MINISTÉRIO DA
DEFESA

Anexo E - Minuta de Guia de Gestão de Riscos

GUIA METODOLÓGICO
DE
GESTÃO DE RISCOS

1ª EDIÇÃO
BRASÍLIA – DF, 2025

MINISTÉRIO DA DEFESA

BRASIL
DO LADO DO POVO BRASILEIRO

MINISTÉRIO DA
DEFESA

EXPEDIENTE

MINISTÉRIO DA DEFESA

ÓRGÃOS DE ASSISTÊNCIA DIRETA E IMEDIATA AO MINISTRO DE ESTADO DA DEFESA

ÓRGÃOS ESPECÍFICOS SINGULARES DO MD

MINISTÉRIO DA
DEFESA

Ficha Técnica

Coordenação e consolidação
Paulo Marcelo Santana Barbosa

Elaboração:
Paulo Marcelo Santana Barbosa
Tiana Santana Cabral
2S Carlos Wilker Leoncio
3º SGT Lucas Marques Santana
Rute da Silva Aires
Yann Victor de Sousa Nascimento

MINISTÉRIO DA
DEFESA

SUMÁRIO

MINISTÉRIO DA
DEFESA

PREFÁCIO

A gestão de riscos é um processo sistemático, iterativo e de necessária comunicação entre as instâncias envolvidas no planejamento e na execução das atividades.

As atividades sistemáticas da gestão de riscos permitem antever possíveis problemas na execução dos macroprocessos, processos, projetos, iniciativas e atividades, além de permitir a percepção de oportunidades de melhoria nas mesmas execuções.

Este Guia Metodológico busca apresentar uma forma, adequada ao Ministério da Defesa, para a realização da gestão de riscos no Ministério da Defesa, exceto os Comandos da Marinha, do Exército e da Aeronáutica.

É necessária a ampla participação das instâncias da estrutura regimental do ministério na constante evolução deste Guia Metodológico.

Este guia metodológico permite a efetiva implementação da Política de Gestão de Riscos e deve ser empregado, inicialmente, vinculado ao Plano Estratégico Organizacional do Ministério da Defesa (PEO-MD).

De antemão, já se vislumbra um processo contínuo de atualização anual, a fim de adequá-lo às particularidades e especificidades do nosso Ministério.

MINISTÉRIO DA
DEFESA

DECLARAÇÃO DA ALTA ADMINISTRAÇÃO

O Ministério da Defesa reafirma seu compromisso com a excelência na gestão pública, reconhecendo a **gestão de riscos** como um instrumento estratégico essencial para o fortalecimento da governança, da integridade e da eficiência institucional.

A adoção sistemática da gestão de riscos está diretamente alinhada ao princípio constitucional da eficiência, contribuindo para a melhoria da qualidade dos serviços prestados à sociedade, para a racionalização do uso dos recursos públicos e para o aprimoramento da tomada de decisões. Ao antecipar e mitigar eventos adversos que possam comprometer os objetivos institucionais, a gestão de riscos fortalece a capacidade da organização de responder de forma proativa aos desafios e incertezas do ambiente público.

Este **Guia Metodológico de Gestão de Riscos** foi elaborado com o propósito de orientar os gestores e servidores do Ministério da Defesa na implementação efetiva da Política de Gestão de Riscos (PGR-MD), promovendo uma cultura organizacional voltada à prevenção, à integridade e à melhoria contínua.

A plena eficácia da gestão de riscos depende do **comprometimento da alta administração** e do engajamento de todos os gestores e equipes técnicas. Somente com atuação coordenada e integrada será possível consolidar um ambiente institucional resiliente, transparente e orientado para resultados que gerem valor público.

Brasília, 27 novembro de 2025

José Mucio Monteiro
Ministro de Estado da Defesa

1. INTRODUÇÃO

A crescente complexidade dos ambientes organizacionais e os desafios impostos à administração pública exigem o fortalecimento contínuo dos mecanismos de governança, integridade e gestão. Nesse cenário, a **gestão de riscos** se apresenta como uma ferramenta indispensável para a promoção da eficiência, da transparência e da responsabilidade na condução das políticas públicas.

A gestão de riscos consiste em um conjunto estruturado de práticas voltadas à **identificação, avaliação, tratamento e monitoramento de eventos que possam impactar negativamente os objetivos institucionais**, bem como à identificação de oportunidades que agreguem valor à organização. Ao ser integrada aos processos de planejamento estratégico e às atividades operacionais, ela potencializa a capacidade do MD de antecipar ameaças, mitigar impactos, prevenir falhas e assegurar a conformidade com os princípios da boa governança.

Este guia metodológico foi desenvolvido para apoiar a implementação da **Política de Gestão de Riscos do Ministério da Defesa (PGR-MD)**, oferecendo uma abordagem prática, clara e alinhada às melhores práticas nacionais e internacionais. Apresenta conceitos fundamentais, etapas do processo de gestão de riscos, responsabilidades institucionais e ferramentas de apoio, com vistas a orientar os gestores na condução das ações de gerenciamento de riscos em seus respectivos contextos organizacionais.

A aplicação efetiva da gestão de riscos contribuirá para a **modernização da administração pública**, a **otimização dos recursos**, o **fortalecimento da integridade institucional** e a **entrega de valor à sociedade**. Este guia é destinado a todos os órgãos que integram o Ministério da Defesa, com exceção dos Comandos da Marinha, do Exército e da Aeronáutica, conforme estabelecido na PGR-MD.

Este guia está estruturado em itens que abordam, de forma sequencial e integrada, os principais elementos da gestão de riscos no âmbito do Ministério da Defesa. Inicia-se com a apresentação da Política de Gestão de Riscos do MD, seguida pela descrição do Sistema de Gestão de Riscos e seus princípios e objetivos. Em seguida, detalha-se a integração da gestão de riscos ao planejamento estratégico, bem como as etapas metodológicas do processo de gestão de riscos — incluindo o estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e comunicação. Por fim, são apresentadas práticas operacionais, responsabilidades institucionais e referências que subsidiam a implementação eficaz da Política de Gestão de Riscos.

2. A POLÍTICA DE GESTÃO DE RISCOS DO MD

A Política de Gestão de Riscos do Ministério da Defesa - PGR-MD, aprovada pela Resolução CG-MD nº 3, de 25 de novembro de 2024, tem por finalidade estabelecer princípios, objetivos, diretrizes e instituir o sistema de gestão de riscos relacionados aos objetivos estratégicos organizacionais, projetos, processos e recursos no âmbito do Ministério da Defesa.

Ela estabelece que a gestão de riscos deve estar integrada ao planejamento estratégico organizacional, abrangendo as três linhas de defesa da gestão e todos os órgãos que integram o Ministério da Defesa, exceto os Comandos da Marinha, do Exército e da Aeronáutica.

Segundo o art. 7º da Resolução ora mencionada, o Sistema de Gestão de Riscos do Ministério da Defesa (SGR-MD), está organizado sob a forma de atividades de direcionamento, monitoramento, avaliação, coordenação, supervisão, consultoria e implementação da gestão de riscos.

As instâncias do Sistema de Gestão de Riscos estão descritas no art. 8º da mesma Resolução, quais sejam:

I - o Comitê de Governança do Ministério da Defesa;
II - o Subcomitê de Gestão de Riscos e Integridade;
III - a Secretaria de Controle Interno;
IV - a Assessoria Especial de Integridade e Segurança da Informação;
V - os proprietários de riscos; e
VI - os gestores de riscos.

2.1 O SISTEMA DE GESTÃO DE RISCOS

No âmbito do Ministério da Defesa, a gestão de riscos é conduzida de forma estruturada e integrada, envolvendo diferentes instâncias que colaboram para fortalecer a governança, a integridade e o controle interno.

Esse sistema é composto por órgãos colegiados, com atores diretamente envolvidos na identificação e tratamento dos riscos. Assim, os principais, são: o Comitê de Governança, o Subcomitê de Gestão de Riscos e Integridade, a Secretaria de Controle Interno, a Assessoria Especial de Integridade e Segurança da Informação, bem como os proprietários e gestores de

riscos, que desempenham papéis essenciais na consolidação de uma cultura organizacional voltada à prevenção e à mitigação de riscos.

Cada componente desempenha funções específicas que contribuem para o fortalecimento da cultura de gestão de riscos e para a tomada de decisões estratégicas mais seguras.

Toda a estrutura do sistema deriva da atuação do Comitê de Governança, que exerce papel central ao aprovar diretrizes e metodologias, definir limites de exposição a riscos e estabelecer prioridades para os processos e projetos estratégicos.

Devido ao seu propósito institucional de aprovar as diretrizes estratégicas, foi editada a Resolução CG-MD nº 3, de 25 de novembro de 2024, que aprova a Política de Gestão de Riscos do Ministério da Defesa, onde é possível apresentar de forma sutil e institucional as instâncias que compõem esse sistema e suas competências.

Na estrutura do sistema os gestores de riscos são responsáveis pela análise e classificação dos riscos, propondo medidas de controle adequadas aos processos sob sua responsabilidade, enquanto os proprietários de riscos garantem que os riscos sejam tratados e monitorados conforme as normas vigentes.

Adicionalmente o Subcomitê de Gestão de Riscos e Integridade, tem a competência, por intermédio de recomendações, de propor modelos e acompanhar a implementação da política, além de estimular a cultura de riscos no âmbito institucional, sendo assessorado pela Assessoria Especial de Integridade e Segurança da Informação que atua na supervisão, orientação, monitoramento das ações desenvolvidas pelos gestores de riscos, e coordenação do sistema, promovendo sua implantação e fomentando a cultura de riscos.

Por fim, a Secretaria de Controle Interno atua como orientadora dos gestores, oferecendo suporte técnico por meio de avaliações e consultorias, além das auditorias preventivas.

Desta maneira, conforme disposto no Mapa de Processo de Gestão de Riscos do MD - Anexo A - depreende-se que a Política de Gestão de Riscos do Ministério da Defesa, conforme estabelecida pela Resolução CG-MD nº 3/2024, consolida um modelo de governança que valoriza a atuação colaborativa e estratégica das instâncias envolvidas. Ao integrar competências e responsabilidades específicas, o sistema fortalece a cultura organizacional voltada à prevenção, à integridade e à tomada de decisões mais seguras, promovendo maior eficiência, transparência e responsabilidade na condução das atividades institucionais.

2.2 PRINCÍPIOS E OBJETIVOS DA GESTÃO DE RISCOS

Os princípios a serem observados quando da Gestão de Riscos, definidos pela Política de Gestão de Riscos (PGR), em seu art. 4º, são:

> I - aderência à integridade, aos valores éticos e às boas práticas de governança;
> II - atuação sistemática e estruturada, em obediência aos princípios da Administração Pública, considerando a oportunidade, a conveniência e o interesse público;
> III - adoção de níveis adequados de apetite a riscos;
> IV - subsídio à tomada de decisão; e
> V - contribuição para a melhoria contínua dos processos, implementada por meio dos ciclos de revisão.

