

METODOLOGIA DE GESTÃO DE RISCOS

1ª Edição / 2022

Brasília – DF

**MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES**



METODOLOGIA DE GESTÃO DE RISCOS

**1ª Edição/ 2022
Brasília-DF**

**MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES**



Esta metodologia foi referendada pelo Comitê Técnico de Gestão de Riscos – CTGR-MCTI, na Reunião Extraordinária realizada em 29 de abril de 2022, e aprovada pelo Comitê Interno de Governança deste Ministério – CIG-MCTI, na 4ª Reunião Ordinária realizada em 30 de maio de 2022.

B823m

Brasil. Ministério da Ciência, Tecnologia e Inovações.

Metodologia de gestão de riscos / Ministério da Ciência, Tecnologia e Inovações. 1. ed. -- Brasília: Ministério da Ciência, Tecnologia e Inovações, 2022.

60 p.

ISBN: 978-65-87432-52-6

1. Gestão de riscos – Metodologia. I. Título

CDU 005.52:005.334:35(81)

Ficha catalográfica elaborada por: Lorena Nelza Ferreira Silva – CRB-1/2474

Ministério da Ciência, Tecnologia e Inovações

Paulo César Rezende de Carvalho Alvim
Ministro de Estado da Ciência, Tecnologia e Inovações

Sergio Freitas de Almeida
Secretário-Executivo

Johnny Ferreira dos Santos
Secretário-Executivo Adjunto Substituto

Christiane Gonçalves Corrêa
Secretária de Articulação e Promoção da Ciência - SEAPC

Marcelo Marcos Morales
Secretário de Pesquisa e Formação Científica - SEPEF

Marcelo Gomes Meirelles
Secretário de Estruturas Financeiras e de Projetos - SEFIP

José Gustavo Sampaio Contijo
Secretário de Empreendedorismo e Inovação - SEMPI

Alex Fabiano Ribeiro de Magalhães
Subsecretário de Unidades Vinculadas - SUV

Comitê Interno de Governança – GIG-MCTI
Membros

Ministro de Estado da Ciência, Tecnologia e Inovações (Presidente)

Secretário-Executivo

Secretário-Executivo Adjunto

Secretária de Articulação e Promoção da Ciência - SEAPC

Secretário de Pesquisa e Formação Científica - SEPEF

Secretário de Estruturas Financeiras e de Projetos - SEFIP

Secretário de Empreendedorismo e Inovação - SEMPI

Subsecretário de Unidades Vinculadas - SUV

Secretaria-executiva do CIG

Departamento de Governança Institucional – DGI/SEXEC

Comitê Técnico de Gestão de Riscos – CTGR

Membros

Johnny Ferreira dos Santos (titular)
Delciene Aparecida Oliveira Pereira (suplente)

Arthur Rodrigo Mota de Miranda (titular)
Natalia Fernandes Matano (suplente)

João Eduardo Tabalipa Ferreira (titular)
Marcella Souza Carneiro (suplente)

Vanessa Montiel Ventura (titular)
Agatha Kavalek de Lima (suplente)

Pedro Gontijo Menezes (titular)
Valdelice da Silva Souza (suplente)

Daniel Alves Natalizi (titular)
Giane Naves Emerick (suplente)

Cristina Vidigal Cabral de Miranda (titular)
César Augusto Rodrigues do Carmo (suplente)

Secretaria-executiva do CTGR

Coordenação-Geral de Gestão de Riscos e Avaliação – CGGR/DGI

Elaboração

Delciene Aparecida Oliveira Pereira

Fernando Silva de Souza

Flávio Fonte-Boa

Tereza Cristina Agut Gamba

Valéria Santana Marques Amaral

Colaboração

Coordenação Geral de Estruturação de Projetos – CGEP/DEPRO/SEFIP

Versão: 1.0 – 2022

SUMÁRIO

1. INTRODUÇÃO	7
2. NORMATIVOS, INSTÂNCIAS E ATORES	10
3. BASES TEÓRICAS	14
4. POLÍTICA DE GESTÃO DE RISCOS DO MCTI	16
5. PROCESSO DE GESTÃO DE RISCOS	19
5.1. PLANEJAMENTO DA APLICAÇÃO DA METODOLOGIA	21
5.2. ANÁLISE DO CONTEXTO	22
5.3. IDENTIFICAÇÃO DOS RISCOS	24
5.4. ANÁLISE DOS RISCOS	29
5.4.1. Identificação do risco inerente	29
5.4.2. Identificação dos controles internos da gestão existentes	33
5.4.3. Identificação do risco residual	36
5.5. AVALIAÇÃO DOS RISCOS	37
5.6. TRATAMENTOS DOS RISCOS	39
5.6.1. Validação dos resultados e do Plano de Tratamento dos Riscos	44
6. MONITORAMENTO	45
7. COMUNICAÇÃO	47
8. MELHORIA CONTÍNUA	48
9. CONSIDERAÇÕES FINAIS	49
10. REFERÊNCIAS	51
11. GLOSSÁRIO	53
ANEXOS	56

Lista de Figuras

Figura 1 - Princípios, estrutura e processo de gestão de riscos.	15
Figura 2 - Ciclo da Metodologia de Gestão de Riscos do MCTI	20
Figura 3 - Análise de <i>SWOT</i>	24
Figura 4 - Componentes do Evento de Risco	25
Figura 5 - <i>Bow Tie</i>	26
Figura 6 - Matriz de Riscos	32
Figura 7 - Controles internos da gestão no <i>Bow Tie</i>	34
Figura 8 - Matriz Simples de Risco e Tolerância ao Risco	38

Lista de Tabelas

Tabela 1 - Fontes de Riscos e Fragilidades	27
Tabela 2 - Escala de Avaliação de Probabilidade	30
Tabela 3 - Escala de Avaliação de Impacto	31
Tabela 4 - Classificação do Risco	32
Tabela 5 - Avaliação da efetividade dos controles existentes	36
Tabela 6 - Limite de Exposição ao Risco	38
Tabela 7 - Possibilidades de tratamento dos riscos	40
Tabela 8 - Ação recomendada perante o risco para cada classificação	41

1. INTRODUÇÃO

Incertezas e riscos são inerentes a praticamente quaisquer atividades dos seres humanos. Isso também se aplica ao contexto das organizações. Portanto, lidar com as inúmeras incertezas decorrentes dos vários fatores (econômicos, sociais, legais, tecnológicos, operacionais, dentre outros) é essencial para o atingimento dos objetivos almejados. Assim, a identificação prévia de potenciais eventos que poderão se materializar em riscos e comprometer o alcance dos objetivos é essencial para eficácia da gestão.

Nesse sentido, compreendendo a importância do aprimoramento das políticas e práticas de gestão como estratégia para a oferta de serviços públicos de maior qualidade para a população, à semelhança de outros países e também atento a diretrizes de organismos internacionais, como por exemplo a Organização para a Cooperação e Desenvolvimento Econômico – OCDE, o governo brasileiro vem envidando esforços significativos na direção da criação de uma cultura de governança e de gestão de riscos de forma estruturada no Poder Executivo Federal.

Com esse intuito, em 2016 foi publicada a Instrução Normativa Conjunta CGU/MP nº 01, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, e no ano seguinte, em 2017, foi publicado o Decreto nº 9.203, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

Com vistas ao cumprimento desses regulamentos, em 2017, o extinto Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC, regulamentou internamente a matéria. Mas, em decorrência das mudanças na estrutura regimental do órgão, ocorridas no segundo semestre de 2020, com a entrada em vigor de uma nova estrutura regimental na Pasta, definida por meio do Decreto 10.463, que criou o Ministério da Ciência, Tecnologia e Inovações – MCTI, houve a necessidade de revisar os normativos e iniciar ações com vistas à

estruturação e a implementação do processo de gestão de riscos no órgão recém-criado.

Como parte dessas ações, o MCTI publicou em 12 de janeiro de 2021 a Portaria nº 4. 301, que instituiu o Comitê Interno de Governança do Ministério da Ciência, Tecnologia e Inovações (CIG-MCTI), em conformidade com o Decreto 9.203/2017. Esse Colegiado é composto pela alta administração do órgão, ou seja, Ministro de Estado e Secretários. Seu pleno funcionamento é essencial para o aprimoramento do processo decisório sobre as várias temáticas constantes no rol de suas competências, dentre essas, a gestão de riscos.

Em setembro de 2021, o Comitê Interno de Governança do MCTI aprovou a Política de Governança Institucional e esta foi instituída por meio da Portaria MCTI Nº 5.205, de 28 de setembro de 2021.

Outro importante dispositivo neste contexto é a Política de Gestão de Riscos do MCTI (Portaria MCTI nº 5.305/2021) que apresenta os conceitos, princípios, objetivos, diretrizes e responsabilidades, que passam a nortear o desenvolvimento da cultura do gerenciamento de riscos. Além disso, esta Política também instituiu o **Comitê Técnico de Gestão de Riscos** que é instância colegiada interna de apoio à governança no tema gestão de riscos no âmbito deste órgão.

A metodologia ora proposta, prevista no art. 8º , inciso IV, da Portaria MCTI nº 5.305/2021, é um desdobramento desta Política e tem como objetivo orientar os gestores do órgão e suas equipes a realizar de forma sistematizada a identificação, avaliação e adoção de respostas aos eventos de riscos nos objetos da gestão de riscos¹ de suas unidades. Esta metodologia é composta por etapas encadeadas de forma que sua aplicação, monitoramento, avaliação e retroalimentação se constituem em um processo que possibilita promover a melhoria contínua da gestão de riscos no âmbito do MCTI, de modo a contribuir com o alcance da estratégia institucional.

¹ Objeto da gestão de riscos: qualquer processo de trabalho, atividade, projeto, iniciativa, ação de plano institucional, assim como quaisquer outros recursos que dão suporte à realização dos objetivos do Ministério da Ciência, Tecnologia e Inovações (Portaria MCTI n. 5.305/2021, art. 5º, inciso XXIV).

Dessa forma, a incorporação da gestão de riscos como um processo contínuo estabelecido para identificar, responder e monitorar eventos que possam afetar o alcance dos objetivos definidos pelo MCTI auxiliará os tomadores de decisão a realizarem escolhas mais assertivas, de forma a priorizar e distinguir as melhores alternativas de ações.

A aplicação desta metodologia deverá ocorrer em todas as unidades deste Ministério, ou seja: nos órgãos de assistência direta e imediata ao MCTI, nos órgãos específicos singulares, nas unidades de pesquisa e unidades descentralizadas/órgãos regionais. Considerando as singularidades e especificidades das unidades de pesquisa, estas poderão promover as adaptações necessárias nesta metodologia de modo a obter a máxima efetividade no processo de gestão de riscos em seus contextos, e, assim, cumprir com o disposto na Política de Gestão de Riscos deste Ministério (Portaria MCTI nº 5.305/2021).

