	a. A IGM faz inspeções. A auditoria está cometida aos sectores funcionais. As boas práticas preveem que o planeamento e a realização das atividades inspetivas devam ter em conta a avaliação do risco, o que nem sempre tem acontecido (Daniel, 2017). b. Durante as inspeções, fazem-se análises de risco aos processos (e às recomendações), numa ótica de conformidade e de prevenção de riscos. Faz-se também a atualização e acompanhamento da execução do PGRCIC, que contém, para os riscos nele identificados, um conjunto de ações a desenvolver pelos vários	a. Normalmente, a IGE não planeia auditorias ou inspeções em função dos riscos existentes. No entanto pretendem aperfeiçoar o processo de planeamento, com base na análise da informação do sistema de controlo de inspeções que estão a implementar pois a identificação de não conformidades comuns em várias unidades pode sinalizar tendências de vulnerabilidades com relevância estratégica, a ser merecedoras de ações concretas complementares (novas inspeções e/ ou implementação de procedimentos e de mecanismos de controlo) (Rosa, 2017). b. A IGE faz inspeções gerais (associadas à segurança das instalações, aos processos	a. A IGFA não planeia as auditorias em função da informação de risco (Vasconcelos, 2017). b. A IGFA faz várias inspeções, incidindo nas áreas financeira, logística, recursos humanos, no âmbito da segurança física, segurança de voo, segurança no trabalho, proteção ambiental etc. São inspeções orientadas aos processos. As não conformidades identificadas dão origem a recomendações definidas em função das normas e riscos percecionados. Faz-se também a atualização do PGRCIC e a elaboração dos respetivos relatórios anuais de execução. Considera-se que

Questões	Marinha	Exército	Força Aérea
	sectores com vista a reduzir ou a prevenir esses riscos. Considera-se que os riscos de corrupção e infrações conexas têm relevância estratégica pois além dos prejuízos patrimoniais, podem por em causa a reputação do Ramo (Daniel, 2017). c. A auditoria e as inspeções são importantes na avaliação dos processos, em especial os críticos que fazem parte da cadeia de valor. O controlo financeiro é também essencial para prevenir riscos associados à gestão dos recursos financeiros, riscos de *reporting*, relacionados com a qualidade do relato financeiro e de gestão, e riscos de conformidade relacionados como o cumprimento de normativo. A existência de riscos e de incerteza, obrigam necessariamente a um maior envolvimento e controlo, mais análises preventivas, maior observação e supervisão (Daniel, 2017).	logísticos, financeiros e de pessoal) e inspeções operacionais (mais orientadas para o treino operacional e certificação das FND de acordo com os padrões NATO. As recomendações identificadas para as não conformidades são objeto de análise de risco e de estimativa de custo de resolução. Fazem-se também inspeções técnicas (p. ex.: HST) e inspeções a processos transversais (p. ex.: alimentação, aquisições e saúde operacional).Os riscos aqui identificados podem ter relevância estratégica. Sobre os riscos de corrupção e infrações conexas, o EME faz o plano, e a IGE o relatório anual de execução com base na informação obtida das unidades. Os riscos estratégicos são avaliados e monitorizados pelo EME durante a execução estratégica (Rosa, 2017). c. Sem dúvida que as ações de auditoria e as inspeções são relevantes para a identificação de anomalias que podem resultar em riscos estratégicos (Rosa, 2017)	os riscos desta natureza têm relevância estratégica porque podem por em causa a imagem e reputação da instituição. A IGFA está a evoluir as suas práticas inspetivas de modo a ter inspeções de gestão (de carácter transversal) e inspeções de execução (Vasconcelos, 2017). c. A auditoria interna é relevante como forma de melhorar os processos permitindo corrigir as não conformidades em ordem a uma utilização mais eficiente dos recursos. No âmbito financeiro, é importante prevenir os riscos associados à gestão e aplicação dos recursos financeiros, que se refletem na qualidade do *reporting*, no mérito da gestão e no respeito pela legalidade (Vasconcelos, 2017).