As ações de gestão de riscos deverão observar os objetivos dispostos no art. 5º da PGR, a saber:

> I - contribuir para alcançar os objetivos estratégicos organizacionais, reduzindo os riscos a níveis aceitáveis;
> II - contribuir para a eficácia e maior eficiência dos processos e dos projetos;
> III - fomentar a gestão proativa;
> IV - aumentar a capacidade da organização de se adaptar a mudanças;
> V - estabelecer controles internos da gestão proporcionais à importância do risco, observado o seu impacto, probabilidade de ocorrência e razoabilidade da relação custo-benefício nas ações para tratamento de riscos;
> VI - agregar valor à organização, por meio da melhoria contínua dos processos, do tratamento adequado aos riscos e dos impactos decorrentes de sua materialização; e
> VII - implementar a prevenção de perdas e a ocorrência de incidentes de impactos negativos, por meio da análise continuada e melhoria dos processos.

2.3 INTEGRAÇÃO DO PLANEJAMENTO COM OS PROCESSOS ORGANIZACIONAIS

Com o propósito de implementar a integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, os processos de trabalho e os projetos relevantes para a execução da estratégia e o alcance dos objetivos institucionais devem ser considerados. Além disso, o planejamento da organização deve considerar os riscos associados aos objetivos e aos projetos estratégicos mais relevantes, de maneira a viabilizar o alcance dos resultados desejados.

Essa integração da gestão de riscos ao processo de planejamento e aos seus desdobramentos deverá observar a seguinte estrutura:

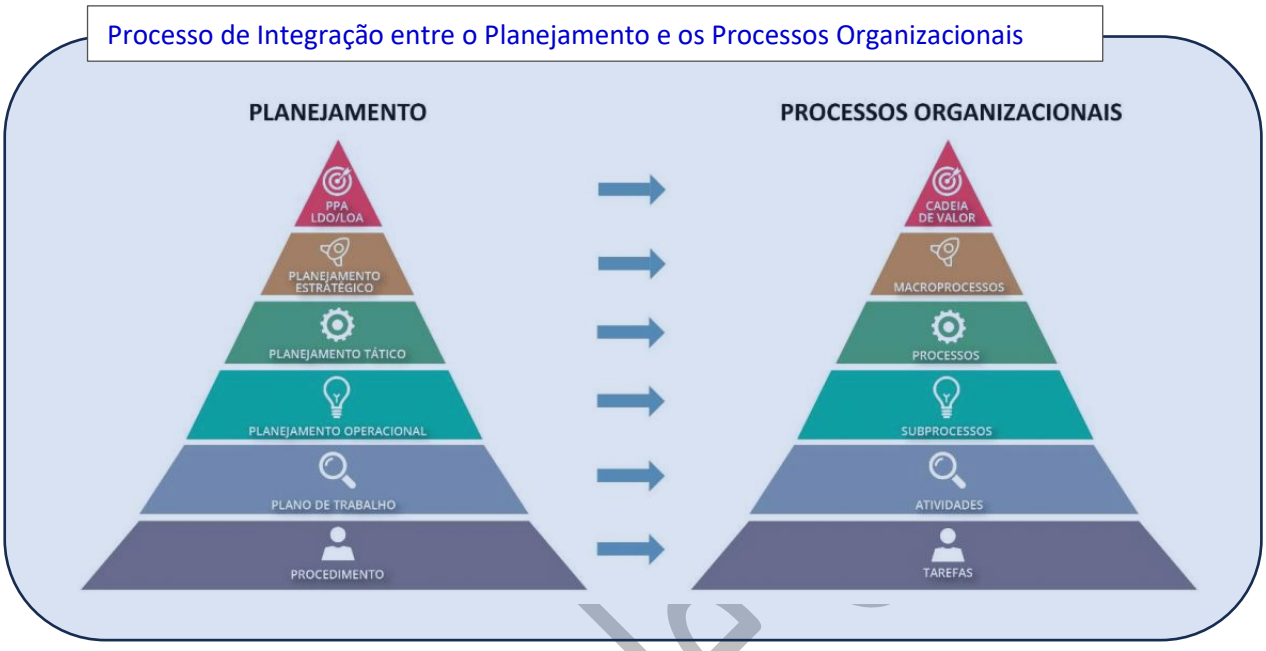


Figura 1 – Integração do Planejamento com os Processos Organizacionais

3. PROCESSO DE GESTÃO DE RISCOS

A gestão de riscos objetiva auxiliar no estabelecimento de estratégias, na tomada de decisões fundamentadas e no alcance dos objetivos estratégicos da organização. Assim, faz-se necessário que o processo de gestão de riscos esteja integrado ao planejamento da organização e aos demais processos de trabalho relevantes dos órgãos que integram o MD.

O processo de gestão de riscos inclui as etapas de estabelecimento do contexto, identificação, análise, avaliação, tratamento dos riscos, comunicação e consulta, e monitoramento e melhoria contínua, conforme apresentado na figura a seguir:

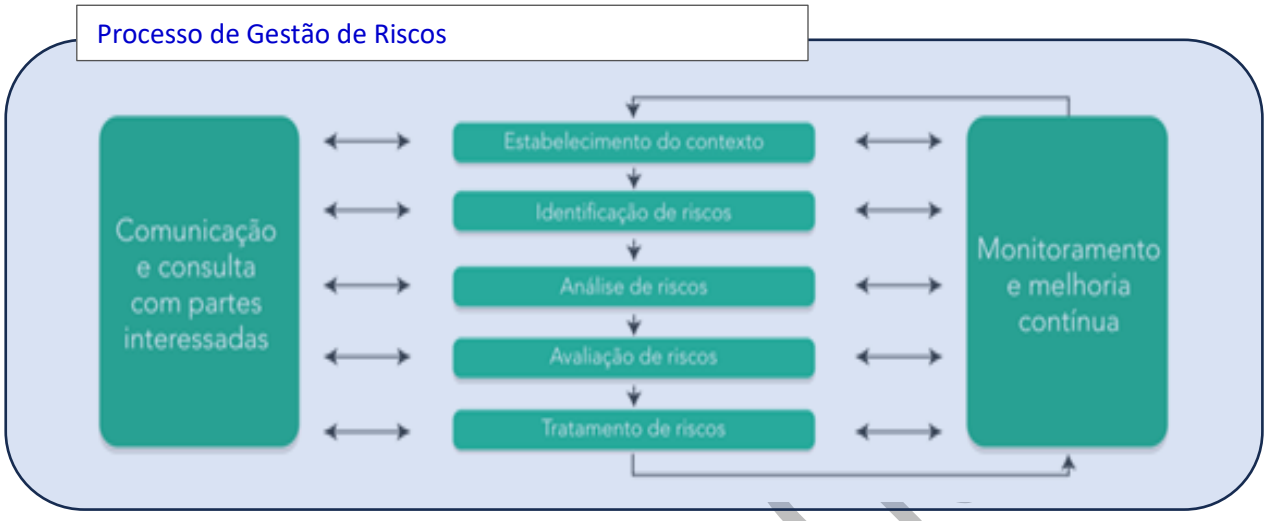


Figura 2 – Processo de Gestão de Riscos(ISO 31000 – Adaptado)

Cabe destacar que, apesar da representação gráfica indicar uma sequência de etapas a serem seguidas, deve-se considerar a natureza dinâmica e iterativa do contexto organizacional. Sendo assim, deve-se priorizar a gestão e melhoria contínua em todas as etapas.

Ressalta-se que as etapas de monitoramento e análise, bem como comunicação e consulta, são concomitantes às demais etapas do processo, ou seja, ocorrem a qualquer tempo.

O sucesso da implementação da gestão de riscos pressupõe que os gestores responsáveis pelos órgãos busquem capacitar seu pessoal continuamente e se utilizem do apoio técnico e das orientações da AESPI e do Subcomitê de Gestão de Riscos e Integridade, sempre que necessário.

3.1 PRÁTICAS PARA A GESTÃO DOS RISCOS

Entende-se por práticas para a Gestão de Riscos, o planejamento e a organização dos trabalhos que têm início antes da execução das etapas de gerenciamento de riscos e servirá para guiar os trabalhos a serem realizados, como a definição dos seguintes pontos principais:

- Processos / projetos objetos da gestão de riscos;
- Riscos identificados e ações de resposta que serão adotadas;
- Responsáveis pelos processos / projetos;
- Custo estimado para a implementação, se aplicável;

- Atividades de sensibilização e capacitação a serem realizadas, se necessário; e
- Cronograma das atividades.

É importante que, em uma primeira abordagem da elaboração do quadro de ações a serem executadas, seja avaliada a necessidade de melhorar ou extinguir controles internos da gestão já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles internos da gestão, observados sempre critérios de eficiência e eficácia da sua implementação.

Se as ações de resposta definidas envolverem mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta para que essas unidades validem as medidas de que participarem.

Em síntese, depois da etapa de avaliação, elabora-se o quadro de ações de resposta a serem adotadas em relação aos riscos identificados, relacionando, **por prioridade** para a execução.

3.2 ESTABELECIMENTO DO CONTEXTO

Contexto é a análise da ambiência organizacional, a partir da qual o ambiente no qual a organização busca atingir os seus objetivos. O conhecimento dos objetivos ou resultados a serem alcançados é fundamental nesta etapa.

O estabelecimento do contexto consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

Assim, o estabelecimento do contexto deve buscar:

- identificar quais objetivos ou resultados devem ser alcançados;
- identificar os processos de trabalho / projetos relevantes para o alcance dos objetivos/resultados;
- identificar as pessoas envolvidas nesses processos e especialistas na área; e
- mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.).

3.2.1 IDENTIFICAÇÃO DOS OBJETIVOS E DEFINIÇÃO DOS OBJETOS DE GESTÃO DE RISCOS

Nesta etapa são identificados e entendidos os objetivos definidos no instrumento de planejamento, objeto da gestão de riscos, conforme os níveis definidos na Figura 01. Esses objetivos definem a direção e os resultados esperados pelo Ministério da Defesa, em seus diversos níveis organizacionais, ao longo do período planejado e funcionam como guia para a tomada de decisões, a alocação de recursos e o alinhamento das ações institucionais à missão, à visão e aos valores do Ministério, promovendo coerência e efetividade na gestão estratégica.

Os objetivos devem ser conhecidos antes da identificação dos eventos em potencial que poderão afetar a sua realização. Nessa fase é importante fixar também os macroprocessos e respectivos processos relevantes para o alcance dos objetivos/resultados definidos no objeto da gestão de riscos, realizando a integração conforme alinhamento disposto na Figura 01.

Na sequência é importante definir os objetos da gestão de riscos, que são os elementos de uma iniciativa, entrega, resultado pretendido, processo, atividade ou iniciativa sujeitos à análise e gestão de riscos.