2. NORMATIVOS, INSTÂNCIAS E ATORES

Os normativos da Administração Pública Federal que respaldam a implementação de iniciativas relativas a gestão de riscos nos órgãos se encontram abaixo relacionados:

- **Instrução Normativa Conjunta CGU/MP nº 1**, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;
- **Decreto nº 9.203, de 22 de novembro de 2017**, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional;
- **Portaria nº 1.089, de 25 de abril de 2018**, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências;
- **Portaria nº 57, de 4 de janeiro de 2019**, que altera a **Portaria CGU nº 1.089, de 25 de abril de 2018**, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências;

Já no âmbito do MCTI, os normativos que tratam do tema gestão de riscos são:

- **Portaria nº 4.301, de 12 de janeiro de 2021**, que institui o Comitê Interno de Governança do Ministério da Ciência, Tecnologia e Inovações e dá outras providências;
- **Portaria MCTI nº 5.205, de 28 de setembro de 2021**, que institui a Política de Governança Institucional do Ministério da Ciência, Tecnologia e Inovações;

- **Portaria MCTI nº 5.305, de 17 de novembro de 2021**, que institui a Política de Gestão de Riscos e cria o Comitê Técnico de Gestão de Riscos do Ministério da Ciência, Tecnologia e Inovações.
- **Portaria Secretaria-Executiva nº 1.395, de 13 de dezembro de 2021**, que designa os membros do Comitê Técnico de Gestão de Riscos do MCTI.

Conforme previsto no art. 10 da Portaria MCTI nº 5.305/2021, o dirigente máximo do MCTI é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão. Portanto, o Ministro de Estado é o principal ator no processo gerencial de gestão de risco neste Ministério. Para viabilizar esse processo ele conta com: (i) instâncias colegiadas que o assessoram para definição de diretrizes, monitoramento e avaliação (governança); e (ii) estrutura de gestão que atuam no planejamento, execução, controle, correção de rumos e prestação de contas.

Em relação às instâncias colegiadas, são duas que possuem competências atinentes à gestão de riscos:

- **Comitê Interno de Governança do Ministério da Ciência, Tecnologia e Inovação - CIG-MCTI**: que é uma instância colegiada consultiva e deliberativa da alta administração do Ministério destinada a atuar no assessoramento ao Ministro de Estado (art. 1º, Portaria MCTI nº 4.301/2021). Dentre as suas várias atribuições, destaca-se sua competência para aprovar políticas, diretrizes, metodologias e mecanismos de monitoramento e comunicação afetas a gestão de riscos no MCTI.
- **Comitê Técnico de Gestão de Riscos – CTGR**: que é uma instância colegiada interna de apoio à governança no tema gestão de riscos (art. 20, Portaria MCTI nº 5.305/2021). O seu papel no contexto da gestão de riscos no MCTI é:

- ✓ elaborar o plano de gestão de riscos e submetê-lo à aprovação do Comitê Interno de Governança – CIG-MCTI;
- ✓ promover a padronização e disseminação das ações institucionais relacionadas à gestão de riscos;
- ✓ monitorar a implementação da política de gestão de riscos neste Ministério;
- ✓ propor método de priorização dos objetos para a gestão de riscos;
- ✓ propor a adoção de boas práticas para o gerenciamento dos riscos;
- ✓ subsidiar CIG-MCTI com as informações necessárias à tomada de decisões relativas à gestão de riscos;
- ✓ zelar para que as informações adequadas sobre os riscos estejam disponíveis em todos os níveis da organização, tais como a matriz de impacto e probabilidade, para definição do nível de risco; a matriz de avaliação e resposta a riscos; a matriz de gerenciamento de riscos; e a matriz de tolerância ao risco;
- ✓ dar conhecimento ao CIG-MCTI dos riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público; e
- ✓ dirimir eventuais conflitos de atuação decorrentes do processo de gestão de riscos.

À estrutura de gestão do MCTI de níveis estratégico, tático e operacional, por sua vez, compete implementar a política de gestão de riscos no planejamento, na execução, no monitoramento, na avaliação e na comunicação dos objetos da gestão de riscos. E dentro deste contexto da gestão, cabe às unidades definir os gestores de risco de âmbito tático e operacional. Estes gestores de riscos possuem um papel essencial no processo de implementação da gestão de riscos, que é de:

- ✓ estabelecer as prioridades para aplicação da gestão de riscos nos objetos sob sua responsabilidade;
- ✓ orientar as ações de mapeamento, avaliação e mitigação do risco;
- ✓ implementar o processo de gestão de riscos no âmbito de suas respectivas unidades observando as fases de estabelecimento do contexto, identificação, análise, avaliação, tratamento de riscos, comunicação e consulta com as partes interessadas, monitoramento e melhoria contínua, conforme disposto no art. 18 desta portaria; e
- ✓ disponibilizar informações adequadas e tempestivas acerca da gestão dos riscos dos objetos da gestão de riscos sob sua responsabilidade a todos os níveis do Ministério, a fim de subsidiar a tomada de decisão e o aprimoramento da gestão e dos resultados deste órgão.

Por fim, para auxiliar os gestores de riscos nesse papel, cada servidor do MCTI é responsável pela operacionalização dos controles internos da gestão e por identificar e comunicar as deficiências às instâncias superiores, de modo que as correções sejam realizadas, o processo aperfeiçoado continuamente e os objetivos do MCTI alcançados.

3. BASES TEÓRICAS

Há diversos modelos e metodologias, mundialmente conhecidos, com foco no gerenciamento de riscos, tais como: Orange Book, do Tesouro Britânico (2001); manuais do *Committee of Sponsoring Organizations of the Treadway Commission* - COSO (2004 e 2017); e normas ISO 31000 (2009 e 2018). Essas duas últimas referências têm sido utilizadas com maior frequência no contexto da Administração Pública Federal.

O Manual de Gerenciamento de Riscos Corporativos – Estrutura Integrada (*Enterprise Risk Management — Integrated Framework*)¹, publicado pelo COSO em 2004, ofertou às organizações norteadores para a estruturação da gestão de riscos ao apresentar princípios, diretrizes e padrão de linguagem comum. Foi proposto também um modelo conceitual integrador das perspectivas de sistema e de processo para a gestão de riscos com o propósito de ampliar as probabilidades de concretização dos objetivos almejados pelas organizações. Em 2017, além de atualizar esse Manual de 2004, o COSO publicou o Manual de Gerenciamento de Riscos Corporativos - Integração com Estratégia e Desempenho (*Enterprise Risk Management - Integrating with Strategy and Performance*)², que buscou, em síntese, esclarecer a importância das organizações se aterem aos riscos no processo de elaboração da estratégia, em sua execução e na busca do desempenho almejado.

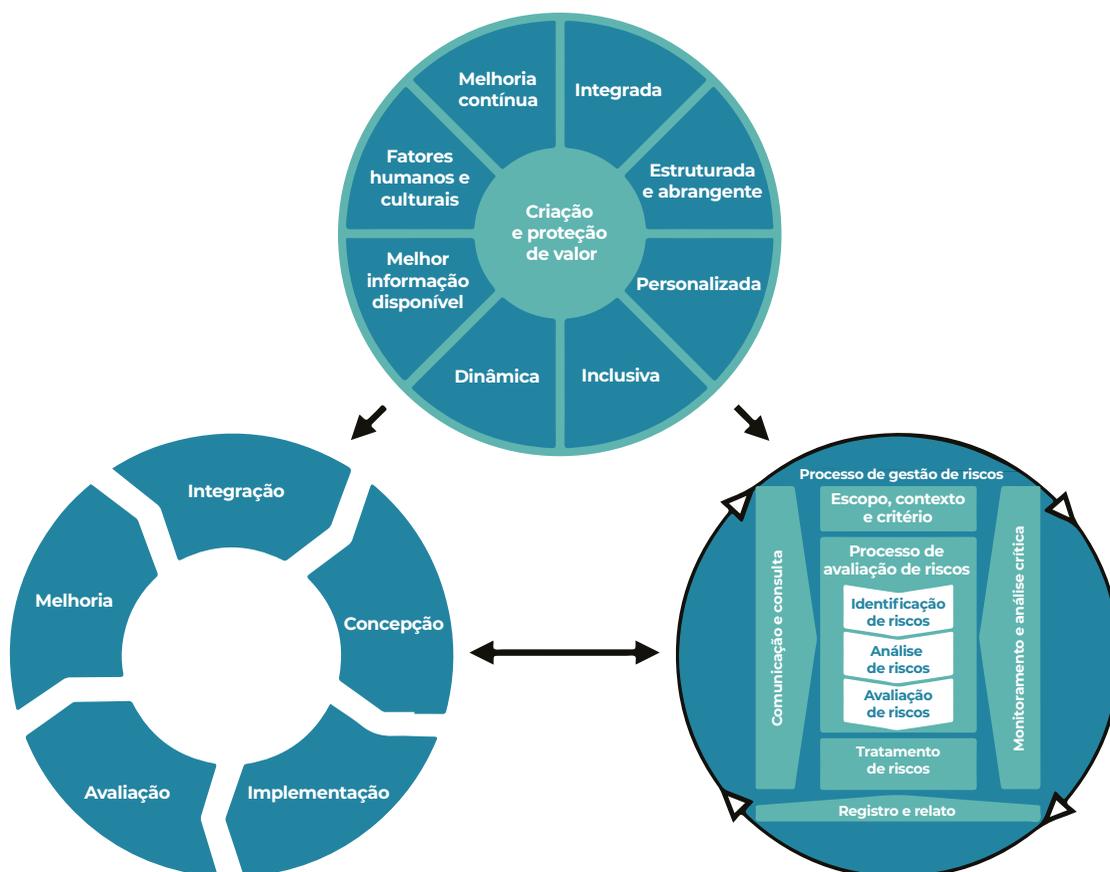
A Norma ABNT NBR 31000 apresenta princípios, diretrizes, conceitos e propõe estrutura e processos para gerenciamento integrado de riscos pelas organizações, objetivando a criação e proteção de valor. Para tanto, essa norma exhibe, em sua edição de 2018, proposta que integra princípios, sistema e o processo de gerenciamento de riscos (**Figura 1**). O sistema proposto articula integração, concepção, implementação, avaliação e melhoria do gerenciamento de riscos na organização. O processo, por sua vez,

1 Link de acesso ao Manual: <https://www.coso.org/documents/coso-erm-executive-summary-portuguese.pdf>

2 Link de acesso: https://repositorio.cgu.gov.br/bitstream/1/41825/8/Coso_portugues_versao_2017.pdf

envolve as etapas de: definição de escopo, contexto e critérios; processo de avaliação de riscos (identificação de riscos, análise de riscos, avaliação de riscos); tratamento de riscos; registro e relato; monitoramento e análise crítica; e comunicação e consulta.