Fonte: Autor (2017)

Apêndice E - Resumo das respostas às questões 8-10 (apoio ao capítulo 4)

Tabela 10 - Resumo das respostas às questões 8-10

Questões	Marinha	Exército	Força Aérea
(8) Como melhorar a gestão do risco no Ramo?	Para melhorar a identificação, avaliação e o controlo dos riscos que podem afetar ou comprometer os resultados pretendidos e, por conseguinte, os objetivos, importa melhorar a cultura de risco definindo uma política e uma estratégia a conduzir pela gestão superior e implementar uma "capacidade de gestão de risco", a operacionalizar com a implementação de metodologias de gestão integrada de riscos. (Marques, 2017; Daniel, 2017; Monteiro, 2017) Há que alargar o âmbito de aplicação e por em prática os conceitos e procedimentos de gestão de risco previstos na norma da Atividade Inspetiva[21] e definir um nível de aceitabilidade de risco (apetite ao risco) (Daniel, 2017).	Conforme decorre da diretiva do CEME para o planeamento, "…num prazo mais alargado, a centralização e formalização de um processo de GR facilita uma visão global dos diferentes riscos e suas interdependências, pelo que o caminho natural do processo de GR é aquele que leva a uma maior centralização da função, até chegar à gestão integrada dos riscos" (CEME, 2016, p. 29 cit.por Ribeiro, 2017). Pretendem integrar a gestão da comunicação e a GR na gestão estratégica, pois consideram que a "definição de objetivos estratégicos e a identificação e avaliação dos riscos são duas componentes interatuantes" (CEME, 2016, p. 30 cit. por Ribeiro, 2017). Também o "… processo de gestão do risco é um elemento central na gestão da estratégia de comando das Entidades Sectoriais (…) promovendo a eficiência e a eficácia operacional em todos os níveis da sua estrutura" (CEME, 2016, p. 30 cit. por Ribeiro, 2017).	A GR deve ser integrada na cultura da organização com uma política eficaz, uma organização e um programa de implementação. (Ferreira, 2017) Considera-se ser possível melhorar a identificação, avaliação e o controlo dos riscos que podem afetar ou comprometer os resultados pretendidos e, por conseguinte, os objetivos, através da implementação de metodologias de gestão integrada de riscos. (Ferreira, 2017; Vasconcelos, 2017)

[21] Referem as normas das Atividades de Inspeção da Marinha que a "…adopção de um modelo de gestão do risco irá contribuir para uma utilização mais eficiente dos recursos dentro da organização e para a melhoria do processo de planeamento, de estabelecimento de prioridades e de tomada de decisão nos diferentes níveis hierárquicos e

Questões	Marinha	Exército	Força Aérea
(9) Existem vantagens na implementação de uma metodologia de gestão integrada e corporativa de riscos no Ramo, do tipo ERM?	Considera-se adequada e aceitável a implementação de uma metodologia de gestão integrada e corporativa de risco, para materialização do processo de gestão de risco previsto na doutrina interna de Marinha[22] reforçando e consolidando as práticas neste âmbito (Daniel, 2017). Para se avançar com uma metodologia desta natureza, deve ser efetuada no âmbito das atividades e processos da Marinha, uma identificação e análise preliminar dos riscos com impacto em objetivos estratégicos, não esquecendo de individualizar para tratamento específico, em sede de normativo próprio, entre outros, os riscos ambientais e riscos associados à HST. (Daniel, 2017).	Os riscos estratégicos, com origem em fatores internos ou externos, podem ser identificados na formulação e na execução da estratégia. No primeiro caso podem limitar as estratégias a ser seguidas, no segundo podem inviabilizar a própria estratégia. A gestão integrada de riscos facilita a visão global dos vários riscos e as relações entre eles. (Ribeiro, 2017). Uma avaliação de desempenho e uma monitorização contínua dos riscos estratégicos que antecipe acontecimentos relevantes, confere mais eficiência e flexibilidade à ação do Exército caso as alterações às condições ambientais venham a afetar de forma muito significativa os objetivos estratégicos, podendo determinar a adoção de medidas corretivas, a reafectação de recursos ou a alteração de prioridades. (Ribeiro, 2017)	Considera-se adequada e aceitável a implementação de uma metodologia de gestão integrada e corporativa de riscos, tendo em conta as ameaças, o quadro restritivo e o ambiente de incerteza sempre presente, que se refletem numa exigência da gestão e por conseguinte na necessidade de aperfeiçoamento de práticas e mecanismos de controlo, entre eles a gestão dos riscos. (Ferreira, 2017; Vasconcelos, 2017)