Podem ser objetos da gestão de riscos os instrumentos de planejamento em seus diversos níveis, assim como processos, planos de trabalho ou procedimentos, assim como os projetos que dão suporte à realização dos objetivos do MD. Unidades organizacionais também podem ser objeto da gestão de riscos.

3.2.2 ANÁLISE DO AMBIENTE

Um dos passos significativos da atividade de estabelecimento do contexto é a identificação dos fatores do ambiente, interno e externo, no qual a organização persegue seus objetivos.

Não menos importante é a identificação das partes interessadas, bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, pois essas partes interessadas devem ser incluídas em cada etapa ou ciclo do processo de gestão de riscos, por meio do processo de comunicação e consulta.

O Ambiente interno contempla os itens que a organização tem controle e pode mudar, pois são resultado de estratégias da organização, como recursos humanos, financeiros, físicos e tecnológicos. Nesse ambiente é possível identificar os pontos fortes e os pontos fracos da organização.

Os pontos fortes correspondem aos recursos e capacidades que juntos se transformam em vantagens para a organização e que podem ser utilizadas para alavancar resultados. Os pontos

fracos são as deficiências, limitações ou falhas que a organização apresenta e que podem impedir ou dificultar o progresso ou o alcance de objetivos e que representam oportunidades de melhoria.

O ambiente interno fornece a base pela qual os riscos são identificados e abordados, bem como a definição da filosofia de gerenciamento de riscos, do apetite a risco, dos valores, além do contexto em que estão inseridos.

O ambiente externo é composto por fatores fora dos limites da organização e, portanto, do seu controle, mas que, de alguma forma, exercem influência sobre ela. Assim, a organização deve se preparar e responder a esses fatores. Este é um ambiente que deve ser monitorado continuamente, pois é importante para o planejamento estratégico.

Essa etapa, refere-se ao entendimento dos ambientes interno e externo a partir da identificação de forças e fraquezas (interno) e das oportunidades e ameaças (externo) utilizados na fase da elaboração do planejamento estratégico.

Os contextos externo e interno constituem pois o ambiente no qual a organização procura definir e alcançar seus objetivos. Convém que o contexto do processo de gestão de riscos seja estabelecido a partir da compreensão dos ambientes externo e interno no qual a organização opera, e deve refletir ao ambiente específico da atividade a qual o processo de gestão de riscos é aplicado.

Compreender o contexto é importante porque:

- a gestão de riscos ocorre no contexto dos objetivos e atividades da organização;
- fatores organizacionais podem ser uma fonte de risco;
- propósito e escopo do processo de gestão de riscos podem estar inter-relacionados com os objetivos da organização como um todo.

Convém que a organização estabeleça os contextos externo e interno do processo de gestão de riscos, considerando alguns fatores.

Segundo a norma ISO 31000, o contexto externo pode incluir, mas não está limitado a:

- fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, em âmbito internacional, nacional, regional ou local;
- direcionadores-chave e tendências que afetem os objetivos da organização;
- relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas;
- relações e compromissos contratuais;

- complexidade das redes de relacionamento e dependências.

Examinar o contexto interno da organização pode incluir, mas não está limitado a:

- visão, missão e valores;
- governança, estrutura organizacional, papéis e responsabilizações;
- estratégia, objetivos e políticas;
- cultura da organização;
- normas, diretrizes e modelos adotados pela organização;
- capacidades entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, propriedade intelectual, processos, sistemas e tecnologias);
- dados, sistemas de informação e fluxos de informação;
- relacionamentos com partes interessadas internas, levando em consideração suas
- percepções e valores;
- relações contratuais e compromissos;
- interdependências e interconexões.

Para essa análise, sugere-se a utilização da ferramenta de SWOT. A SWOT é uma ferramenta que ajuda a identificar fatores internos (Forças e Fraquezas) e externos (Oportunidades e Ameaças) que afetam o desempenho da organização. Ao categorizar estes elementos numa matriz, é possível compreender a posição atual, identificar áreas para melhoria e definir estratégias para o futuro.

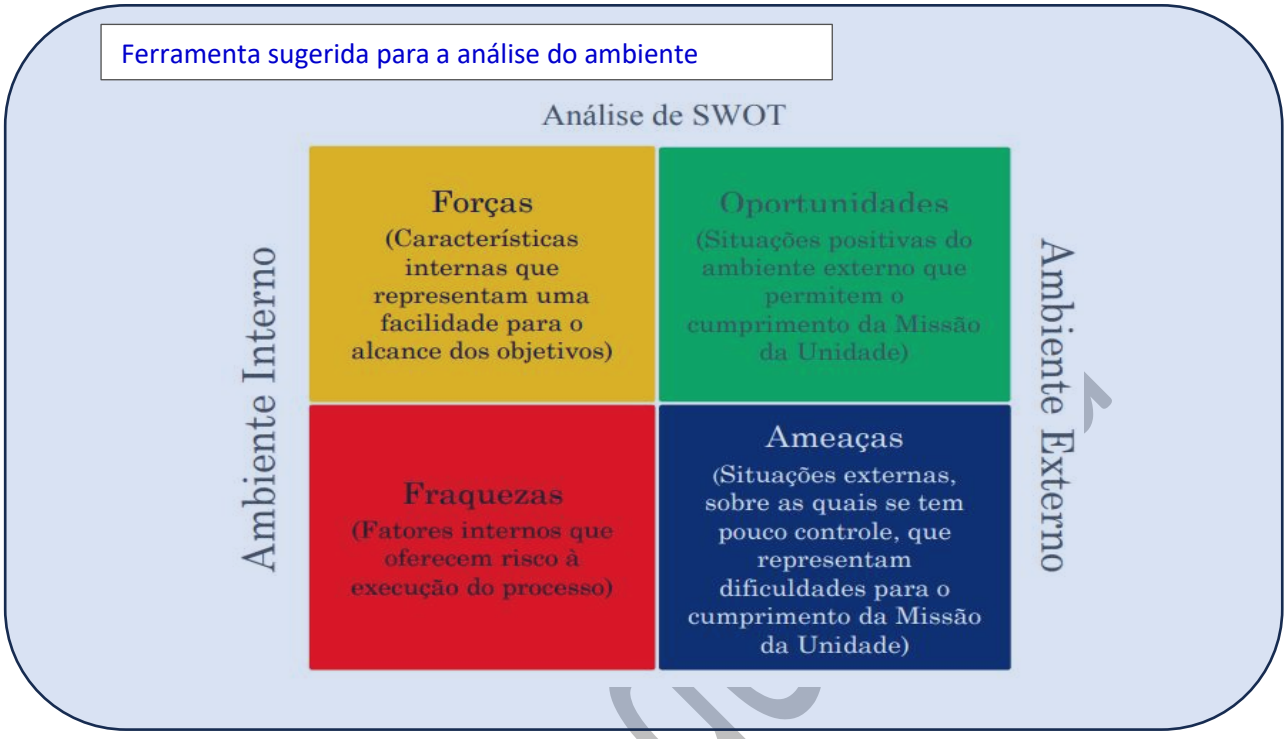


Figura 3 – Matriz SWOT

3.3 IDENTIFICAÇÃO DE RISCOS

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou evitar, atrasar, impedir ou prejudicar o alcance dos objetivos da organização. Informações pertinentes, apropriadas e atualizadas são importantes na identificação de riscos.

A identificação de riscos pode basear-se em dados históricos, análises teóricas, opiniões de pessoas capacitadas em gerenciamento de riscos e especialistas nas áreas analisadas, e nas necessidades das partes interessadas. A equipe deverá ser composta de pessoas que conheçam bem o objeto da gestão de riscos e tenham uma visão holística a respeito dele e dos objetivos a serem alcançados.

A presente etapa envolve a identificação e a descrição dos eventos de riscos, com a caracterização das suas causas (fontes) e consequências (efeitos). Assim, primeiramente deverá ser desenvolvida uma relação de eventos de riscos que podem constranger os resultados e o alcance dos objetivos organizacionais, afetando o seu desempenho e o valor público a ser entregue à sociedade.

Nesta etapa, pode-se empregar uma combinação de técnicas que aliam análise de eventos passados e potenciais eventos futuros.

Recomenda-se o emprego da Bow Tie, ferramenta que auxilia na identificação das causas e consequências de um evento de risco. O método Bow-Tie ou gravata borboleta, considerado uma evolução do diagrama de causa e efeito, consiste em identificar e analisar os possíveis caminhos de um evento de risco, dado que ele pode estar relacionado a diversas causas e consequências. Como no diagrama de causa e efeito, identifica-se o evento de risco e em seguida suas possíveis causas e consequências. Segundo a norma ABNT NBR ISO/IEC 31010:2012, a análise Bow Tie "é uma maneira esquemática simples de descrever e analisar os caminhos de um risco desde as causas até as consequências". Além disso, possibilita a análise em duas dimensões, a das causas, que representam uma forma de prevenir a sua ocorrência (controles preventivos), e a das consequências, que representam formas de mitigar os impactos (controles corretivos).

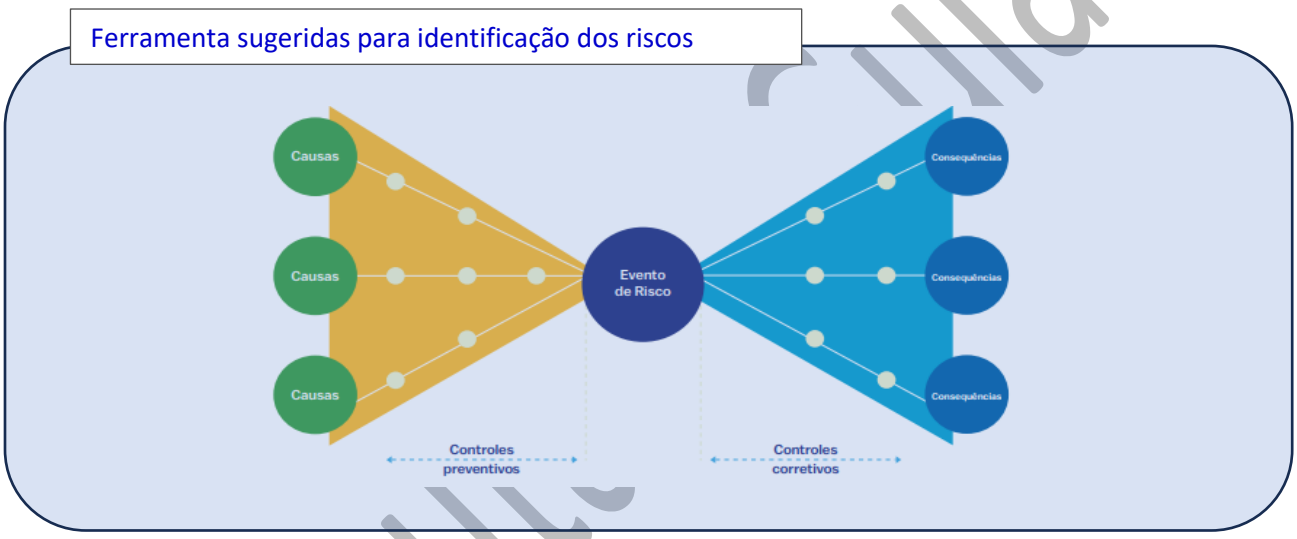


Figura 4: Diagrama *Bow Tie*

Existem outras técnicas na compreensão das causas e consequências dos riscos e que podem ser utilizadas, como o Diagrama de Ishikawa (espinha de peixe) e o método dos "5 Porquês", também citadas na ABNT NBR ISO/IEC 31010:2012. Sugestões de modelos e formulários estão disponíveis nos anexos deste guia.