Figura 1 - Princípios, estrutura e processo de gestão de riscos.



Fonte: ABNT NBR ISO 31000, 2018.

A publicação das edições dessas normas ISO pela ABNT, em 2009 e 2018, ofertou importante contribuição para nortear as organizações na temática gestão de riscos. O desafio que se impõe desde então é a adaptação desses modelos para a realidade da administração pública. Esforços nesse sentido vêm sendo, desde 2016, realizados por diversos órgãos¹, devendo serem ressaltadas as iniciativas pioneiras e que orientam os demais órgãos, as realizadas

¹ Cujas metodologias também foram consultadas e serviram de fonte de inspiração para a construção da metodologia do MCTI.

pelos Ministério do Planejamento, Desenvolvimento e Gestão (atual Ministério da Economia) e Controladoria-Geral da União (CGU), que coordenam sistemas estruturantes do Governo Federal responsáveis por orientarem os órgãos e entidades nessa temática.

Para elaboração desta metodologia do MCTI, foram selecionadas como referências os manuais do COSO e a norma NBR ISO 31000, considerando que esses referenciais vêm sendo amplamente utilizados no contexto da Administração Pública Federal e têm produzido bons resultados, como foi verificado nos *benchmarkings* realizados pelo MCTI junto a órgãos públicos, a partir do segundo semestre de 2020. Ademais, essas duas referências possuem compatibilidade entre si, possibilitando o uso em conjunto para produção de metodologia que melhor se adeque a realidade de cada organização.

4. POLÍTICA DE GESTÃO DE RISCOS DO MCTI

A Política de Gestão de Riscos do MCTI, aprovada por meio da Portaria MCTI nº 5.305, de 17 de novembro de 2021, apresenta os objetivos, princípios e diretrizes aplicadas à gestão de riscos neste Ministério.

Em relação aos **objetivos**, o art. 6º da referida política determina que a gestão de riscos aplicada no âmbito do MCTI tem por objetivo promover:

- a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais;
- o alinhamento do apetite ao risco com as estratégias adotadas;
- o estabelecimento de uma base confiável para tomada de decisões objetivando uma gestão resiliente aos riscos;
- a melhoria da capacidade deste Ministério para lidar com incertezas;
- o aprimoramento da governança institucional;

- a melhoria do potencial de alcance dos objetivos deste Ministério, reduzindo os riscos a níveis aceitáveis;
- o aumento da capacidade deste Ministério de se adaptar a mudanças;
- a implementação mais eficaz e segura do planejamento estratégico para o alcance de seus objetivos;
- a melhoria dos processos de tomada de decisão e do tratamento adequado dos aos riscos e dos impactos negativos decorrentes de sua materialização;
- o aprimoramento dos controles internos da gestão para mitigação dos efeitos danosos;
- o uso eficiente, eficaz e efetivo dos recursos públicos;
- o aprimoramento da conformidade legal e normativa dos processos organizacionais; e
- o aprimoramento da transparência organizacional e fortalecimento da reputação deste Ministério.

Conforme dispõe o art. 7º da Política de Gestão de Riscos do MCTI, além dos **princípios** específicos estabelecidos na política de governança da administração pública federal direta, autárquica e fundacional, deverão ser observados os seguintes:

- fomentar a inovação e a ação empreendedora responsáveis;
- ser dirigida, apoiada e monitorada pela alta administração;
- criar e proteger valor público;
- ser parte integrante dos processos organizacionais;
- ser parte da tomada de decisões;
- abordar explicitamente a incerteza;
- ser sistemática, estruturada e oportuna;
- ser baseada nas melhores informações disponíveis;
- estar alinhada ao contexto e ao perfil de risco deste Ministério;
- considerar fatores humanos e culturais;
- ser transparente e inclusiva;
- ser dinâmica, iterativa e capaz de reagir a mudanças;
- facilitar a melhoria contínua deste Ministério;

- aplicar-se de forma contínua e integrada aos objetos da gestão de riscos;
- considerar a identificação de riscos e oportunidades; e
- observar conceitos, parâmetros, referenciais técnicos e procedimentos comuns em todas as unidades a que se aplica.

Em seguida, o art. 8^a discorre sobre as **diretrizes** para a implementação da gestão de riscos neste Ministério, conforme abaixo:

- integrar-se ao planejamento estratégico, às políticas, aos projetos, às ações, aos processos e à cultura organizacional;
- estabelecer contexto que compreenda o ambiente externo e interno no qual o objeto da aplicação da gestão de riscos encontra-se inserido, que contribuam para a identificação e avaliação de vulnerabilidades que possam impactar no alcance de resultados e no cumprimento da missão institucional, assim como na imagem e na segurança da instituição e de pessoas;
- ser implantada por meio de ciclos de revisão e melhoria contínua, de acordo com metodologia de gestão de riscos definida pelo Ministério;
- ser formalizada por meio de metodologias, normas, manuais e procedimentos;
- responder aos riscos de forma adequada ao nível de apetite estabelecido para os objetos da gestão de riscos;
- promover a contínua capacitação do corpo funcional em gestão de riscos, por meio de soluções educacionais adequadas a cada nível organizacional;
- utilizar de procedimentos proporcionais aos riscos e em conformidade à prioridade dos objetos da gestão de riscos, baseada na relação custo-benefício e na agregação de valor à instituição; e
- prestar informações confiáveis, relevantes e tempestivas dos riscos levantados, mantendo o compartilhamento de informações entre as partes interessadas nos objetos da

gestão de riscos, observada a classificação da informação quanto ao sigilo.

Destaca-se que esta metodologia é uma importante ferramenta de apoio ao gerenciamento de riscos para unidades deste Ministério e está alinhada com as diretrizes dos órgãos centrais do Governo Federal que coordenam a temática.

5. PROCESSO DE GESTÃO DE RISCOS

As atividades de qualquer organização envolvem riscos em algum nível, portanto, o processo de gestão de riscos deve ser integrado a estratégia e operações. “Com uma boa gestão de riscos, a organização obterá aumentos graduais na sua capacidade de gerar, preservar e entregar valor público com desempenho otimizado, alcançando melhores resultados na implementação de políticas públicas e na prestação de serviços de interesse da sociedade” (TCU, 2018, p. 31).

Ao longo do processo de gerenciamento de riscos é necessário que a organização mantenha ativa comunicação e consulta entre as partes interessadas, monitorando e analisando criticamente o risco e os controles que o modificam, a fim de minimizar a necessidade de tratamentos de risco adicionais.

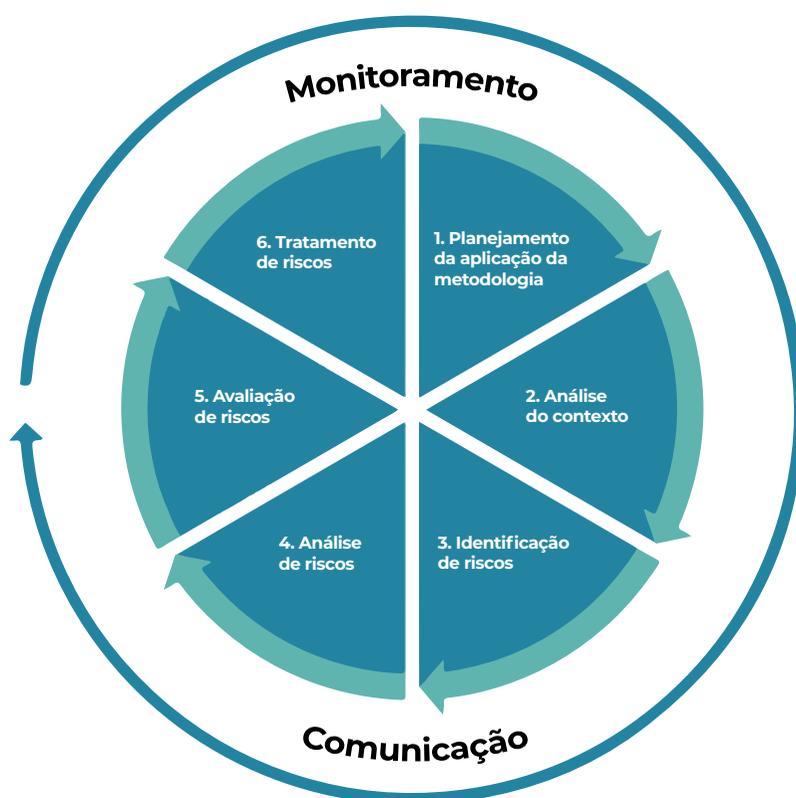
Dada a natureza multidisciplinar da gestão de riscos, a metodologia deverá ser aplicada, preferencialmente, de forma coletiva, em oficinas de trabalho, pelos responsáveis por cada objeto da gestão de riscos em conjunto com suas equipes.

Para que o processo de gestão de riscos em qualquer objeto seja bem-sucedido, no âmbito do MCTI, seguindo as melhores práticas disponíveis no setor público e nas Normas ISO/ABNT, foi elaborada esta metodologia que é composta pelas seguintes etapas (**figura 2**):

- 1) Planejamento da aplicação da metodologia;
- 2) Análise do contexto;
- 3) Identificação de riscos;
- 4) Análise de riscos;
- 5) Avaliação de riscos; e
- 6) Tratamento de riscos.

Além das seis etapas já mencionadas, para que o processo de gestão de riscos seja exitoso, faz-se necessário o estabelecimento pelas unidades de 02 (dois) processos de trabalho específicos: **monitoramento** e **comunicação**, ambos explicitados na **figura 2** e detalhados nesta metodologia.

Figura 2 - Ciclo da Metodologia de Gestão de Riscos do MCTI



Fonte: adaptado da CGU, 2021.

Assim, conforme se visualiza na **figura 2**, o processo de gestão de riscos deve ocorrer em ciclos sucessivos, de modo a promover a melhoria contínua dos processos decisórios e da gestão institucional. Estes ciclos, conforme prevê a Política de Gestão de Riscos do MCTI (Portaria MCTI nº 5.305/2021), terão sua periodicidade definida pelos respectivos gestores do risco e deverá observar as características de cada objeto da gestão de riscos.

Nos tópicos seguintes são detalhadas cada uma destas etapas de modo a possibilitar a compreensão e aplicação desta metodologia pelos gestores e suas equipes do MCTI.

5.1. PLANEJAMENTO DA APLICAÇÃO DA METODOLOGIA

Todos nós fazemos gestão de riscos o tempo todo, mas na maioria das vezes essas ações não são sistematizadas e formalizadas. Esta metodologia surge justamente como uma ferramenta de gestão para que as unidades do MCTI estabeleçam rotinas de gerenciamento de riscos de modo a potencializar o alcance dos objetivos dos processos, projetos, ações, etc.