em todas as áreas funcionais da Marinha, permitindo desta forma melhorar a eficiência na gestão dos recursos e agilizar o rastreio e a resolução das situações irregulares detetadas", e que "…para além da identificação dos principais fatores de risco, este modelo de gestão permitirá ainda conhecer e priorizar os riscos já existentes, estimar os custos associados à sua resolução ou mitigação e implementar as medidas de controlo que se venham a revelar mais adequadas em cada situação." (Marinha, 2011, p. 5.1).

[22] Os procedimentos de gestão de risco previstos na norma da Atividade Inspetiva da IGM são semelhantes aos utilizados pela IGDN e que constam do seu Manual de Procedimentos de Auditoria. Nos processos de auditoria da IGDN são aplicados modelos de avaliação do risco do tipo COSO-ERM (IGDN, 2013).

Questões	Marinha	Exército	Força Aérea
(10) Como configurar no Ramo uma organização adequada e eficiente neste âmbito e como suportar a gestão dos riscos com impacto estratégico?	a. O departamento mais adequado para essa coordenação seria o órgão de governação da "capacidade de gestão de risco"[23], a criar eventualmente junto do órgão de governação da Gestão Estratégica, o EMA, e contaria com o envolvimento da DAGI e da IGM. Face às restrições em pessoal, contaria com o suporte de uma bolsa de auditores colocados noutras unidades, especialistas em determinadas atividades e processos internos, alguns deles comuns a vários sectores e unidades (Daniel, 2017). b. A implementação de uma solução ERM deve ser suportada por um adequado sistema de informação que articule com os sistemas já existentes no âmbito da gestão estratégica, do EPM e SIGDN (Daniel, 2017; Monteiro, 2017).	a. A área mais adequada para essa coordenação seria o EME através da estrutura já existente no GGIC. Contaria com a IGE no âmbito da monitorização e controlo (Ribeiro, 2017; Rosa, 2017) b. A gestão de riscos com impacto estratégico baseado em soluções integradas requer o suporte de um adequado sistema de informação, que articule com os restantes sistemas de gestão. Importa contudo avaliar as condições de um eventual projeto dessa natureza. (Ribeiro, 2017; Rosa, 2017)	a. Não sendo exequível face à conjuntura restritiva, a criação de uma área específica para a gestão do rico, seria aceitável atribuir a coordenação e controlo dessa função à IGFA, envolvendo sempre o EMFA em termos de política e doutrina. (Vasconcelos, 2017) b. Poderia ser implementado uma solução ERM com suporte em adequado sistema informático. Esta implementação deveria ser acompanhada também com formação específica que incrementasse as aptidões dos decisores para a GR. (Vasconcelos, 2017)

Fonte: Autor (2017)

[23] Apesar de ser uma capacidade gestionária, a sua edificação, à semelhança do verificado com a capacidade de gestão de projetos, respeitaria as componentes de Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLPII).

Apêndice F - Prevenção e mitigação de riscos com relevância estratégica

Tabela 11 – Ações de prevenção e de mitigação de riscos - exemplos

Tipo de Risco	Fatores de risco	Descrição das acções
Riscos operacionais	Segurança nas Operações	– Planear e executar treino e certificação operacional; – Aplicar ao planeamento das missões operacionais o processo de planeamento operacional da NATO, que inclui análise de risco em cada uma das fases.
	Segurança da informação[24]	Garantir a continuidade do negócio, a segurança e a privacidade da informação e a proteção contra a fraude, mantendo a disponibilidade, a integridade e a segurança da informação e dos sistemas através da execução de: – Planos de *backup* e de recuperação de dados *(disaster recovery);* – Planos de resposta a incidentes; – Planos de resposta a falhas de energia; – Planos de resposta a ataques informáticos (âmbito ciberdefesa). – Ações de apoio à manutenção do Sistema Integrado de Gestão da Defesa Nacional (SIGDN)[25].
	Segurança das tecnologias de informação	
	Recrutamento do Pessoal	Assegurar as existências e as qualificaões do pessoal necessário[26] ao normal desempenho das missões e atividades, através de: – Executar planos de comunicação e divulgação para apoio ao recrutamento; – Executar planos de formação e de certificação profissional. Assegurar o cumprimento das normas de saúde, higiene e segurança no trabalho[27]; Auditar os sistemas de gestão de recursos humanos.
	Formação do pessoal	
	Gestão do pessoal	