Por fim, importa destacar que os riscos, as causas e as consequências devem ser descritas de forma clara e precisa, além de ser necessário observar a lógica correlacional entre estes. Assim, sugere-se a utilização da sintaxe de riscos, disposta a seguir, para auxílio:

Sintaxe do Evento de Riscos

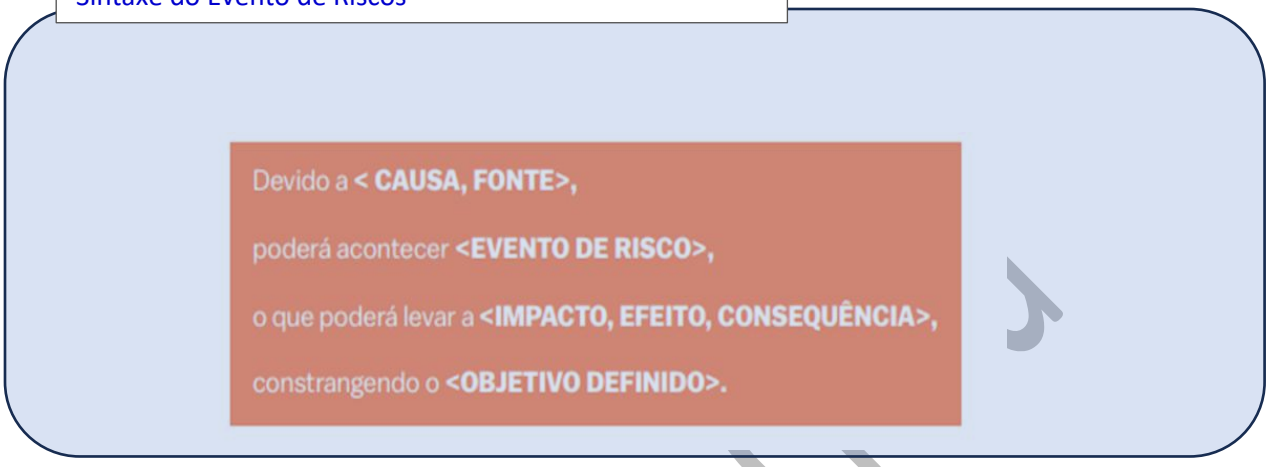


Figura 5: Sintaxe do evento de Riscos

São dicas que facilitam a identificação dos riscos:

- responder à seguinte pergunta-chave: o que pode atrapalhar o alcance do objetivo/resultado?
- considerar os fatores de sucesso para a consecução dos objetivos – qualquer evento que afete o fator de sucesso potencialmente afeta o objetivo/resultado;
- considerar as principais fontes de riscos: infraestrutura, recursos de quaisquer naturezas, pessoal, processos e tecnologia.

A organização pode usar uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos. Convém que os seguintes fatores e o relacionamento entre estes fatores sejam considerados:

- fontes tangíveis e intangíveis de risco;
- causas e eventos;
- ameaças e oportunidades;
- vulnerabilidades e capacidades;
- mudanças nos contextos externo e interno;
- indicadores de riscos emergentes;
- natureza e valor dos ativos e recursos;
- consequências e seus impactos nos objetivos;
- limitações de conhecimento e de confiabilidade da informação;
- fatores temporais;
- vieses, hipóteses e crenças dos envolvidos.

3.3.1 CATEGORIA DOS RISCOS

Para cada risco identificado deve ser indicada a respectiva categoria do risco. No âmbito do Ministério da Defesa, serão consideradas as seguintes categorias de riscos: **estratégico, operacional e de integridade**.

Essa simplificação visa proporcionar maior clareza e facilidade na categorização dos riscos, priorizando aqueles que possam comprometer o alcance dos objetivos institucionais, a eficiência dos processos e a conduta ética da organização.

As categorias de riscos estratégicos, operacionais e de integridade são pilares fundamentais na gestão de riscos de qualquer organização e podem assim ser definidos:

- **Riscos estratégicos** dizem respeito a fatores que podem afetar diretamente o alcance dos objetivos, o cumprimento da missão, o caminhar em direção da visão e o atingimento das metas de longo prazo da organização.
- **Riscos operacionais** envolvem falhas, ineficiências ou interrupções nos processos internos, sistemas e recursos que sustentam as atividades diárias.
- **Riscos de integridade** estão relacionados a desvios éticos ou de conduta, fraudes, corrupção, conflitos de interesse e outras práticas que possam comprometer a reputação, a legalidade e a confiança institucional.

Figura 6: Categorias de Riscos

3.4 ANÁLISE DOS RISCOS

A análise de riscos tem como propósito compreender a natureza do risco e suas principais características, incluindo causas, consequências e fatores de incerteza. Esse processo envolve uma avaliação detalhada das fontes de risco, da probabilidade de ocorrência, dos possíveis eventos e cenários, bem como dos controles existentes e sua eficácia.

É importante considerar que um único evento pode ter múltiplas causas e gerar diversas consequências, afetando diferentes objetivos organizacionais.

Figura 7: Componentes do Evento de Riscos

As causas dos riscos, também conhecidas como fatores de risco, são condições que originam a possibilidade de ocorrência de um evento indesejado. Esses fatores podem estar presentes tanto no ambiente interno quanto externo à organização. Identificá-los é essencial para compreender a origem dos riscos e desenvolver estratégias eficazes de prevenção e controle.

As causas de riscos devem ser identificadas a partir da fonte/fator de riscos (pessoas, processos, sistemas, infraestrutura física, tecnologia, governança, eventos externos, entre outros) consideradas juntamente com as vulnerabilidades identificadas (fraquezas e ameaças).

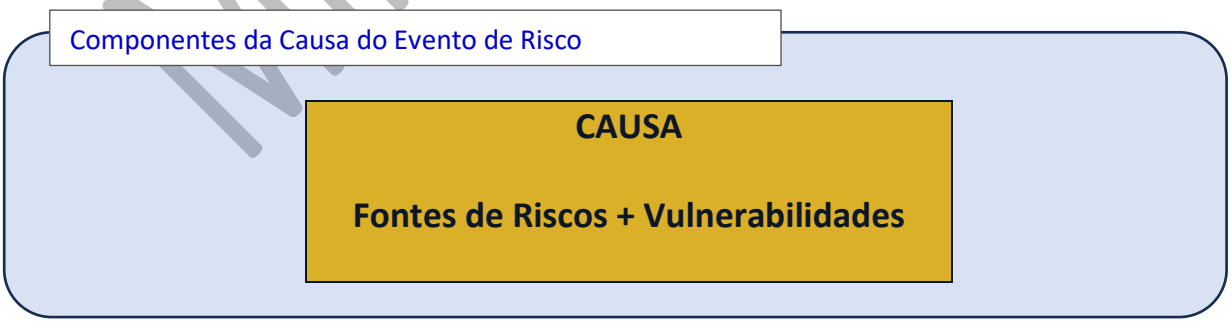


Figura 8: Componentes Causa do Evento de Risco

O quadro abaixo mostra alguns exemplos de fontes de riscos e suas respectivas vulnerabilidades:

CAUSA = FONTES + VULNERABILIDADES	
FONTES DE RISCO	VULNERABILIDADES (AMEAÇAS E FRAQUEZAS)
Pessoas	Em número insuficiente; sem capacitação; perfil inadequado; desmotivadas, alta rotatividade, propensas a desvios éticos e/ ou fraudes.
Processos	Mal concebidos (exemplo: fluxo, desenho, centralização, custosos ....); sem manuais ou instruções formalizadas (procedimentos, documentos padronizados e rotinas); sem segregação de funções, sem transparência.
Sistemas	Obsoletos; sem manuais de operação; sem integração com outros sistemas; inexistência de controles de acesso lógico/ backups, baixo grau de automação.
Infraestrutura Física	Localização inadequada; instalações ou leiaute inadequados; inexistência de controles de acesso físico.
Tecnologia	Técnica ultrapassada/produto obsoleto; falta de investimento em TI; tecnologia sem proteção de patentes; processo produtivo sem proteção contraespionagem, controles insuficientes sobre a transferência de dados.
Eventos Externos	Ambientais: mudança climática brusca; incêndio, inundação, epidemia. Econômicos: oscilações de juros, de câmbio e de preços, contingenciamento, queda de arrecadação, crise de credibilidade, elevação ou redução da carga tributária. Políticos: novas leis e regulamentos, restrição de acesso a mercados estrangeiros, ações de responsabilidade de outros gestores; "guerra fiscal" entre estados, conflitos militares, divergências diplomáticas. Sociais: alterações nas condições sociais e demográficas ou nos costumes sociais, alterações nas demandas sociais, paralisações das atividades, aumento do desemprego. Tecnológicos: novas formas de comércio eletrônico, alterações na disponibilização de dados, reduções ou aumento de custo de infraestrutura, aumento da demanda de serviços com base em tecnologia, ataques cibernéticos. Infraestrutura: estado de conservação das vias de acesso; distância de portos e aeroportos; interrupções no abastecimento de água, energia elétrica, serviços de telefonia; aumento nas tarifas de água, energia elétrica, serviços de telefonia. Legais/jurídicos: novas leis e normas reguladoras; novos regulamentos; alterações na jurisprudência de tribunais; ações judiciais.
Governança	Competências e responsabilidades não identificadas ou desrespeitadas; centralização ou descentralização excessiva de responsabilidades; delegações exorbitantes; falta de definição de estratégia de controle para avaliar, direcionar e monitorar a atuação da gestão; deficiência nos fluxos de informação e comunicação; produção e/ou disponibilização de informações, que tenham como finalidade apoiar a tomada de decisão, incompletas, imprecisas ou obscuras; pressão competitiva; falta de rodízio de pessoal; falta de formalização de instruções.
Planejamento	Ausência de planejamento. Planejamento elaborado sem embasamento técnico ou em desacordo com as normas vigentes, objetivos e estratégias inadequados, em desacordo com a realidade.

Tabela 1 - Causas, Fontes de Riscos e Vulnerabilidades

No que tange à consequência, estas devem ser identificadas a partir dos resultados da ocorrência do efeito do risco afetando a entrega, os resultados esperados ou iniciativa e, consequentemente, produzindo efeitos nos objetivos do planejamento. Para tanto, orienta-se a identificação da consequência frente ao efeito resultante do impacto na da execução do objetivo disposto no planejamento.