Porém, antes de iniciar a aplicação desta metodologia e realizar um trabalho sistematizado, considerando que os recursos são escassos e, geralmente, é preciso fazer escolhas e conferir foco aos objetos da gestão de riscos mais relevantes para o MCTI, faz-se necessário, primeiramente, **planejar** a aplicação desta metodologia, que inclui realizar a priorização dos objetos da gestão cujos riscos serão avaliados.

Este momento prévio de planejamento é essencial para o bom andamento das próximas etapas do processo de gestão de riscos. Nesta fase os seguintes pontos devem ser observados:

- Priorizar os objetos da gestão de riscos que serão avaliados – escopo do trabalho;
- Definir os atores envolvidos, o responsável pelo objeto da gestão de riscos e a equipe que irá realizar as atividades de aplicação da metodologia;

- Definir todas as atividades que serão realizadas no projeto de aplicação da metodologia;
- Definir reuniões de progresso do projeto, de modo a manter informados os gestores e dar ciência a autoridade máxima da unidade (o secretário, em se tratando de uma secretaria, por exemplo) sobre todos os resultados alcançados ao longo de cada etapa da metodologia;
- Definir o cronograma detalhado;
- Formalizar o projeto de aplicação da metodologia nos objetos prioritizados;
- Definir as entregas prioritárias do projeto que deverão ser consubstanciadas em relatório ao final da iniciativa.

5.2. ANÁLISE DO CONTEXTO

Nesta etapa deve-se explicitar as informações acerca do objeto da gestão de riscos (processo, projeto, ações, atividades, etc.) que está sob análise de modo a compreender o ambiente externo e interno no qual esse objeto está inserido.

As informações produzidas nesta etapa também são de suma importância para subsidiar as etapas subsequentes de aplicação desta metodologia.

Para a compreensão completa do contexto do objeto da gestão de riscos é necessária análise e produção, no mínimo, das seguintes informações:

- Em relação ao **contexto externo**: informações sobre o cenário político, social, legal, econômico e financeiro, tecnológico, ambiental referentes ao contexto nacional, regional ou local e, no que couber, internacional. Além disso, devem ser observados fatores-chave e tendências que tenham impacto sobre os objetivos da organização e as relações com as partes interessadas externas e suas percepções e valores.

- Em relação ao **contexto interno** do MCTI: informações sobre características do objeto da gestão de riscos relativos à legislação correlacionada, objetivo, etapas, atividades, contribuição para a Política de Ciência, Tecnologia e Inovações e para os objetivos estratégicos e prioridades do órgão, usuários (internos e externos) dos produtos ou serviços produzidos, unidades organizacionais envolvidas, equipes alocadas, estrutura de governança, infraestrutura física e tecnológica, principais fatos críticos históricos do objeto em análise, aspectos culturais.

ORIENTAÇÕES BÁSICAS:

A análise do contexto do objeto da gestão de riscos facilita a identificação, análise e a avaliação dos riscos. Para descrever o resultado da análise do contexto, deve-se utilizar o **Formulário de Análise de Contexto de Objeto de Gestão de Riscos**, disponível no ANEXO I desta metodologia.

Para melhor entendimento e explicitação do contexto externo e interno, nos quais os objetos de gestão de riscos em análise estejam inseridos, sugere-se a utilização da Matriz SWOT (ou FOFA) (**Figura 3**) como ferramenta para identificação dos pontos fortes e fracos (ambiente interno) e as oportunidades e ameaças (ambiente externo).

Figura 3 - Análise de SWOT



Fonte: adaptado da Enap, 2018.

5.3. IDENTIFICAÇÃO DOS RISCOS

Etapa que compreende o reconhecimento e a descrição dos riscos relacionados a um objeto de gestão, envolvendo a identificação de possíveis fontes de riscos. Nesta etapa é possível identificar e registrar tanto os eventos de riscos que comprometem o alcance dos objetivos dos processos, dos projetos, atividades, etc., assim como as causas e efeitos ou consequências de cada um deles. Para auxiliar nessa tarefa, utilize a **Tabela Modelo de Suporte à identificação de riscos**, no ANEXO II desta Metodologia.

É importante destacar que eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer.

Os eventos podem ter efeitos positivos (oportunidades de ganho) ou negativos (possibilidades de perdas). No entanto, na aplicação desta metodologia, serão analisados apenas os riscos com potenciais efeitos negativos.

Os eventos de riscos devem ser entendidos como parte de um contexto e não devem ser analisados de forma isolada. É essencial que os eventos de riscos sejam identificados adequadamente para que seja possível determinar o tipo de resposta ao risco e o planejar a melhor forma de tratamento.

A **figura 4**, abaixo, apresenta de maneira esquemática os componentes de um evento de risco e orienta o exercício de identificação das causas dos riscos e suas consequências.

Figura 4 - Componentes do Evento de Risco



Fonte: adaptado do Manual do MPOG, 2017.

Conceitos importantes:

Causas: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fontes de riscos e podem ter origem no ambiente interno e externo.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Consequência: o resultado de um evento de risco sobre os objetivos.

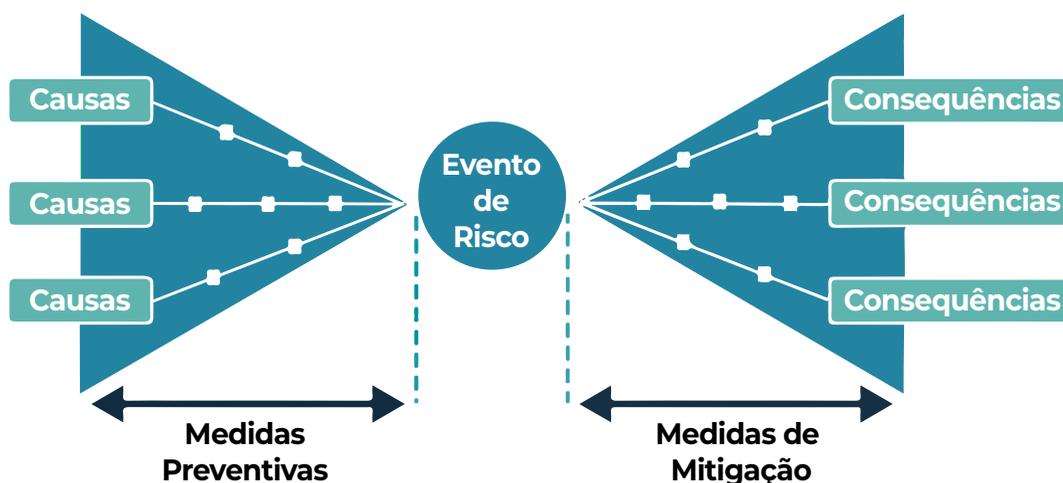
A sintaxe, abaixo, auxilia na descrição de aspectos envolvendo um evento de risco promovendo uma melhor reflexão e um desenvolvimento mais apurado para esta etapa.

Devido a (CAUSA, FONTE), poderá acontecer (EVENTO DE RISCO), o que poderá levar a (EFEITOS, CONSEQUÊNCIAS), impactando no (OBJETIVO).

Exemplo: Devido à falta de manutenção da rede elétrica poderá acontecer um incêndio, o que poderá levar a destruição total ou parcial do imóvel, impactando na interrupção de pesquisas em andamento.

A **figura 5**, abaixo, é recomendada para auxiliar no levantamento dos eventos de riscos, suas causas e consequências. Outras ferramentas, como *Brainstorming* e entrevistas com especialistas no objeto da gestão de riscos, também poderão ser utilizadas nesta etapa.

Figura 5 - Bow Tie



Fonte: adaptado da ISO 31010, 2012.

Após a aplicação de técnicas que facilitam na identificação dos eventos de risco, estes devem ser caracterizados conforme a seguir:

- 1) **Objeto da Gestão de Risco:** informe o objeto ao qual o risco está associado.
- 2) **Evento de Risco:** descreva o evento de risco identificado.
- 3) **Causas:** descreva as possíveis causas do evento de risco identificado, que podem ter origem no ambiente interno e/ou externo.
- 4) **Efeitos ou Consequências:** descreva os possíveis efeitos ou consequências de um possível evento de risco sobre os objetivos do objeto de gestão de riscos que está sob análise.
- 5) **Fonte/Fator de Riscos:** no momento de identificação das causas dos eventos de risco é importante analisar também as possíveis fontes/fatores que dão origem a esses eventos, que são: pessoas, processos, sistemas, tecnologias, infraestrutura e fatores externos. As causas dos riscos são decorrentes da adição das fontes/fatores e as fragilidades. Na **tabela 1**, abaixo, são explicitados exemplos de fragilidades associadas a cada uma destas fontes/fatores.

Tabela 1 - Fontes de Riscos e Fragilidades

FONTE / FATOR DE RISCO	FRAGILIDADES
1. Pessoas:	Capacitação insuficiente, desmotivação; estresse; negligência; corrupção, etc.
2. Processos:	Ineficiente, mal estruturado, redundante, imaturo, etc.
3. Sistemas:	Obsoleto, incompatível, sem documentação, baixa segurança, etc.
4. Tecnologias:	Ultrapassada, alto custo, baixa acessibilidade, alta complexidade, etc.
5. Infraestruturas:	Inadequada, inacessível, ineficiente, precária, etc.
6. Evento Externo:	Desastre natural, crise econômica, influência política, etc.
Causa = Fonte/Fator + Fragilidades	

Fonte: adaptado da CGU, 2021.

6) **Tipologia dos Riscos:** no MCTI os riscos serão categorizados segundo as seguintes tipologias:

- **Estratégico:** envolve eventos de potencial impacto na missão, metas ou objetivos estratégicos da unidade/órgão;
- **Operacional:** envolve eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e à eficiência dos processos organizacionais;
- **Orçamentário e Financeiro:** envolve eventos que podem comprometer a capacidade da unidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam afetar a própria execução orçamentária;
- **Fiscal:** eventos que podem afetar negativamente o equilíbrio das contas públicas;
- **Imagem:** envolve eventos que podem comprometer a confiança da sociedade em relação à capacidade da unidade em cumprir sua missão institucional com integridade e interferem nos conceitos que se tem associados ao órgão;
- **Integridade:** envolve eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possam comprometer os valores preconizados pelo Ministério e a realização de seus objetivos;
- **Legal/Regulatório:** envolve eventos que podem afetar a não conformidade com a legislação e as normas obrigatórias aplicáveis ao Ministério e suas atividades;
- **Social:** envolve eventos que podem comprometer o valor público esperado ou percebido pela sociedade em relação ao resultado da prestação de serviços públicos da instituição.

Deve estar claro que um evento de risco poderá ser categorizado em uma ou mais tipologia de risco. Sendo que o Comitê Técnico de Gestão de Riscos - CTGR (Port. nº 5.305/2021) poderá rever as categorizações realizadas de determinados eventos de risco, caso compreenda ser necessário para subsidiar a adequada tomada de decisão e comunicação gerencial.