[24] Se não for garantida a integridade e segurança da informação, existem também riscos de comunicação (*reporting*) porque está posta em causa a fiabilidade da informação (operacional, financeira, recursos humanos, etc) reportada pelos Ramos aos vários *stakeholders* internos e externos.
[25] Sistema crítico de alta disponibilidade. Por ser único e integrado acaba por ser disruptivo para a atividade dos Ramos em caso de falha.
[26] A insuficiência de pessoal pode limitar a capacidade instalada e comprometer os objetivos.
[27] Havendo incumprimento de normas, leis e regulamentos, há risco de conformidade (*compliance*).

	Manutenção dos meios operacionais e das infraestruturas	Assegurar a disponibilidade e a operacionalidade dos meios operacionais através da: – Execução dos planos de manutenção programados; – Expansão de protocolos de sustentação logistica com parceiros internacionais para mitigar as ruturas na cadeia de fornecimento de material crítico, obviando assim a obsolescência logistica de meios. Assegurar a manutenção e conservação das infraestruturas.
Riscos financeiros	Orçamento e níveis financiamento	– Garantir a cobertura permanente dos encargos fixos com pessoal e com as instalações; – Ajustar os planos de atividade e os níveis de esforço operacional, em função das alterações de prioridade nas políticas internas de financiamento suscitadas pelas variações orçamentais; – Reduzir os custos organizativos, otimizando os recursos disponíveis de suporte às atividades principais, eliminando assim redundâncias; – Assegurar o cumprimento dos procedimentos legais e regulamentares de âmbito financeiro;[28] – Reforçar o controlo financeiro combatendo o desperdício e avaliando o mérito das despesas.
Riscos de reputação	Corrupção e riscos conexos	– Auditar a execução dos PGRCIC, prevenindo ou mitigando os riscos de fraude ou corrupção; tráfico de influências; peculato; suborno; abuso de poder e conluio. – Incrementar a *accountability.*

Fonte: Autor (2017)

[28] Idem[27]

Apêndice G – *Governance, Risk and Compliance*

1. **O que é o GRC?**
   - ***Governance*** é um conceito global de gestão da organização que abrange o ambiente estratégico e de negócio, a estrutura, os processos, as políticas e os procedimentos que afetam o sucesso de uma organização. (BWise, 2017)
   - ***Risk management*** comporta a identificação e análise dos riscos que importa superar para alcançar os objetivos, e os mecanismos de controlo a implementar para evitar que esses riscos aconteçam. (BWise, 2017)
   - ***Compliance*** significa o compromisso/ conformidade para os limites de risco aceites para tentar alcançar os objetivos. (BWise, 2017)
2. **Qual o valor do GRC para as organizações?**
   - Permite que as organizações consigam conciliar o ambiente estratégico (objetivos, missão, visão e valores fundamentais) e a gestão dos riscos, enfrentado a complexidade legal, regulamentar inerente ao seu funcionamento. (BWise, 2017)
   - Permite que as organizações adotem uma abordagem integrada de gestão de riscos, abandonando o seu tratamento separado (em "silos"). (BWise, 2017)
   - Disponibiliza às organizações controlos e procedimentos documentados de funcionamento relevantes para a função auditoria interna. (BWise, 2017)
3. **Qual o foco do GRC?**
   A plataforma GRC ajuda a explorar três conceitos:
   - **Eficiência.** As organizações procuram soluções para aumentar a eficiência e obter resultados. Não podemos esquecer que a auditoria, a gestão de conformidade e a gestão do risco são grandes consumidores de tempo e recursos. (BWise, 2017)
   - **Reduzir riscos.** A plataforma GRC permite às organizações fazer melhor, ter as decisões mais informados, identifica causas e aloca recursos para mitigar os riscos. (BWise, 2017)
   - **Suporte estratégico para a performance**: Apoia o processo de decisão com uma definição clara dos objetivos e das metas e com métricas geradas que ajudam ao nível de sucesso. (BWise, 2017)
4. **Que soluções aplicacionais suportam o GRC ?**
   O *Enterprise Resource Planning* da SAP dispõe de um módulo de GRC, o SAP *Risk Management*[29] (Deloitte & ISACA, 2013).