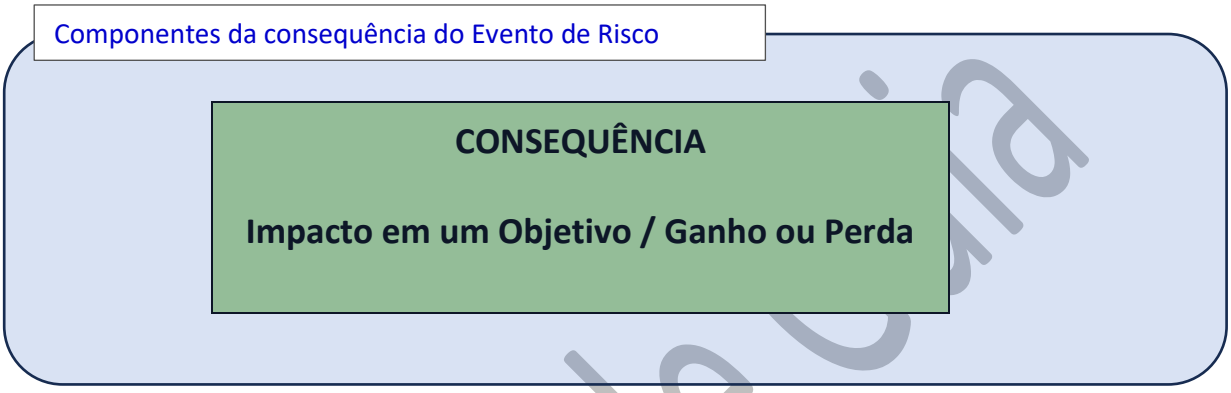


Figura 9: Componentes da Consequência do Evento de Risco

O quadro a seguir mostra as etapas da descrição do efeito da atuação negativa da entrega/resultado no Objetivo disposto no planejamento, ocasionando consequências para a organização:

Consequência = efeitos + atuação negativa na iniciativa e no objetivo	
Descrição dos efeitos da atuação negativa da entrega/resultado no objetivo disposto no planejamento.	Descrição da consequência da atuação negativa na inciativa e no objetivo disposto no planejamento.

Tabela 2 - Consequência Efeitos e Objetivos.

Já o evento de risco refere-se à ocorrência de um incidente ou irregularidade que pode comprometer os objetivos da organização. Ele representa a materialização de um risco identificado e pode ter impactos variados.

São definidos como riscos ao planejamento os eventos ou circunstâncias que têm potencial para comprometer, no todo ou em parte, entregas, resultados pretendidos, iniciativas, metas, indicadores ou ações necessárias ao alcance dos objetivos, observando seus desdobramentos.

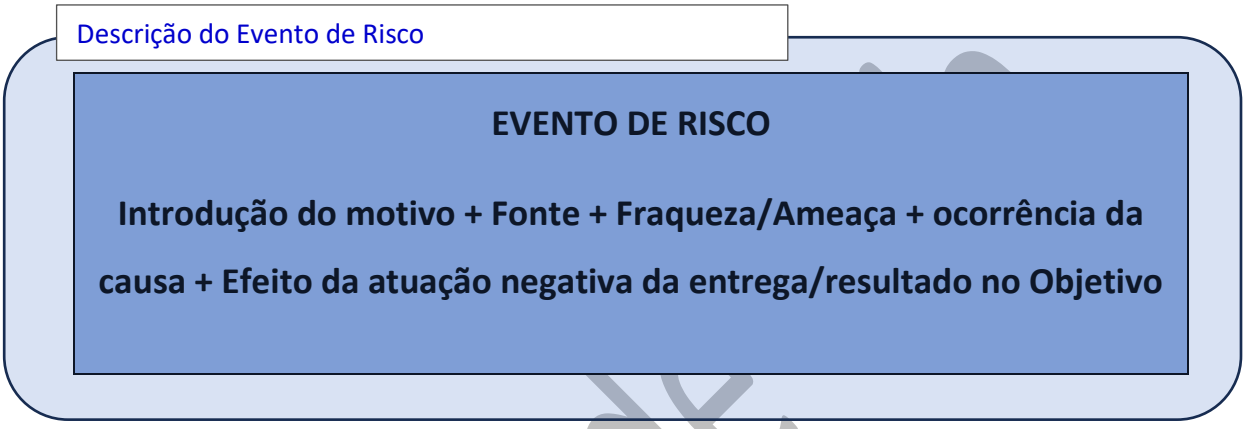


Figura 10: Descrição do Evento de Risco

A análise de riscos pode ser influenciada por divergências de opiniões, vieses, percepções do risco e julgamentos. Influências adicionais são a qualidade da informação utilizada, as hipóteses e as exclusões feitas, quaisquer limitações das técnicas e como elas são executadas. Convêm que estas influências sejam consideradas e comunicadas aos tomadores de decisão, quando significativas.

A análise de riscos fornece insumos para a avaliação de riscos, para decisões sobre se o risco necessita ser tratado e como, e sobre a estratégia e os métodos mais apropriados para o tratamento de riscos. Os resultados propiciam discernimento para decisões, em que escolhas estão sendo feitas e as opções envolvem diferentes tipos e níveis de risco.

3.5 AVALIAÇÃO DE RISCOS

A avaliação de riscos é um processo essencial para garantir a integridade, eficiência e conformidade das operações organizacionais.

Posteriormente à análise, procede-se a avaliação dos riscos cujo propósito é apoiar decisões com base no nível de risco.

Um risco é avaliado em termos de probabilidade de sua ocorrência e do impacto que pode causar nos objetivos organizacionais caso se materialize. Quanto maior a probabilidade e maior o impacto, maior é o nível do risco.

Nesta etapa são estimados os níveis dos riscos identificados, a partir de critérios de probabilidade e impacto (estimativas a partir da percepção e experiência dos participantes). Os principais riscos associados aos objetivos estratégicos do MD devem ser avaliados quanto ao grau de impacto que podem trazer ao tempo, qualidade, custos, viabilidade ou resultados das iniciativas, combinado com a probabilidade de ocorrência do evento.

Trata-se, portanto, de uma análise qualitativa, na qual a equipe de gestão de riscos irá ponderar, para cada risco identificado, o grau de impacto e a sua probabilidade de ocorrer. Assim:

- a probabilidade é a chance de o evento ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado pretendido e está associada a um incidente ou uma ocorrência potencial (chance de o evento vir a ocorrer, a partir de fontes internas ou externas) (p.ex.: um evento cuja ocorrência seja quase certa de acontecer é um evento de alta probabilidade); e
- o impacto avalia o potencial comprometimento do objetivo/resultado pretendido e está associado à consequência do evento ocorrido (materialização do risco). (p.ex.: um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto).

Para se determinar o nível de risco, é necessário atribuir graus de probabilidade e de impacto. Desta forma, serão utilizadas escalas qualitativas com amplitude de 5 (cinco) níveis para probabilidade e também para impacto, de acordo com os seguintes critérios:

Tabelas para análise de risco no MD – Escalas de Probabilidade

Probabilidade	Descrição	Critério
1	Muito Baixa	**Evento extraordinário** para os padrões conhecidos da gestão e operações do processo. Embora possa assumir dimensão estratégica para a manutenção do processo, **não há histórico disponível de sua ocorrência.**
2	Baixa	**Evento casual, inesperado**. Muito embora raro, há histórico conhecido de sua ocorrência por parte dos principais gestores e operadores do processo.
3	Média	**Evento esperado**, que se reproduz com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo.
4	Alta	**Evento usual, corriqueiro**. Devido à sua ocorrência habitual ou conhecida em uma dezena ou mais de caos, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo.
5	Muito Alta	**Evento se reproduz muitas vezes**, se repete seguidamente, de maneira assídua, numerosa e, não raro, de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo.

Figura 11: Escala de Probabilidade (Plano de Gestão de Riscos EMCFA)

Tabelas para análise de risco no MD – Escalas de Impacto

Impacto	Descrição	Critério
1	Muito Baixo	Degradação de operações, atividades, projetos, programas ou da organização, porém causando **impactos mínimos** nos objetivos (de tempo, prazo, custos, quantidade, qualidade, acesso, escopo, imagem, etc) relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).
2	Baixo	Degradação de operações, projetos, programas ou processos da organização, causando **impactos pequenos** nos objetivos.
3	Médio	Interrupção de operações ou atividades da organização, de projetos, programas ou processos, causando **impactos significativos** nos objetivos, **porém recuperáveis.**
4	Alto	Interrupção de operações, atividades, projetos, programas ou processos da organização, causando **impactos de reversão muito difícil** nos objetivos.
5	Muito Alto	Interrupção abrupta de operações, atividades, projetos, programas ou processos da organização, **impactando fortemente outros processos**, causando **impactos de dificílima reversão** nos objetivos.

Figura 12: Escala de Impacto (Plano de Gestão de Riscos EMCFA)

É possível que sejam identificados um número elevado de riscos. Entretanto, como os recursos são limitados, há a necessidade de se estabelecer a prioridade sobre quais riscos serão tratados primeiro.

Assim, um risco é avaliado, racionalmente, em termos de probabilidade de ocorrência e impacto sobre os objetivos organizacionais do MD, nos seus diversos níveis. Quanto maior a probabilidade e maior o impacto, maior é o nível do risco.

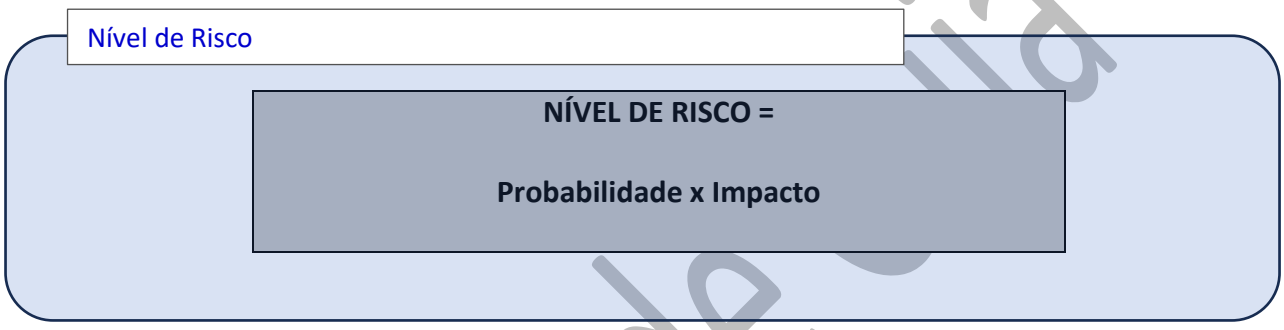


Figura 13: Nível de Risco

Com o intuito de associar o nível do risco com a prioridade para o tratamento, foram estabelecidos cinco faixas que enquadram as classificações dos níveis de risco para priorização:

25	**Risco Crítico**
15 - 20	**Risco muito alto**
10 - 12	**Risco alto**
6 - 9	**Risco médio**
1 - 5	**Risco baixo**

Tabela 3 - Escalas de Classificação dos Níveis de Risco

Dessa forma, foi utilizada a matriz Probabilidade X Impacto, a seguir apresentada. A partir dela, o produto dos conceitos probabilidade e impacto de cada risco são posicionados e enquadrados nas faixas dos níveis supracitados.