Ademais, os tipos de riscos elencados nesta metodologia não devem ser vistos como um rol exaustivo. Pois, no decorrer do processo de avaliação dos riscos, uma nova tipologia de risco poderá ser identificada e esta deve ser registrada e descrita de modo a ser incorporada em novas edições desta metodologia.

5.4. ANÁLISE DOS RISCOS

5.4.1. Identificação do risco inerente

Risco inerente é o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto (Art. 2º, XIV, IN Conjunta MP/CGU Nº 01/2016).

Para identificar o risco inerente é necessário analisar o nível do risco, levando em consideração a probabilidade de sua ocorrência e do impacto destes eventos de riscos nos objetivos do objeto de gestão de riscos que está sendo analisado, sem considerar, ainda, os controles internos da gestão existentes no momento da aplicação desta metodologia.

Mas o que são “probabilidade” e “impacto” no contexto da gestão de riscos?

1) **Probabilidade** de ocorrência do risco: chance de o evento de risco ocorrer dentro do prazo previsto para alcançar o objetivo.

Por exemplo: um evento cuja ocorrência seja quase certa de acontecer é um evento de alta probabilidade.

No contexto desta metodologia, para avaliar a Probabilidade, a seguinte escala será utilizada:

Tabela 2 - Escala de Avaliação de Probabilidade

ESCALA DE PROBABILIDADE		
Probabilidade	Descrição da probabilidade	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito alta	Praticamente certa. De forma esperada, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	5

Fonte: adaptado da Metodologia de Gestão de Riscos da CGU, 2021.

2) **Impacto** do risco sobre o objetivo: efeito resultante da ocorrência do evento.

Por exemplo: um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco muito alto ou catastrófico.

Para a avaliação do **Impacto**, nesta metodologia, será utilizada a escala a seguir:

Tabela 3 - Escala de Avaliação de Impacto

ESCALA DE IMPACTO		
Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos do processo.	1
Baixo	Pequeno impacto nos objetivos do processo.	2
Médio	Moderado impacto nos objetivos do processo, porém recuperável.	3
Alto	Significativo impacto nos objetivos do processo, de difícil reversão.	4
Muito alto	Catastrófico impacto nos objetivos do processo, de forma irreversível.	5

Fonte: adaptado da Metodologia de Gestão de Riscos da CGU, 2021.

Após identificar a **Probabilidade** e o **Impacto** dos eventos de riscos, realiza-se a multiplicação dos pesos obtidos para se identificar o nível do risco. O produto desta multiplicação irá apontar a classificação do risco nas faixas a seguir na **tabela 4**:

Tabela 4 - Classificação de Riscos

CLASSIFICAÇÃO DE RISCOS	
Classificação	FAIXA
Risco Baixo	0 – 4,99
Risco Médio	5 – 11,99
Risco Alto	12 – 19,99
Risco Extremo	20 - 25

Fonte: adaptado da Metodologia de Gestão de Riscos da CGU, 2021.

Na **Matriz de Risco**, a seguir (**figura 5**), são apresentados os resultados possíveis obtidos a partir da combinação das escalas de **Probabilidade x Impacto**.

Figura 6 - Matriz de Riscos

MATRIZ DE RISCO
(probabilidade x impacto)

IMPACTO	Muito Alto 5	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito Baixo 1	1	2	3	4	5
		1	2	3	4	5
		Muito baixa	Baixa	Média	Alta	Muito alta
		PROBABILIDADE				

Fonte: adaptado da Metodologia de Gestão de Riscos da CGU, 2021.

Atenção! Para definir os níveis de probabilidade e de impacto, nesta metodologia usaremos a escala que vai de 1 (um) a 5 (cinco), sendo 1 a menor classificação e 5 a mais elevada, conforme representado na **Matriz de Risco**. Quanto ao nível de criticidade do risco, são quatro as classificações possíveis: **Risco Baixo**, **Risco Médio**, **Risco Alto**, **Risco Extremo**. O nível do risco é dado pelo número inscrito em cada célula da matriz. São 25 possíveis combinações, em que cada nível está associado a uma estimativa de probabilidade e de impacto.

5.4.2. Identificação dos controles internos da gestão existentes

Os **controles internos da gestão** são um conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, dentre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores, destinados a enfrentar os riscos e fornecer segurança razoável para que este Ministério, na consecução de sua missão, realize execução ordenada, ética, econômica, eficiente e eficaz das operações, cumpra com as obrigações de *accountability*, as leis e os regulamentos, e salvasgarde os recursos para evitar perdas, mau uso e danos, conforme a Instrução Normativa Conjunta nº 1, de 2016.

É importante destacar a distinção entre os controles internos da gestão e os controles internos das atividades do Sistema de Controle Interno previsto no art. 74 da Constituição ou com as atribuições da auditoria interna. A Instrução Normativa Conjunta nº 1, de 2016, esclarece essa diferença em seu art. 7º, conforme abaixo:

Art. 7º Os controles internos da gestão tratados neste capítulo não devem ser confundidos com as atividades do Sistema de Controle Interno relacionadas no artigo 74 da Constituição Federal de 1988, nem com as atribuições da auditoria interna, cuja finalidade específica é a medição e avaliação da eficácia e eficiência dos controles internos da gestão da organização.

Os controles podem ser classificados quanto ao **tipo, natureza, frequência e relação com o risco**, conforme abaixo:

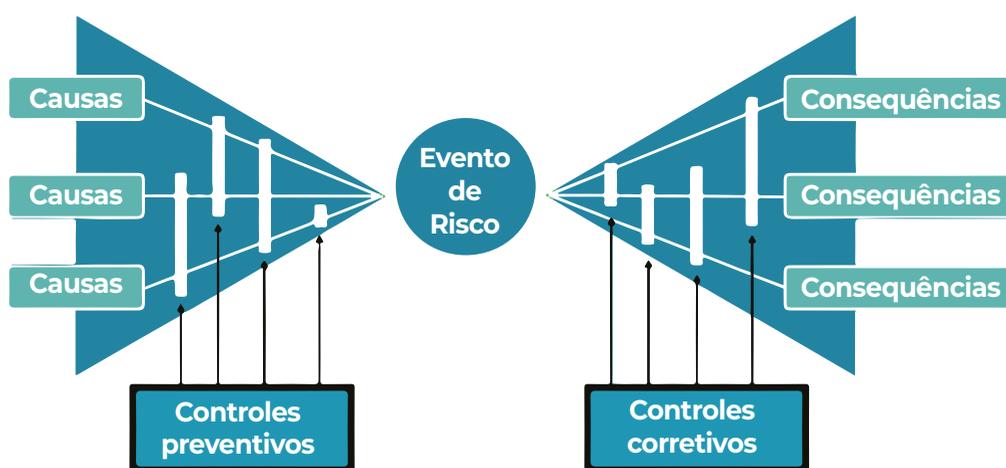
a) Tipo de controle: preventivos ou corretivos:

Preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplo: *backup*, definição de requisitos, capacitação dos servidores, procedimentos de autorização de acesso, realização de *checklist* definidos para processos, projetos, etc.

Corretivos: tem como objetivo mitigar falha que já ocorreu, apurada após o processamento inicial ter ocorrido. Atua sobre a consequência do evento. Exemplo: acionamento de plano de contingência, revisão normativa, troca de equipamento defeituoso, instalação de extintores de incêndio, detecção de pessoas que acessaram as dependências do órgão sem identificação prévia, instalação de gerador de energia, etc.

Na **figura 6**, a seguir, é representado o posicionamento dos controles internos da gestão de acordo com seu tipo, se preventivo ou corretivo.

Figura 7 - Controles internos da gestão no *Bow Tie*



Fonte: adaptado da ISO 31010, 2012.

b) Natureza do controle: manual, automático ou híbrido:

Manual: controles que são realizados por pessoas. Exemplo: conferência de assinatura.

Automático: controles processados por um sistema, com mínima intervenção humana na sua realização. Exemplo: detector de incêndio.

Híbridos: controles que mesclam atividades manuais e automáticas.

c) Frequência do controle: anual, semestral, mensal, semanal, diário ou várias vezes ao dia.

d) Relação com o Risco: controles diretos ou indiretos.

Controles diretos: têm como objetivo mitigar o risco. Estão mais relacionados aos controles operacionais. Exemplo: conferência dos pagamentos a serem efetuados.

Controles indiretos: têm como objetivo a prevenção e a detecção de eventos de risco, auxiliando na mitigação do risco. Estão mais relacionados ao ambiente de controle. Exemplo: grade de treinamentos obrigatórios para os funcionários.

É necessário avaliar o nível de efetividade dos controles existentes para determinar o nível do risco residual. Desta forma, os níveis dos controles deverão ser classificados em **Inexistente, Fraco, Mediano, Satisfatório e Forte**, conforme as orientações da **tabela 5** abaixo:

Tabela 5 - Avaliação da efetividade dos controles existentes

AVALIAÇÃO DA EFETIVIDADE DOS CONTROLES EXISTENTES		
Nível	Descrição	Fator de Avaliação
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles têm abordagens <i>ad hoc</i> , tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

Fonte: adaptado da CGU, 2018.

No decorrer da análise de riscos de determinado objeto, é possível obter um resultado do risco inerente com níveis críticos e em função da efetividade dos controles existentes o nível deste risco ser reduzido. Isso ocorre quando os controles existentes são fortes e extremamente importantes impedindo que o evento de risco se materialize. No entanto, o monitoramento desses controles deve ser realizado com maior frequência e efetividade.

5.4.3. Identificação do risco residual

Risco residual é o risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco

(Art. 2º, XV, IN Conjunta MP/CGU N° 01/2016). É desejável que o nível do risco residual seja inferior ao nível do risco inerente, considerando que a diferença do nível do risco inerente e do risco residual explicita o quão eficaz são os controles internos implementados para mitigar os riscos identificados.

Para calcular o nível do risco residual é necessário multiplicar o valor do **Risco Inerente** pelo valor do **Fator de Avaliação**, conforme previsto na **tabela 5**. Por exemplo, quando a efetividade do controle é classificada como inexistente o resultado do nível do risco inerente será multiplicado por 1 (um), isto é, o nível do risco residual será igual ao nível do risco inerente. Por outro lado, caso o controle seja classificado como forte, então multiplica-se o nível do risco inerente por 0,2 (zero vírgula dois), ou seja, o nível do risco residual será reduzido em 80% (oitenta por cento) do risco inerente identificado.