[29] O SAP *Risk Management* incorpora as seguintes capacidades funcionais:

- *"**Risk strategy and planning** - Define risk-relevant business activities, set up your organizational risk hierarchy, and assign risk appetite, risk owners, and responsibilities. Develop risk libraries to structure and report on risk assessment results – and define your KRI framework to automate risk monitoring.*
- ***Risk identification** - Document the potential root causes and consequence of risks – and identify the relationship between risks and events. Capabilities include: defining survey questions, documenting activities, proposing risks, and documenting risks and opportunities.*
- ***Risk analysis** - Run quantitative and qualitative risk analysis to determine the likelihood of occurrence and the potential impact of identified risks. Capabilities include: conducting assessments, building risk scenarios, scenario analysis, performing Monte Carlo simulations, risk response, and documenting responses and enhancement plans.*
- ***Risk monitoring** - Analyze and report on your company's risk situation. Capabilities include: documenting incidents and losses for risk events."* (SAP, 2017)

Apêndice H - Síntese das etapas de implementação da metodologia ERM

Tabela 12 - Etapas de implementação da metodologia ERM

Fases	Descrição
Planeamento	1. Identificar os benefícios de uma iniciativa de gestão integrada de risco e obter a aprovação do Chefe do Estado-Maior do Ramo; 2. Planear o nível da iniciativa ERM e desenvolver uma taxonomia própria sobre o risco para garantir a consistencia da terminologia em toda a organização. Relevar a importância do risco nas expetativas dos *stakeholders*. 3. Definir uma politica de GR e uma arquitetura de risco. Estabelecer uma estratégia de risco, uma organização, regras e responsabilidades.
Implementação	4. Adotar adequados procedimentos de gestão de risco, sistemas de classificação e caraterização de riscos. 5. Estabelecer análises comparativas e empreender a avaliação do risco (usar técnicas de avaliação e fazer testes comparativos). 6. Determinar o apetite ao risco e os níveis de tolerância aos riscos e avaliar os controlos existentes (registo de riscos e do apetite ao risco).
Monitorização	7. Efetuar análise custo/ benefício dos controlos existentes e de controlos adicionais e introduzir alterações através de planos de melhoria de riscos. 8. Integrar a cultura de risco e o alinhamento da gestão de risco com outras tarefas de gestão.
Aprendizagem e comunicação	9. Monitorizar e rever os indicadores de performance de risco para medir a contribuição do ERM (definir planos de auditoria e de revisão sobre o risco). 10. Reportar a performance do risco em linha com os compromissos e obrigações de gestão.

Fonte: Autor, adaptado de (FERMA, 2010)

Apêndice I - Entidades entrevistadas

Foram entrevistados os seguintes militares:

Marinha

- CALM M Simões Marques, Subchefe do Estado-Maior da Armada
- CMG EMQ Modas Daniel, Coordenador da Inspeção-Geral da Marinha
- CMG M Silva Monteiro, Diretor de Análise e Gestão da Informação da Marinha

Exército

- COR TIR INF Boga Ribeiro, Chefe da Divisão de Planeamento de Forças do Estado-Maior do Exército
- COR INF Pedro Leal Rosa, Chefe de Gabinete do Inspetor-Geral do Exército - Inspeção-Geral do Exército

Força Aérea

- MGEN PILAV Barros Ferreira, Subchefe do Estado-Maior da Força Aérea
- COR TIR PILAV Teodorico Lopes, Chefe da Divisão de Planeamento do Estado-Maior da Força Aérea.
- COR ADMAER Maria Antónia Vasconcelos, Coordenadora da Inspeção-Geral da Força Aérea