Matriz de análise de risco no MD - Probabilidade x Impacto

Legenda Nível de Risco: Risco Crítico Risco Muito Alto Risco Alto Risco Médio Risco Baixo		Probabilidade				
		1 Muito Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
Impacto	5 Muito Alto	5	10	15	20	25
	4 Alto	4	8	12	16	20
	3 Médio	3	6	9	12	15
	2 Baixo	2	4	6	8	10
	1 Muito Baixo	1	2	3	4	5

Figura 14: Matriz Probabilidade X Impacto

3.6 TRATAMENTO DE RISCOS

O planejamento de respostas aos riscos é o processo de desenvolvimento de ações para potencializar as oportunidades e reduzir as ameaças para os objetivos estratégicos do MD listados no Planejamento. Trata as respostas aos riscos conforme sua prioridade.

De modo geral, considera-se que os eventos de riscos situados nos quadrantes definidos como risco crítico e risco muito alto são indicativos de necessidade de acompanhamento mais próximo e controles mais rígidos, enquanto os riscos situados nos quadrantes de risco baixo e médio sinalizam para controles mais moderados. Em alguns casos não há necessidade de implementar controles, sendo possível, inclusive, a retirada de controles em algumas situações.

O tratamento de riscos consiste na adoção de medidas para mitigar, transferir, aceitar ou eliminar riscos que possam comprometer os objetivos organizacionais.
A escolha das ações de tratamento deve ser baseada em uma análise criteriosa dos riscos identificados, considerando sua probabilidade, impacto e os controles existentes, devendo estar alinhada ao apetite de risco do MD.

Segundo a ISO 31000:2018, o tratamento do risco:

- é o processo de modificar o risco; e
- consiste em determinar uma resposta que seja a mais adequada para modificar a probabilidade ou a consequência (impacto) de um risco.

Adicionalmente pode envolver:

- remoção da fonte de risco;
- alteração de probabilidade;
- alteração de consequências;
- compartilhamento do risco com outra parte; e
- evitar o risco pela decisão de não iniciar ou descontinuar uma atividade.

Assim, no tratamento de riscos, existem quatro posturas possíveis:

Postura	Definição
Aceitar	Tolerar o risco.
Mitigar	Tomar ações para restringi-los a um nível aceitável, reduzindo as chances de ocorrência (probabilidade) e/ou seu impacto.
Transferir	Incumbir outra organização ou agente das ações para mitigar o risco.
Eliminar	Alterar o plano ou processo ou findar a atividade que gerou o risco.

Tabela 4 - Possíveis respostas aos riscos

Existem várias estratégias ou combinação de estratégias que podemos adotar com relação a riscos:

a. Mitigar

Um grande número de riscos será tratado desta forma. O propósito desta ação é que, mesmo continuando com a iniciativa que deu origem ao risco, a organização adote ações administrativas

de controle para conter o risco em um determinado nível. Implica a redução da probabilidade e/ou impacto de um evento de risco para dentro de limites aceitáveis.

b. Transferir

Para alguns riscos, a melhor resposta pode ser transferi-los para terceiros. Isto pode ser feito por meio de seguros ou contratualmente através de cláusulas específicas e garantias. A opção do seguro é particularmente útil para mitigar riscos financeiros ou riscos de ativos.

A transferência de riscos também pode ser considerada para transferir o nível de exposição da organização ou porque outra organização é mais capaz de gerenciar o risco. É importante notar que alguns riscos não são totalmente transferíveis (em particular geralmente não é possível transferir risco de reputação e imagem, mesmo se a entrega dos serviços foi contratada para um terceiro). O relacionamento com o terceiro para o qual o risco foi transferido deve ser muito bem gerenciado para assegurar êxito na transferência. As contratações por meio de licitações podem conter cláusulas específicas que tratem de transferência de riscos para o licitante, contudo esse tipo de prática acarreta ônus para o contratante.

c. Eliminar

Alguns riscos podem ser tratados somente pela alteração dos objetivos envolvidos, de escopo, alteração de requisitos e do cronograma, e até pelo término da atividade, e do processo ou projeto. Esta opção pode ser particularmente adotada em projetos em que a relação custo/benefício coloca o projeto em nível de risco inaceitável.

d. Aceitar

Aceitar significa que a exposição ao risco é tolerada sem que nenhuma ação específica seja tomada. Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco. Mesmo se o risco estiver acima da faixa de apetite, a capacidade para fazer alguma coisa com relação ao risco pode ser limitada, ou o custo de tomar uma ação pode ser desproporcional ao benefício potencial gerado. Nesses casos, a resposta pode ser tolerar o nível de risco. Esta opção, é claro, pode ser suplementada por um plano de contingência/ Plano de Continuidade do Negócio (PCN) para conter os impactos que adviriam caso a ameaça acorra.

4. CONTROLES INTERNOS DA GESTÃO

A atividade de controle se constitui em políticas e procedimentos estabelecidos e implementados que contribuem para assegurar que a resposta ao risco definida pela decisão da gestão da organização seja executada. Ocorre em todos os níveis da organização e, também, em todas as funções, compreendendo em ações típicas de aprovação, autorização, verificação, reconciliação e revisão do desenho operacional, da segurança de bens e da segregação de responsabilidades.

Nessa etapa são estabelecidos os controles internos da gestão proporcionais ao nível de riscos a que o Ministério da Defesa está exposto, considerando conforme parâmetros definidos na resolução CG-MD nº 3, de 25 de novembro de 2024 - Política de Gestão de Riscos do Ministério da Defesa.

Sobre esta etapa, sugere-se, considerando a relação entre o custo-benefício e a geração de valor público, a observância do quadro a seguir:

Nível de Risco	Ação Necessária e Critérios
Crítico	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser encaminhado ao proprietário de riscos, devendo ser submetido à supervisão da AESPI e posterior envio ao SGRI para análise da medida de controle interno da gestão mais adequada por meio de recomendação específica a ser encaminhada para homologação do CG-MD.
Muito Alto	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser encaminhado ao proprietário de riscos, devendo ser submetido à supervisão da AESPI e posterior envio ao SGRI para análise da medida de controle interno da gestão mais adequada por meio de recomendação.
Alto	Nível de risco além do apetite a risco. Requer medida de controle interno pelo proprietário de riscos, com atividades de monitoramento.
Médio	Nível de risco além do apetite a risco. Requer medida de controle interno pelo proprietário de riscos, com atividades de monitoramento.
Baixo	Nível de risco dentro do apetite a risco. É possível que existam oportunidades de maior retorno que possam ser exploradas assumindo-se mais riscos, com uma avaliação da relação entre custo e benefício, como diminuir o nível de controles.

Tabela 5 - Ações Necessárias em resposta aos riscos

Fonte: Adaptado do Roteiro de Avaliação de Maturidade da Gestão de Riscos (TCU, 2018)

Para definição do apetite aos riscos, deve-se utilizar como parâmetro aceitar a existência de um risco identificado e mensurado sem que exista uma ação necessária para evitar, reduzir ou compartilhar.

4.1 IDENTIFICAÇÃO E ACOMPANHAMENTO DOS CONTROLES INTERNOS DA GESTÃO

É essencial que os riscos, suas causas e respectivas consequências sejam descritos com clareza, objetividade e precisão. A consistência nessa correlação é fundamental para assegurar uma análise robusta e embasar decisões mais estratégicas e eficazes no âmbito da gestão de riscos

Segundo a Política de Gestão de Riscos do MD o Controles Internos da Gestão é o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os objetivos serão alcançados.

É importante destacar que inicialmente a administração deve levar em conta os riscos inerentes às iniciativas estratégicas constantes no PEO.

Risco Inerente é o risco que se apresenta na ausência de qualquer medida gerencial (controle) que poderia alterar a probabilidade ou o impacto de sua materialização.

Após a identificação dos riscos, causas e consequências, é necessário identificar quais controles estão presentes nas etapas de execução das iniciativas e mitigam os riscos identificados.

Após feita a identificação dos controles existentes, devem ser levantados os riscos que resistem à atuação das medidas já adotadas (controles existentes), considerando a avaliação inicial. Assim, os riscos são avaliados quanto à sua condição de inerentes e residuais.

Risco Residual é aquele que ainda permanece após a resposta da administração mediante a implementação de controles.

Após se identificar os controles associados aos riscos identificados é importante tentar identificar outros controles presentes no processo, possibilitando a identificação de outros riscos ou até mesmo de controles puramente burocráticos.

Ao propor controles, é fundamental que o gestor de risco considere as informações identificadas desde o início, com ênfase na etapa de identificação de riscos.

O gestor de risco deve, portanto, desenvolver alternativas para implementação de controles que mitiguem os riscos de forma preventiva, caso atenuem suas fontes, ou de forma corretiva, se atuarem sobre os efeitos dos riscos.

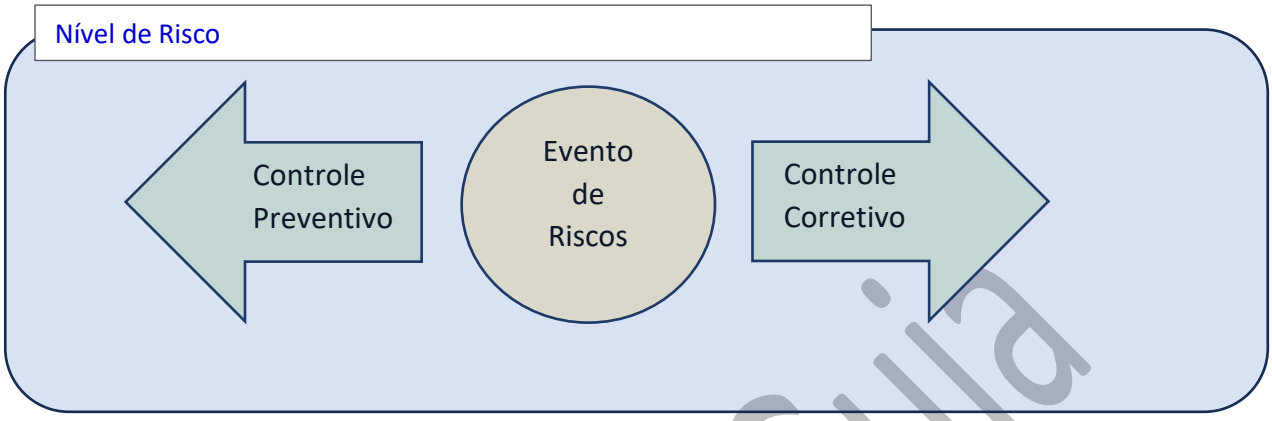


Figura 15: Controles preventivos e corretivos

Os controles podem ser classificados em:

- Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos / checklist definidos para o processo e capacitação dos servidores envolvidos no processo.
- Controles de atenuação e recuperação (corretivos): controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.
- Controles detectivos: controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

Após escolhido o tipo de resposta e definido o controle mais adequado para tratar os riscos que estão fora do limite de exposição a riscos da organização, o gestor de riscos deve planejar as ações que serão tomadas para tratamento de cada risco.