5.5. AVALIAÇÃO DOS RISCOS

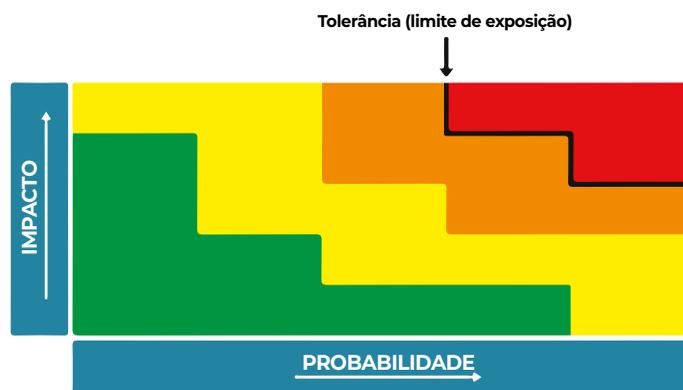
Após analisar a probabilidade da ocorrência do risco e o nível do seu impacto, é necessário avaliar os eventos de riscos identificados considerando os seus componentes (causas e consequências). A partir da avaliação dos riscos é possível ter uma visão geral dos níveis de risco de cada um dos eventos de risco identificados e, desse modo, priorizá-los. Esta priorização compete ao gestor do risco, que irá definir quais dos eventos de risco devem ser tratados prioritariamente, considerando a classificação dos riscos.

O limite de exposição ao risco, embora possa ser fixado entre outras faixas conforme a tolerância ao risco, ficou padronizado no limite entre os riscos classificados como altos e extremos, vide (**figura 7**). Para os eventos que se situem em um nível de risco residual acima do limite estabelecido, ficará exigida a definição de medidas de tratamento de modo a adequar o risco a níveis tolerados.

Diante da impossibilidade de o risco ficar abaixo do limite de exposição definido pelo órgão; e caso o gestor do risco opte por aceitar

o risco, é necessária a anuência e justificativa do dirigente máximo da unidade, que deverá dar ciência ao Comitê Técnico de Gestão de Riscos - CTGR (Portaria MCTI nº 5.305/2021), para que este possa analisar e, se necessário, reportar ao Comitê Interno de Governança - CIG-MCTI (Portaria MCTI nº 4.301/2021).

Figura 8 - Matriz Simples de Risco e Tolerância ao Risco



Fonte: adaptado do TCU, 2020.

Na **tabela 6** são apresentadas as faixas de limite de exposição ao risco de acordo com a classificação.

Tabela 6 - Limite de Exposição ao Risco

LIMITE DE EXPOSIÇÃO AO RISCO		
Classificação	Faixa	Descrição
Risco Baixo (RB)	0 - 4,99	Riscos abaixo do limite de exposição.
Risco Médio (RM)	5 - 11,99	
Risco Alto (RA)	12 - 19,99	
Risco Extremo (RE)	20 - 25	Riscos acima do limite de exposição.

Fonte: adaptado do TCU, 2020.

No **quadro 1** a seguir são apresentados passos que devem ser seguidos para realizar a avaliação dos riscos, considerando o conjunto de informações já apresentadas nesta metodologia.

Quadro 1 - Passos para a Avaliação de Riscos

Para a avaliação dos riscos, os seguintes passos devem ser seguidos:

1. Identificar na matriz a probabilidade x impacto e os riscos cujos níveis estão acima do limite de exposição a risco (faixa vermelha da matriz);
2. Identificar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a organização como um todo;
3. Identificar os riscos que estão abaixo do limite de exposição: (i) para os riscos cujos níveis se encontram nas faixas amarela e laranja, deverá ser avaliada a possibilidade de tratamento mais adequada; e (ii) os riscos cujos níveis se encontram na faixa verde, poderão ser aceitos.

Fonte: adaptado do TCU (2020).

É importante ponderar que a avaliação dos riscos provê subsídios para a tomada de decisão, mas não se constitui como fator exclusivo para eventual tratamento do risco, podendo o gestor do risco adicionalmente lançar mão de outros insumos para definir as estratégias de tratamento do risco.

5.6. TRATAMENTOS DOS RISCOS

Tratamento dos riscos consiste no planejamento e na execução de ações para modificar o nível do risco. Esta modificação ocorre por meio de medidas de resposta ao risco que mitiguem, transfiram ou compartilhem, ou evitem o risco.

Conforme a ISO 31000:2018 (p. 14), escolher as opções mais adequadas de tratamento de riscos “envolve balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação”. Portanto, isso requer análise criteriosa do gestor de risco para tomar a decisão que representa o melhor custo/benefício para o órgão.

As possibilidades de tratamento de riscos podem ser categorizadas em **aceitar, mitigar/reduzir, transferir/compartilhar e evitar**, conforme pode ser verificado na **tabela 7** a seguir.

Tabela 7 - Possibilidades de tratamento dos riscos

POSSIBILIDADES DE TRATAMENTO DOS RISCOS		
OPÇÃO DE TRATAMENTO	DESCRIÇÃO	ORIENTAÇÃO
ACEITAR	Não necessariamente se deve adotar quaisquer medidas, mas precisa avaliar se é o caso de monitorar ao longo do tempo.	Um risco normalmente é aceito quando seu nível está classificado como “Baixo”. Nessa situação, poderá ser dispensada a implementação de novo controle para mitigar o risco.
MITIGAR / REDUZIR	Desenvolver e implementar medidas para evitar que o risco se concretize ou medidas para atenuar o impacto/consequência caso ocorra.	Um risco normalmente é mitigado quando é classificado como “Médio”, “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta um custo-benefício adequado. No MCTI, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
TRANSFERIR/ COMPARTILHAR	Compartilhar o risco do objeto com terceiros, por meio, por exemplo, de realização de seguro.	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, a implementação de controles não apresenta custo-benefício adequado, e o compartilhamento/transferência é vantajoso para a Administração. No MCTI, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
EVITAR	Descontinuar a atividade do projeto, do processo, da ação ou do objeto ao qual o risco está associado.	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com o MCTI. Quando os riscos “Altos” ou “Extremos” estiverem associados a objetos estratégicos, a adoção dessa opção deverá ser previamente submetida à aprovação do secretário da unidade e informado ao Comitê Interno de Governança – CIG-MCTI.

Fonte: adaptado do TCU (2020) e CGU (2021).

Pela faixa de classificação do risco (Risco Baixo, Risco Médio, Risco Alto e Risco Extremo), conforme **tabela 8** abaixo, é possível que o gestor do risco defina a ação mais coerente de priorização para tratamento.

Tabela 8 - Ação recomendada perante o risco para cada classificação

AÇÃO RECOMENDADA PERANTE O RISCO PARA CADA CLASSIFICAÇÃO	
CLASSIFICAÇÃO	AÇÃO
Risco Baixo	<p>O nível de risco encontra-se abaixo do nível de tolerância, portanto, poderá ser aceito. Mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos. No entanto, esta opção precisa ser precedida de avaliação da relação custo-benefício, como diminuir o nível de controles, por exemplo.</p> <p>Caso o risco seja priorizado para implementação de medidas de tratamento e acarrete custos adicionais ao órgão, esta priorização deve ser justificada pela unidade e aprovada pelo secretário da unidade.</p>
Risco Médio	<p>O nível de risco encontra-se abaixo do nível de tolerância. Requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.</p> <p>Caso o risco seja priorizado para implementação de medidas de tratamento e acarrete custos adicionais ao órgão, esta priorização deve ser justificada pela unidade e aprovada pelo secretário da unidade.</p>
Risco Alto	<p>O nível de risco encontra-se abaixo do nível de tolerância. No entanto, os riscos neste nível devem ser comunicados ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do secretário da unidade.</p> <p>Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada e aprovada pelo secretário da unidade.</p>
Risco Extremo	<p>O nível de risco encontra-se acima do nível de tolerância. Qualquer risco nesse nível deve ser comunicado pelo secretário da unidade ao Comitê Interno de Governança – CIG-MCTI juntamente com proposta de resposta ao risco imediata. Postergação de medidas só com autorização do Comitê Interno de Governança – CIG-MCTI.</p> <p>Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo secretário da unidade e aprovada pelo Comitê Interno de Governança – CIG-MCTI</p>

Fonte: adaptado da CGU (2021).

Para realizar o tratamento dos riscos as medidas mitigadoras podem envolver, por exemplo, a adoção de controles, o redesenho de processos, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, dentre outras medidas.

Para o tratamento dos riscos os seguintes passos devem ser seguidos:

- 1) Revisitar as causas e consequências dos riscos priorizados;
- 2) Registrar as possíveis medidas de resposta ao risco;
- 3) Avaliar a viabilidade da implantação dessas medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.);
- 4) Decidir quais medidas serão implementadas;
- 5) Elaborar plano de implementação das medidas. No **Anexo III** é apresentado um **Modelo de Plano de Tratamento de Riscos a ser utilizado** para sistematizar as informações acerca das medidas de tratamento priorizadas; e
- 6) Validar do Plano de Tratamento de Riscos. Passo que será detalhado no item 5.6.1 desta metodologia.

DICAS PARA FACILITAR A DEFINIÇÃO DAS MEDIDAS DE TRATAMENTO DOS RISCOS!

Refleta sobre as seguintes perguntas-chave:

- ✓ Que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
- ✓ Que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado?
- ✓ É possível adotar medidas para compartilhar ou transferir o risco?

Considere os seguintes aspectos:

- ✓ Fontes e causas dos riscos – em princípio, as medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência, ou também podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize, ou uma combinação das duas abordagens;
- ✓ Na decisão quanto à implantação das medidas de resposta ao risco, considerar a quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível do risco gerado pela medida;
- ✓ Priorizar as medidas de tratamento de riscos que possam mitigar mais causas ou consequências ao mesmo tempo e de eventos de riscos com maior impacto.

Por fim, para a elaboração do **Plano de Tratamento de Riscos** é importante observar aspectos como:

- Instituir controles automatizados em substituição aos controles manuais, quando possível;
- Definir indicadores de desempenho adequados;
- Segregar funções e atribuição de obrigações entre pessoas com a finalidade de reduzir risco, erro ou fraude;
- Estabelecer limites para transações;

- Estabelecer procedimentos e rotinas de conferência e verificação;
- Instituir políticas e procedimentos adequados aos objetos de gestão de riscos.

5.6.1. Validação dos resultados e do Plano de Tratamento dos Riscos

Como previsto na etapa de planejamento da aplicação da metodologia, os gestores (responsáveis pelo objeto da gestão cujo riscos estejam em avaliação) e dirigente máximo da unidade (o secretário, em se tratando de uma secretaria, por exemplo) devem estar cientes e acompanhar os resultados de cada etapa do processo de gerenciamento de riscos. Assim, quando lhes for apresentado o Plano de Tratamento de Riscos para validação, tudo transcorrerá de modo célere.

Após a validação pelo dirigente máximo da unidade, as ações do Plano de Tratamento de Riscos deverão ser incluídas nos planejamentos institucionais de modo a fazer parte das prioridades das unidades responsáveis.

Caso haja necessidade de envolver outras áreas na viabilização das ações de tratamento de riscos, é essencial que as negociações sejam efetuadas antes da validação pelo dirigente máximo da unidade. Isso evitará surpresas ou dificuldades futuras na execução das ações. Sendo assim, o gestor do risco, juntamente com a equipe que estará envolvida na aplicação da metodologia, terá a responsabilidade de promover esse alinhamento, antes da submissão do Plano de Tratamento de Riscos ao dirigente máximo para validação.

6. MONITORAMENTO

O monitoramento é um processo de trabalho de natureza continuada que consiste no acompanhamento e na verificação sistemática dos elementos da gestão de riscos, abrangendo a coleta, análise e geração de informações para tomada de decisão.

Assim, monitorar constantemente os eventos de riscos identificados contribui substancialmente para neutralizar ameaças aos objetivos institucionais e possibilita aproveitar as oportunidades. Ademais, o órgão se resguarda de forma mais adequada e tempestiva aos múltiplos eventos indesejáveis que oferecem riscos e podem afetar o alcance dos objetivos das diferentes unidades que compõem o Ministério. Sua execução regular leva à melhoria da capacidade de identificação de possíveis fragilidades sistemáticas diante das possíveis ameaças, tornando a gestão de riscos mais eficaz, reduzindo surpresas e suas implicações, mitigando custos de enfrentamentos e prejuízos associados ao desempenho institucional acometido por materialização de riscos.

No MCTI o monitoramento será acerca:

- (i) da implementação da política de gestão de riscos;
- (ii) da implementação do processo de gerenciamento de riscos pelas unidades;
- (iii) da implementação dos planos de tratamento de riscos pelas unidades; e
- (iv) dos níveis de riscos.

Assim, o monitoramento abrange e requer a participação de todos os atores envolvidos com a temática gestão de riscos no Ministério: Comitê Interno de Governança – CIG-MCTI; Comitê Técnico de Gestão de Riscos no MCTI; Gestores de nível estratégico (dirigente máximo do órgão e seus secretários); Gestores de nível tático (diretores e coordenadores-gerais); Gestores de nível operacional, responsáveis

direto pelos objetos da gestão de riscos (processos, projetos, atividades, etc.); e Departamento de Governança Institucional – DGI/SEEXEC, que prestará apoio e orientação técnica especializada às unidades do órgão visando a implantação do processo de gestão de riscos em seus âmbitos.

Cada um desses atores tem papel específico dentro do processo de monitoramento, conforme disposto na Política de Gestão de Riscos do MCTI (Portaria MCTI nº 5.305/2021), e o desempenho deste papel é essencial para o funcionamento exitoso do processo de monitoramento. Destaca-se as competências dos gestores de risco de âmbito tático e operacional previstas no art. 15, incisos III e IV, considerando que esses atores serão os provedores das informações acerca dos riscos que gerenciam em suas unidades. Estas informações subsidiarão tanto a tomada de decisão no âmbito da gestão em cada secretaria, como também a tomada de decisão no âmbito das instâncias colegiadas que tratam do tema: Comitê Interno de Governança – CIG-MCTI e Comitê Técnico de Gestão de Riscos – CTGR-MCTI.

Os ciclos de monitoramento ocorrerão de acordo com a seguinte periodicidade:

- ✓ Bianaualmente, em se tratando da implementação da política de gestão de riscos;
- ✓ Anualmente, no que se refere à implementação do processo de gerenciamento de riscos pelas unidades; e
- ✓ No caso da implementação dos planos de tratamento de riscos pelas unidades e da verificação dos níveis de riscos, os ciclos de monitoramento devem considerar o tempo requerido para que as ações contidas no Plano de Tratamento de Riscos (já especificado no item 5.6) sejam implementadas e produzam seus efeitos.

Por fim, quando os riscos forem associados aos objetivos estratégicos do planejamento estratégico institucional, os ciclos de monitoramento precisam acompanhar a periodicidade de monitoramento deste processo.

7. COMUNICAÇÃO

Trata-se de processo de trabalho contínuo que consiste em relatar e compartilhar informações referentes à gestão de riscos sobre determinado objeto às partes interessadas, observada a classificação da informação quanto ao sigilo.

O acesso a informações confiáveis, íntegras e tempestivas é vital para a eficiência da gestão visando facilitar o alcance dos objetivos institucionais. Para que isso seja possível, o fluxo das comunicações deve permitir que as informações fluam em todas as direções, bem como a orientação tempestiva e clara quanto a melhor aplicação de ferramentas que suportam a gestão de risco deve ser acessível.

Quanto à direção, o fluxo de comunicação pode ser dividido em duas: **vertical** e **horizontal**.

A **comunicação vertical** é executada a partir da base para a alta administração ou vice-versa, possibilitando que a alta administração seja informada de riscos por todas as unidades organizacionais e que os demais servidores tenham consciência dos principais riscos que afetam a organização.

A **comunicação horizontal** é importante para dar conhecimento igualitário sobre os riscos de um processo que envolva diferentes unidades (processos transversais), a todos os que trabalham ou são afetados por esse processo. Também se dará via comunicação horizontal o assessoramento técnico especializado na metodologia de gestão de risco adotada pelo órgão. Esse suporte especializado será importante para que as áreas técnicas compreendam a temática, procedam com a implementação do processo de gerenciamento de riscos e, também, verificam a pertinência de se acionar as instâncias colegiadas para dirimir tema de cunho geral para a boa gestão de riscos no órgão.

No âmbito do processo de gestão de riscos no MCTI cada ator tem suas competências estabelecidas na Política de Gestão de Riscos do MCTI (Portaria MCTI nº 5.305/2021). Dessa forma, para que a comunicação deste processo seja efetiva, cada ator deverá ficar atento e executar seu papel de modo efetivo.

8. MELHORIA CONTÍNUA

A gestão de riscos é aperfeiçoada sucessivamente por meio do aprendizado e experiências (ISO 31000, 2018). Assim, como em outros processos organizacionais, a melhoria contínua é a estratégia para aprimorar as práticas no processo de gestão de risco.

A melhoria contínua consiste no aperfeiçoamento e ajustes sistemáticos de aspectos da gestão de riscos a partir da identificação de oportunidades de aprimoramento decorrentes do exercício da governança e da gestão do processo de gestão de riscos no âmbito do MCTI.

Em grande medida, é a partir do monitoramento e da avaliação, que incidem sobre todas as etapas do processo de gestão de riscos, que são evidenciadas as necessidades de aprimorar o processo de gestão de riscos de um órgão.

Na busca por maior efetividade do processo de gestão de risco, a necessidade de melhoria contínua poderá incidir nas seguintes dimensões:

- 1ª) nos normativos internos que regulamentam o tema no órgão;
- 2ª) no arranjo de governança do processo de gestão de riscos; e
- 3ª) em todas as etapas do processo de gestão de riscos, ora apresentado nesta metodologia, que será implementado pelas unidades deste Ministério.

9. CONSIDERAÇÕES FINAIS

Esta Metodologia de Gestão de Riscos do Ministério da Ciência, Tecnologia e Inovações (MCTI) tem como principal objetivo subsidiar a sistematização e a padronização da gestão de riscos nas unidades deste órgão. Pretende-se também contribuir para o estabelecimento de cultura de boas práticas da gestão de riscos para tomada de decisão gerencial.

A metodologia adotada pelo Ministério da Ciência, Tecnologia e Inovações (MCTI), incorpora boas práticas reconhecidas pelo COSO ERM e pela ISO 31000. Além disso, é aderente à Instrução Normativa Conjunta CGU/MP nº 01, de 10 de maio de 2016 e ao Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

Na aplicação desta metodologia, é importante registrar, organizar, documentar e referenciar os dados e informações considerados, visando evidenciar o embasamento do resultado, subsidiar a sua aprovação pelos atores competentes, bem como produzir um histórico dos fatos que serão importantes para futuras ações dos gestores.

Destaca-se que em qualquer iniciativa de desenvolvimento de metodologias, é fundamental a realização de ajustes para adequação ao contexto da unidade. Com intuito de melhorar continuamente o processo de gestão de riscos no MCTI, esta metodologia estará em constante aperfeiçoamento. Portanto, *feedbacks* após a aplicação pelas unidades serão essenciais ao seu aprimoramento.

Ressalta-se que a realização de projetos-piloto pelas unidades para implantação do processo de riscos, com uso desta metodologia e suas ferramentas de suporte, é recomendada. A partir das experiências-piloto, os gestores e equipes terão maior *expertise* e segurança para prosseguirem com a aplicação nos demais objetos da gestão de riscos priorizados pelas unidades.

Por fim, destaca-se que é primordial que o levantamento e gerenciamento de riscos façam parte das atividades cotidianas de cada unidade do MCTI, e para que isso aconteça é necessário que os gestores (de nível estratégico, tático e operacional) priorizem internamente em suas áreas a implementação desta metodologia nos objetos da gestão de riscos (processo, projetos, atividades, etc.) sob sua responsabilidade. Esta medida, juntamente com a implantação e monitoramento do plano de tratamento de riscos, irá contribuir com a entrega de melhores serviços pelo MCTI.

10. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**: gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**: gestão de riscos: princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 31010**: gestão de riscos: técnicas para o processo de avaliação de riscos. Rio de Janeiro: ABNT, 2012.

BRASIL. Controladoria-Geral da União. **Metodologia de gestão de riscos da CGU**. Brasília: CGU, 2021.

BRASIL. Controladoria-Geral da União. **Portaria nº 57, de 4 de janeiro de 2019**. Altera a Portaria CGU nº 1.089, de 25 de abril de 2018, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. Brasília, DF: CGU, 2019. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/58029864 . Acesso em: 9 fev. 2022.

BRASIL. Controladoria-Geral da União; Ministério do Planejamento, Orçamento e Gestão. **Instrução Normativa Conjunta nº 1, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, DF: CGU, MP, 2016. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197 . Acesso em: 9 fev. 2022.

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF: Presidência da República, 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm . Acesso em: 9 fev. 2022.