5. MONITORAMENTO

O monitoramento e a análise são componentes fundamentais da gestão de riscos e compreendem o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos. Busca propiciar que os processos e controles estabelecidos funcionem de forma eficaz e contínua.

Assim, por meio da observação sistemática, da coleta de dados e da avaliação de desempenho, é possível identificar falhas, desvios e oportunidades de melhoria. Esse acompanhamento constante, inclusive no que se refere à implementação do Plano de Gestão de Riscos, permite à organização ajustar suas estratégias, reforçar a conformidade com normas e regulamentos, e assegurar que os objetivos institucionais sejam alcançados com segurança e eficiência. O monitoramento deve ser efetivo sem onerar demasiadamente o processo.

Nesta etapa, as atividades definidas pela estratégia de gerenciamento de riscos devem ser acompanhadas visando identificar se riscos ainda existem, se novos riscos apareceram, se a probabilidade e/ou impacto dos riscos mudaram, de modo a reportar mudanças significativas que alteram o nível de riscos, e assegurar a eficácia do controle.

Para o monitoramento de riscos, deve-se:

- monitorar se o perfil de risco está mudando;
- adotar as ações preventivas e corretivas necessárias;
- verificar a implementação e os resultados do tratamento dos riscos de forma a garantir que o gerenciamento de riscos está sendo efetivo;

Caberá às Chefias e às Secretarias do Ministério da Defesa verificarem a situação atual e as ações que estão sendo adotadas em relação ao tratamento dos riscos dos Objetivos Estratégicos (OEE) sob suas respectivas responsabilidades. Deve-se estabelecer a frequência de monitoramento dos riscos de acordo com o nível do risco e demais parâmetros relacionados ao risco identificado, a critério do órgão responsável.

A Política de Gestão de Riscos do Ministério da Defesa - PGR-MD, define alguns direcionadores para as atividades de monitoramento e supervisão da gestão de riscos, merecendo destaque o disposto no art. 14, que trata das competências dos proprietários de riscos:

> "Art. 14. Cabe aos proprietários de riscos:
> I - assegurar que o risco seja gerenciado de acordo com a Política de Gestão de Riscos e demais normas sobre o assunto;

II - monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a Política de Gestão de Riscos e demais normas sobre o assunto;
III - informar, de acordo com o previsto nas normas referentes à gestão de riscos, tempestivamente, a situação do gerenciamento dos riscos e se as medidas de controle definidas estão adequadas para o tratamento dos riscos; e
IV - propor medidas de controle mais adequadas às peculiaridades de seus processos."

6. COMUNICAÇÃO E CONSULTA

Refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo.

Comunicar riscos é fornecer as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco.

Ao promover o diálogo contínuo entre gestores, colaboradores e partes interessadas, a organização fortalece a compreensão dos riscos, melhora a tomada de decisões e assegura que os controles internos da gestão estejam alinhados com os objetivos estratégicos.

A comunicação e consulta com partes interessadas apropriadas externas e internas, no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos, potencializa o alcance dos resultados.

7. REGISTRO E RELATO

Convém que o processo de gestão de riscos do Ministério da Defesa e seus resultados sejam documentados e relatados por meio de mecanismos apropriados. O registro e o relato visam:

- comunicar atividades e resultados de gestão de riscos em toda a organização;
- fornecer informações para a tomada de decisão;
- melhorar as atividades de gestão de riscos;
- auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

As decisões relativas à criação, retenção e manuseio de informação documentada levem em consideração, mas não se limitem a: o seu uso, a sensibilidade da informação e os contextos externo e interno.

O relato é parte integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a Alta Administração do MD e os órgãos de supervisão a cumprirem suas responsabilidades. Os fatores a considerar para o relato incluem, mas não estão limitados a:

- diferentes partes interessadas e suas necessidades específicas de informação e requisitos;
- custo, frequência e pontualidade do relato;
- método de relato;
- pertinência da informação para os objetivos organizacionais e para a tomada de decisão.

8. CONSIDERAÇÕES

A gestão de riscos no âmbito do Ministério da Defesa representa um compromisso institucional com a excelência, a integridade e a efetividade na condução das ações estratégicas voltadas à defesa nacional. Alinhado ao Plano Estratégico Organizacional 2024–2027, este guia consolida uma abordagem estruturada, integrada e contínua, voltada à identificação, à análise, à avaliação, ao tratamento, ao monitoramento e à comunicação dos riscos que possam comprometer a missão institucional e a integridade dos processos.

O alinhamento com o PEO reforça a necessidade de uma atuação coordenada e transversal, que envolva todos os níveis organizacionais e promova uma cultura de integridade e responsabilidade compartilhada. A gestão de riscos deve ser incorporada aos processos decisórios, aos planos de ação e aos mecanismos de controle interno, de forma a garantir que os recursos sejam utilizados de maneira eficiente, segura e orientada para resultados.

Ele reafirma a importância da atuação preventiva, da identificação proativa de vulnerabilidades e da implementação de controles eficazes, contribuindo para a resiliência institucional e a proteção dos interesses estratégicos. A consolidação de uma abordagem sistêmica e integrada de gestão de riscos permitirá ao Ministério da Defesa enfrentar os desafios com maior segurança, transparência e responsabilidade.

Assim, a efetividade da gestão de riscos depende do comprometimento institucional, da liderança engajada e da participação ativa dos servidores civis e militares. A consolidação dessa prática como parte integrante da cultura organizacional é essencial para que o Ministério da Defesa continue a cumprir sua missão com excelência.

Por fim, reforça-se que a gestão de riscos não é um fim em si mesma, mas um instrumento de apoio à missão institucional, à valorização das pessoas e à promoção do esforço integrado de todos. Seu êxito depende do engajamento contínuo de todos os níveis organizacionais, da capacitação permanente e da melhoria dos processos, em consonância com os valores que norteiam a atuação do Ministério da Defesa.

REFERÊNCIAS BIBLIOGRÁFICAS

Associação Brasileira de Normas Técnicas. ABNT. NBR ISO 31073:2022 - Gestão de riscos - Vocabulário. Rio de Janeiro, 2022.

Associação Brasileira de Normas Técnicas. ABNT. NBR ISO/IEC 31010:2012. Gestão de Riscos: Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012.

Associação Brasileira de Normas Técnicas. ABNT. NBR ISO 31000:2018. Gestão de Riscos: Diretrizes. Rio de Janeiro, 2018.

Ministério da Defesa. Política de Gestão de Riscos do Ministério da Defesa – PGR-MD. Resolução CG-MD nº 3, de 25 de novembro de 2024.gov

Ministério da Gestão e da Inovação em Serviços Públicos (MGI).Guia de Gestão de Riscos – 1ª edição. Brasília: MGI, 2025.gov

Instituto Federal de Pernambuco (IFPE). Política e Plano de Gestão de Riscos do IFPE. Resolução CONSUP nº 225/2023 e CGRC nº 11/2024.ifpe

Tribunal de Contas da União (TCU). Referencial Básico de Gestão de Riscos. Brasília: TCU, 2018.tcu

Controladoria-Geral da União (CGU). Gestão de Riscos no Poder Executivo Federal. Brasília: CGU, 2024.gov

Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal.

Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016. Estabelece diretrizes para controles internos, gestão de riscos e governança.

COSO ERM.Enterprise Risk Management – Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission.

Tribunal de Contas da União (TCU). Referencial Básico de Gestão de Riscos. Brasília: TCU, 2018. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/referencial-basico-de-gestao-de-riscos.tcu

Controladoria-Geral da União (CGU). Referencial Básico de Gestão de Riscos. Brasília: CGU, 2018. Disponível em: https://repositorio.cgu.gov.br/handle/1/33144.cgu

Ministério da Defesa. Referencial Básico de Gestão de Riscos. Brasília: Ministério da Defesa, 2022. Documento interno disponível na seção de Governança do Setor de Defesa.

BRASIL. Ministério da Defesa. Resolução CG-MD nº 2, de 18 de dezembro de 2023. Aprova o Planejamento Estratégico Organizacional do Ministério da Defesa 2024–2027 (PEO-MD 2024–2027). Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca/colegiados/governanca-md/resolucoes-1. Acesso em: 12 set. 2025.

BRASIL. Ministério da Defesa. Resolução CONSUG-MD nº 20, de 27 de novembro de 2024. Aprova o Planejamento Estratégico Setorial de Defesa – PESD 2024–2035. Diário Oficial da União, Brasília, DF, 29 nov. 2024. Disponível em: https://www.gov.br/defesa/pt-br/orgaos-vinculados/conselho-superior-de-governanca-do-ministerio-da-defesa/arquivos/resolucao-consug-md-no-20-de-27-de-novembro-de-2024-dou-imprensa-nacional.pdf. Acesso em: 12 set. 2025.

BRASIL. Ministério da Defesa. Resolução CG-MD nº 3, de 25 de novembro de 2024. Aprova a Política de Gestão de Riscos do Ministério da Defesa – PGR-MD. Diário Oficial da União, Brasília, DF, 10 dez. 2024. Seção 1, p. 35. Disponível em: https://www.gov.br/defesa-exercito/pt-br/acesso-a-informacao/governanca/colegiados/governanca-md/resolucoes-1/arquivos/resolucao-cg-md-no-3-de-25-de-novembro-de-2024-dou-imprensa-nacional.pdf. Acesso em: 12 set. 2025.

BRASIL. Ministério da Defesa. Resolução CG-MD nº 1, de 12 de novembro de 2021. Aprova o Regimento Interno do Comitê de Governança do Ministério da Defesa. Diário Oficial da União, Brasília, DF, 22 dez. 2021. Seção 1, p. 156. Disponível em: https://www.gov.br/defesa/pt-br/acesso-a-informacao/governanca-e-gestao/colegiados/governanca-md/arquivos/resolucao-no-1-cg-md-md-de-12-de-novembro-de-2021_aprova-regimento-interno-republicada.pdf. Acesso em: 12 set. 2025.

BRASIL. Lei nº 14.133, de 1º de abril de 2021. Estabelece normas gerais de licitação e contratação para as administrações públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios. Diário Oficial da União, Brasília, DF, 1 abr. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14133.htm. Acesso em: 12 set. 2025.

BRASIL. Decreto nº 9.991, de 28 de agosto de 2019. Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da administração pública federal direta, autárquica e fundacional, e regulamenta dispositivos da Lei nº 8.112, de 11 de dezembro de 1990. Diário Oficial da União, Brasília, DF, 29 ago. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9991.htm. Acesso em: 12 set. 2025.

BRASIL. Decreto nº 11.337, de 1º de janeiro de 2023. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das gratificações do Ministério da Defesa, e remaneja cargos em comissão, funções de confiança e gratificações. Diário Oficial da União, Brasília, DF, 1 jan. 2023. Edição especial. Disponível

em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11337.htm. Acesso em: 12 set. 2025.

BRASIL. Decreto nº 11.579, de 27 de junho de 2023. Altera o Decreto nº 11.337, de 1º de janeiro de 2023, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das gratificações do Ministério da Defesa, e remaneja e transforma cargos em comissão, funções de confiança e gratificações. Diário Oficial da União, Brasília, DF, 28 jun. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11579.htm. Acesso em: 12 set. 2025.

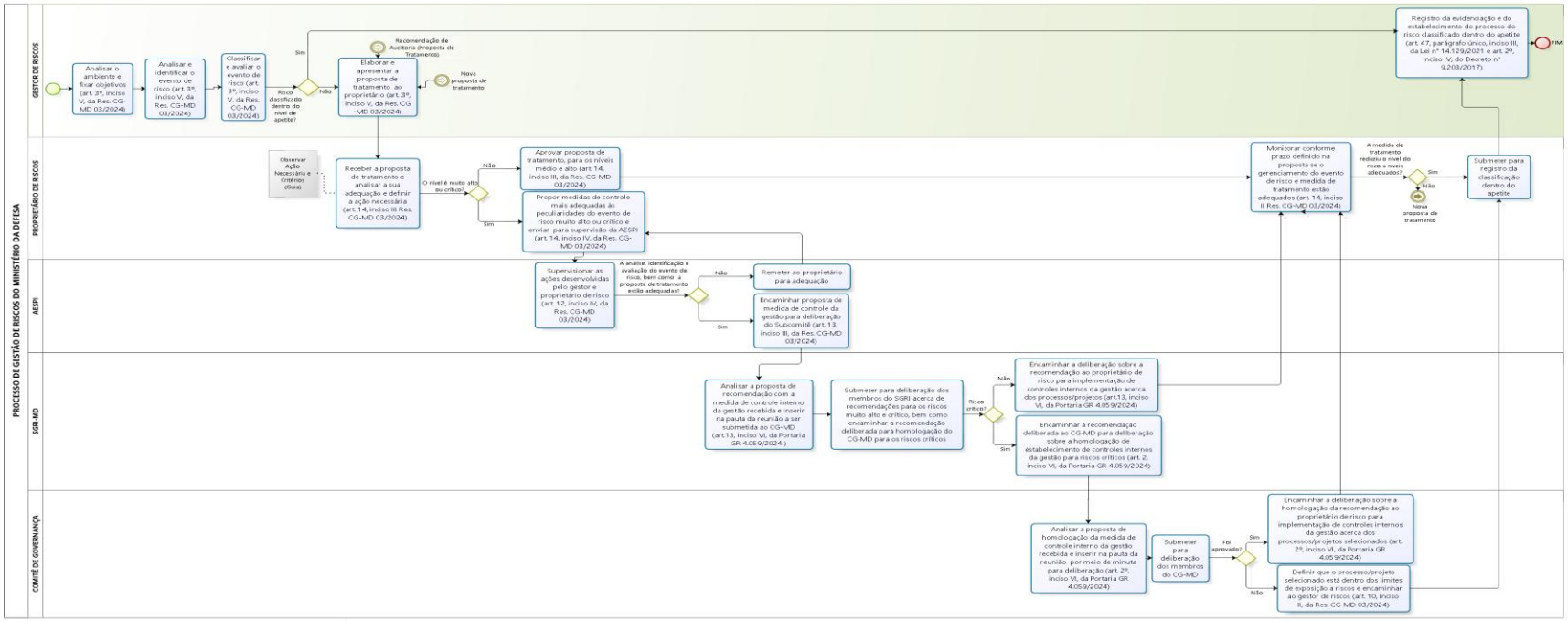
BRASIL. Decreto nº 11.337, de 1º de janeiro de 2023. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das gratificações do Ministério da Defesa, e remaneja cargos em comissão, funções de confiança e gratificações. Diário Oficial da União, Brasília, DF, 1 jan. 2023. Edição especial. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11337.htm. Acesso em: 12 set. 2025.

BRASIL. Decreto nº 11.579, de 27 de junho de 2023. Altera o Decreto nº 11.337, de 1º de janeiro de 2023, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das gratificações do Ministério da Defesa, e remaneja e transforma cargos em comissão, funções de confiança e gratificações. Diário Oficial da União, Brasília, DF, 28 jun. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11579.htm. Acesso em: 12 set. 2025.

BRASIL. Superior Tribunal de Justiça. Manual de Consultoria: exercício 2023. Brasília, DF: Secretaria de Auditoria Interna – AUD, 2023. Disponível em: https://bdjur.stj.jus.br/server/api/core/bitstreams/bfae7811-e3fd-4a0a-bc98-ea54e36f995a/content. Acesso em: 12 set. 2025.

BRASIL. Controladoria-Geral da União. Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Brasília, DF: CGU, 2017. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/auditoria-e-fiscalizacao/arquivos/manual-de-orientacoes-tecnicas-2017.pdf/@@download/file. Acesso em: 12 set. 2025.

ANEXO A – PROCESSO DE GESTÃO DE RISCOS MD



MINISTÉRIO DA
DEFESA

ANEXO B – ESTABELECIMENTO DO CONTEXTO E FIXAÇÃO DOS OBJETIVOS

CONTEXTO, ESCOPO e OBJETO

UNIDADE	
NOME	
MISSÃO	
VISÃO	

DEFINIÇÃO DO OBJETO	
OBJETIVO ESTRATÉGICO DO PEO	
INICIATIVA	
STATUS	
SITUAÇÃO	
TÉRMINO	
ENTREGA	
RESULTADOS ALCANÇADOS	
RESULTADOS PRETENDIDOS (PRÓXIMOS PASSOS)	
ORÇAMENTO ANUAL	
INICIATIVA DESENHADA / DETALHADA?	

ANÁLISE SWOT (DO PROCESSO)

FORÇAS	FRAQUEZAS

OPORTUNIDADES	AMEAÇAS

ANEXO C – ANÁLISE AMBIENTAL

A análise ambiental SWOT (STRENGTHS, WEAKNESSES OPPORTUNITIES, THREATS) é usada para identificar os pontos fortes e fracos da sua unidade, e as principais oportunidades e ameaças, na gestão de riscos de um objeto. Está alinhada à visão moderna da gestão de riscos, que não busca apenas identificar potenciais problemas, mas também oportunidades.

Com isso, permite visualizar se a organização possui forças internas suficientes para enfrentar as ameaças (riscos negativos) ou para aproveitar as oportunidades (riscos positivos). Além disso, ajuda a identificar se as fraquezas são tais que possam inviabilizar o objeto.

ANÁLISE DO AMBIENTE INTERNO

Pontos Fortes

Descreva seus diferenciais.

Pontos Fracos

Descreva suas principais deficiências. Pontos a serem melhorados ou revistos.

ANÁLISE DO AMBIENTE EXTERNO

Oportunidades

Descreva as principais oportunidades identificadas. Eventos potenciais que podem gerar grandes benefícios.

Ameaças

Descreva as principais ameaças identificadas. Eventos potenciais que podem causar um grande estrago ao projeto ou entrega.

CONCLUSÃO

Procure relacionar os pontos fracos e fortes, com as ameaças e oportunidades, a fim de se ter uma análise mais abrangente do ambiente em que o objeto está inserido.

MINISTÉRIO DA
DEFESA

ANEXO D – IDENTIFICAÇÃO, ANÁLISE, AVALIAÇÃO E DESCRIÇÃO DO EVENTO DE RISCO

Nº	SETOR	EVENTO						FIXAÇÃO DOS OBJETIVOS				PROBABILIDADE	IMPACTO	NÍVEL DE RISCO	EVENTO DE RISCO
			CAUSA												
		Introdução do motivo do evento de riscos (A)	Fonte (B)	Fraqueza/ Ameaça (C)	Ocorrência da Causa (Nível e Descrição) (D)	Efeito da atuação negativa da entrega/resultado no Objetivo (Nível e Descrição) (E)	Descrição da Entrega ou Resultado Esperado	Conectivo de atuação negativa	Descrição da Iniciativa	Conectivo	Descrição do Objetivo	Ocorrência da Causa (Nível e Descrição)	Efeito da atuação negativa da entrega/resultado no Objetivo (Nível e Descrição)	Multiplicação do Nível de Probabilidade e do Impacto (Nível e Descrição)	Transcrever o evento conforme escrito nas colunas A+B+C+D+E
Ordem crescente dos eventos	Descrever o setor do MD responsável pelo Objetivo o objeto descrito na análise do ambiente	Ex: Em Razão da; Por causa de; Em virtude de; Em decorrência de; Por conta de; Resultante de; Motivado por; Tendo em vista; Por efeito de ; Como consequência de;	Fonte de Riscos conforme Tabela XXXX	Ex: Fraqueza ou Ameaça conforme análise SWOT, elaborada na Análise do Amb0069ente	poderá acontecer	Ex: retardar; prorrogar; cancelar; suspender; impossibilitar; prejudicar; anular	Ex: entrega ou resultado previsto no descritivo do PEO ou do Plano de Ação ou do Indicador	Ex: prejudicando; constrangendo; lesando; comprometendo; atrapalhado; enfraquecendo; desfavorecendo; dificultando;	Transcrever a iniciativa do objeto descrito na análise do ambiente	Ex: portanto assim logo por conseguinte desse modo dessa forma em consequência como resultado por isso de modo consequente	Transcrever o objetivo do objeto descrito na análise do ambiente	Descrever conforme níveis da Tabela para análise de risco no MD - Fator Probabilidade XXXXXX	Descrever conforme níveis da Tabela para análise de risco no MD - Fator Impacto XXXXXX	Descrever conforme níveis da Matriz de análise de risco no MD - Probabilidade x Impacto	Transcrever o conteúdo das colunas realizando os ajustes dos conectivos e respectiva concordância

MINISTÉRIO DA
DEFESA

ANEXO E – TRATAMENTO DE RISCOS, IDENTIFICAÇÃO, ACOMPANHAMENTO E MONITORAMENTO DOS CONTROLES INTERNOS DA GESTÃO

AÇÕES DE TRATAMENTO DE RISCOS								
Riscos	Nível de Risco	Apetite	Tipo de Resposta	Controle Proposto	Como Será Implantado?	Responsável	Data de Início	Data de Conclusão