BRASIL. Escola Nacional de Administração Pública. **Implementando a gestão de riscos no setor público**. Brasília: ENAP, 2018. Disponível em: <https://www.escolavirtual.gov.br/curso/127> . Acesso em: 9 fev. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 5.202, de 23 de setembro de 2021**. Aprova o Regimento Interno do Comitê Interno de Governança do Ministério da Ciência e Tecnologia e Inovações - CIG-MCTI e altera a Portaria MCTI nº 4.301, de 12 de janeiro de 2021. Brasília, DF: MCTI, 2021. Disponível em: <https://in.gov.br/en/web/dou/-/portaria-n-5.202-de-23-de-setembro-de-2021-348154495> . Acesso em: 9 fev. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 5.205, de 28 de setembro de 2021**. Institui a Política de Governança Institucional do Ministério da Ciência, Tecnologia e Inovações. Brasília, DF: MCTI, 2021. Disponível em: <https://in.gov.br/en/web/dou/-/portaria-mcti-n-5.205-de-28-de-setembro-de-2021-349280966> . Acesso em: 9 fev. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 5.305, de 17 de novembro de 2021**. Institui a Política de Gestão de Riscos e cria o Comitê Técnico de Gestão de Riscos do Ministério da Ciência, Tecnologia e Inovações. Brasília, DF: MCTI, 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-5.305-de-17-de-novembro-de-2021-360546754> . Acesso em: 9 fev. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 4. 301, 12 de janeiro de 2021**. Institui o Comitê Interno de Governança do Ministério da Ciência, Tecnologia e Inovações e dá outras providências. Brasília, DF: MCTI, 2021. Disponível em: <https://www.in.gov.br/web/dou/-/portaria-n-4.301-de-12-de-janeiro-de-2021-299075399>. Acesso em: 9 fev. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. Secretaria Executiva. **Portaria nº 1.395, de 13 de dezembro de 2021**. Designa membros do Comitê técnico de gestão de riscos do MCTI. Brasília, DF: MCTI, 2021. Disponível em: <https://repositorio.mctic.gov.br/handle/mctic/3705>. Acesso em: 9 fev. 2022.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de gestão de riscos**. Brasília: CGU, 2018. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/41820/14/Manual_Operacional.pdf. Acesso em: 9 fev. 2022.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 1.089, de 25 de abril de 2018**. Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. Brasília: CGU, 2018. Disponível em: https://www.in.gov.br/web/guest/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/11984199/do1-2018-04-26-portaria-n-1-089-de-25-de-abril-de-2018-11984195. Acesso em: 9 fev. 2022.

BRASIL. Ministério do Desenvolvimento Regional. **Metodologia de gestão de riscos do Ministério do Desenvolvimento Regional**. Brasília: MDR, 2020. Disponível em: https://www.gov.br/mdr/pt-br/aceso-a-informacao/governanca/Metodologia_de_Gesto_de_Riscos_final2.pdf. Acesso em: 9 fev. 2022

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Manual de gestão de integridade, riscos e controles internos da gestão**. Brasília: MP, 2017. Disponível em: https://www.gov.br/economia/pt-br/centrais-de-conteudo/publicacoes/planejamento/controle-interno/manual_de_girc__versao_2_0.pdf. Acesso em: 9 fev.2022.

BRASIL. Tribunal de Contas da União. **10 passos para a boa gestão de riscos**. Brasília: TCU, 2018. Disponível em: https://portal.tcu.gov.br/data/files/3F/D5/65/C0/27A1F6107AD96FE6F18818A8/10_passos_boa_gestao_riscos.pdf. Acesso em: 12 dez. 2021.

BRASIL. Tribunal de Contas da União. **Manual de gestão de riscos do TCU. 2. ed.** Brasília: TCU, 2020. Disponível em: https://portal.tcu.gov.br/data/files/46/B3/C6/F4/97D647109EB62737F18818A8/Manual_gestao_riscos_TCU_2_edicao.pdf. Acesso em: 7 maio 2021.

Committee of Sponsoring Organizations of the Treadway Commission. **Enterprise risk management: integrated framework**. [S. l]: COSO, 2004.

Committee of Sponsoring Organizations of the Treadway Commission. **Enterprise risk management: integrating with strategy and performance**. [S. l]: COSO, 2017.

THE ORANGE book: management of risk: principles and concepts. UK: HM Treasury on behalf of the Controller of Her Majesty's Stationery Office, 2001.

11. GLOSSÁRIO

Apetite pelo risco: quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir.

Bow-Tie: diagrama que permite visualizar o risco, suas causas e consequências, medidas preventivas (para evitar as causas) e medidas atenuantes (para lidar com as consequências).

Componentes dos controles internos da gestão: são o ambiente de controle interno da entidade, a avaliação de risco, as atividades de controles internos, a informação e comunicação e o monitoramento.

Consequência: resultado de um evento que afeta os objetivos.

Controle: medida que está modificando o risco.

Controles internos da gestão: 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, destinados a enfrentar os riscos e fornecer segurança razoável para que o Ministério da Ciência, Tecnologia e Inovações, na consecução de sua missão, realize execução ordenada, ética, econômica, eficiente e eficaz das operações, cumpra com as obrigações de *accountability*, as leis e os regulamentos, e salvguarde os recursos para evitar perdas, mau uso e danos.

Crterios de risco: termos de referncia contra os quais a significncia de um risco avaliada.

Estrutura de gesto de riscos: conjunto de elementos que fornecem os fundamentos e disposies organizacionais para conceber, implementar, monitorar, rever e melhorar continuamente a gesto do risco em toda a organizao.

Evento: ocorrncia ou mudana em um conjunto especfico de circunstncias.

Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrnseco para dar origem ao risco.

Gerenciamento de riscos: processo de identificação, avaliação, administração e controle de potenciais eventos para fornecer maior segurança quanto ao alcance dos objetivos organizacionais.

Gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestor de risco: agente que tem a responsabilidade e a autoridade para gerenciar determinado risco.

Impacto: efeito resultante da ocorrência do evento.

Monitorar riscos: compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

Nível de risco: magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades.

Objeto de gestão de riscos: qualquer processo de trabalho, atividade, projeto, iniciativa, ação de plano institucional, assim como quaisquer outros recursos que dão suporte à realização dos objetivos do Ministério da Ciência, Tecnologia e Inovações.

Parte interessada: pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade.

Plano de gestão de riscos: esquema dentro de uma estrutura de gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos.

Política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

Perfil de risco: descrição de um conjunto qualquer de riscos.

Probabilidade: chance de algo acontecer.

Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

Processo de trabalho: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.

Processo prioritário: processo que devido a sua relevância deverão ser priorizados na implementação da Gestão de Riscos no MCTI.

Resposta a risco: refere-se à identificação da estratégia, se evitar, transferir, aceitar ou tratar, a ser seguida pela organização em relação aos riscos mapeados e avaliados, considerando os níveis de exposição aos riscos previamente estabelecidos.

Risco-chave: risco que, em função do impacto potencial ao MCTI, deve ser conhecido pela alta administração.

Risco inerente: risco a que uma organização está exposta desconsiderando quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco Real: nível do risco que existe na situação concreta, considerados os controles porventura existentes.

Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

Riscos: efeito da incerteza nos objetivos a serem atingidos pela instituição.

Tolerância ao risco: nível de variação aceitável quanto à realização de um determinado objetivo

ANEXOS

ANEXO I - FORMULÁRIO DE ANÁLISE DE CONTEXTO DE OBJETO DA GESTÃO DE RISCOS*

ANÁLISE DO CONTEXTO	
1. Quais objetivos ou resultados devem ser alcançados pelo objeto da gestão de risco em análise?	
2. Quais as atividades são relevantes para o alcance dos objetivos e resultados deste objeto em análise?	
3. Quais são os atores envolvidos no objeto da gestão de riscos em análise e quais são os especialistas da área?	
ANÁLISE SWOT	
FORÇAS	OPORTUNIDADES
<i>Descreva aqui as características internas que representam uma facilidade para o alcance dos objetivos.</i>	<i>Descreva aqui as situações positivas do ambiente externo que permitem o cumprimento da Missão do MCTI.</i>
FRAQUEZAS	AMEAÇAS
<i>Descreva aqui os fatores internos que oferecem risco à execução do processo.</i>	<i>Descreva aqui as situações externas sobre as quais se tem pouco controle, que representam dificuldades para o cumprimento da Missão do MCTI.</i>
<p>* Objeto da gestão de riscos: qualquer processo de trabalho, atividade, projeto, iniciativa, ação de plano institucional, assim como quaisquer outros recursos que dão suporte à realização dos objetivos do Ministério da Ciência, Tecnologia e Inovações (Portaria MCTI n. 5.305/2021, art. 5º, inciso XXIV).</p>	

Orientações para preenchimento da Tabela Modelo de Suporte à Identificação de Riscos.

1. Informe o nome do objeto que será objeto de avaliação de riscos.
2. Poderá ser classificado em Processo, Projeto, Atividade, Programa, Ação, etc.
3. Descreva o objeto (processo, projeto, ação, etc.) que será submetido à avaliação de riscos, detalhando suas principais etapas e seus objetivos com clareza.
4. Descreva o evento de risco identificado: o efeito da incerteza nos objetivos a serem atingidos.
5. Descreva as condições que dão origem à possibilidade de um evento de risco ocorrer.
6. Descreva os possíveis impactos do evento de risco sobre os objetivos, caso ele se materialize.
7. Poderá ser classificado em Pessoas, Processos, Sistemas, Tecnologias, Infraestrutura ou Evento Externo. Vide a “Tabela 1 - Fontes de Riscos e Fragilidades” no capítulo 5.3.
8. Responda se o risco identificado está associado à integridade com “sim” ou “não”.
9. Informe a tipologia de risco prevalente: Estratégico, Operacional, Orçamentário e Financeiro, Fiscal, Imagem, Integridade, Legal ou Social.
10. Informe a tipologia de risco secundária, dentre o rol: Estratégico, Operacional, Orçamentário e Financeiro, Fiscal, Imagem, Integridade, Legal ou Social.

ANEXO III - MODELO DE PLANO DE TRATAMENTO DE RISCOS

PLANO DE TRATAMENTO DE RISCOS														
EVENTOS DE RISCOS					RISCO RESIDUAL			MEDIDAS DE TRATAMENTO DOS RISCOS						
N. Ord.	Evento de Risco	Causas	Efeitos ou Conseqüências	Nome do objeto da Gestão de Riscos	Tipo de objeto da gestão de riscos	Classificação ¹	Nível do Risco ²	Opção de Tratamento ³	Tipo de Controle ⁴	Descrição da medida de tratamento ⁵	Unidade Responsável	Gestor do Risco ⁶	Data do Início	Data da Conclusão
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														

Orientações para preenchimento da Tabela Modelo de Plano de Tratamento de Riscos

1. Poderá ser classificado em Baixo, Médio, Alto ou Extremo, de acordo com o previsto na Tabela 4 - Classificação do Risco e Figura 6 - Matriz de Riscos, da página 19 desta metodologia.
2. O risco residual poderá variar de 0,2 a 25, conforme se verifica na Tabela 4 - Classificação do Risco página 19 desta metodologia.
3. São opções de tratamento: Aceitar, Mitigar, Transferir/Compartilhar ou Evitar.
4. Poderá ser: corretivo ou preventivo, conforme detalhado na p.20.
5. Descreva as medidas que serão implementadas para modificar o nível do risco, sempre considerando custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do das medidas de tratamento, dentre outros critérios.
6. O agente que tem a responsabilidade e a autoridade para gerenciar o risco identificado.



METODOLOGIA DE GESTÃO DE RISCOS

1ª Edição / 2022

Brasília – DF

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES



METODOLOGIA DE GESTÃO DE RISCOS

1ª Edição / 2022

Brasília – DF

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES

