# Metodologia de Gestão de Riscos

Ministério da Previdência Social

Assessoria Especial de Controle Interno

MINISTÉRIO DA PREVIDÊNCIA SOCIAL

Maio de 2026

Ministério da Previdência Social

## Ficha Técnica

Wolney Queiroz Maciel

Ministro da Previdência Social

Felipe Cavalcante e Silva

Secretário-Executivo

Benedito Adalberto Brunca

Secretário de Regime Geral de Previdência Social

Paulo Roberto dos Santos Pinto

Secretário de Regime Próprio e Complementar

## Equipe Técnica

Isadora Jinkings Melo Silva

Chefe da Assessoria Especial de Controle Interno

Gilvaneire Cavalcanti Beltrão

Coordenadora-Geral de Demandas de Controle

Rhamu Guimarães Aguiar de Oliveira

Assessor Técnico

# Sumário

## Apresentação

O fortalecimento da governança pública exige que as organizações desenvolvam capacidade institucional para lidar com incertezas, antecipar riscos e aprimorar continuamente seus processos decisórios.

Nesse contexto, a gestão de riscos constitui instrumento essencial para apoiar a tomada de decisão baseada em evidências, promover o uso eficiente dos recursos públicos e fortalecer a integridade institucional.

No âmbito da Administração Pública Federal, a adoção de práticas estruturadas de gestão de riscos foi consolidada por importantes marcos normativos, entre os quais se destacam:

- Instrução Normativa Conjunta CGU/MP nº 1, de 2016;
- Decreto nº 9.203, de 2017, que estabelece a política de governança da administração pública federal;
- Orientações metodológicas da Controladoria-Geral da União e do Tribunal de Contas da União.

No Ministério da Previdência Social, a gestão de riscos integra o conjunto de instrumentos destinados ao fortalecimento da governança institucional, ao lado do planejamento estratégico, do Programa de Integridade e dos controles internos da gestão.

A presente Metodologia de Gestão de Riscos do MPS tem por objetivo estabelecer diretrizes, conceitos, processos e instrumentos que orientem a identificação, análise, avaliação, tratamento e monitoramento de riscos institucionais.

O documento consolida um modelo metodológico integrado aplicável a diferentes dimensões da atuação institucional, contemplando:

- riscos estratégicos;
- riscos de processos organizacionais;
- riscos relacionados às contratações públicas;
- riscos associados à implementação de políticas públicas;
- riscos à integridade.

Ao estabelecer uma linguagem comum e procedimentos padronizados, a metodologia busca fortalecer a cultura de gestão de riscos no Ministério e

apoiar os gestores no aprimoramento contínuo da administração previdenciária.

## • Introdução

A gestão de riscos constitui um dos instrumentos centrais da governança pública contemporânea, sendo reconhecida como mecanismo essencial para fortalecer a capacidade do Estado de formular, implementar e avaliar políticas públicas, bem como assegurar o uso eficiente, eficaz e transparente dos recursos públicos.

No âmbito da Administração Pública Federal, a adoção de práticas estruturadas de gestão de riscos foi consolidada por importantes marcos normativos, destacando-se a Instrução Normativa Conjunta MP/CGU nº 1/2016 e o Decreto nº 9.203/2017, que estabeleceu a governança pública como conjunto de mecanismos de liderança, estratégia e controle destinados a avaliar, direcionar e monitorar a gestão.

Em consonância com essas diretrizes, o Ministério da Previdência Social instituiu sua Política de Governança por meio da Portaria MPS nº 166/2026, que reconhece a gestão de riscos, o programa de integridade e os controles internos como instrumentos estruturantes para o fortalecimento da governança institucional e da geração de valor público.

Nesse contexto, a presente Metodologia de Gestão de Riscos do Ministério da Previdência Social tem por objetivo estabelecer um modelo integrado para identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos relacionados às diversas dimensões da atuação institucional.

## • Gestão de Riscos

## 2.1. O que é Risco

Conforme a ABNT ISO 31000:2018, risco é entendido como o efeito da incerteza sobre os objetivos. Isso significa que o risco pode ter um impacto positivo (oportunidades) ou negativo (ameaças) nos resultados de uma organização. A norma enfatiza que a gestão de riscos deve ser parte integrante da governança e da tomada de decisões em todos os níveis organizacionais.

## 2.2. Quais categorias riscos estamos expostos

- **Da Estratégia** - Eventos que podem impactar a estratégia organizacional com efeitos sobre a missão, as metas ou os objetivos estratégicos do MPS.
- **Operacionais** - Probabilidade de ocorrência de impactos ou consequências resultantes de falhas, devido a deficiências ou inadequações em processos internos, pessoas, sistemas ou de eventos externos que afetam a operação cotidiana.
- **Imagem ou Reputação** - Eventos que podem prejudicar a credibilidade, confiança pública e, consequentemente, os resultados do MPS.
- **Legais ou Conformidade** – Eventos que podem afetar o cumprimento de leis, regulamentos, normas ou obrigações contratuais aplicáveis ao ministério.
- **Financeiros/Orçamentários** - Eventos que podem comprometer o orçamento planejado e o realizado, com efeito sobre a sustentabilidade financeira, a execução de políticas públicas e projetos ou o cumprimento de metas institucionais.
- **Integridade** – Eventos que podem comprometer as atividades do MPS, normalmente associados a corrupção, fraude, irregularidade ou desvio ético ou de conduta. Os riscos para a integridade podem ser causa,

evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem (Portaria CGU nº 1.089/2018[1]).

#### 2.2.1. Riscos Estratégicos

Riscos estratégicos para o MPS são todos os eventos que sozinho ou combinado podem afetar o atingimento dos objetivos estratégicos. Desta forma, qualquer evento categorizado conforme relação acima, se impactar o objetivo do ministério, pode ser considerado estratégico.

### 2.3. Porque gerenciar risco

A gestão de riscos é uma importante ferramenta para avaliar potenciais problemas e para prevenir (prevenção de imprevistos) ou reduzir os impactos (correlação e custo) a que um processo pode ser sujeito.

O propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos. Ainda, conforme a ABNT ISO 31000:2018, gerenciar riscos auxilia as organizações no estabelecimento de estratégias, no alcance dos objetivos e na tomada de decisão, principalmente por ser parte integrante da governança e liderança.

### 2.4. Modelo de gestão de risco

O modelo adotado baseia-se nas boas práticas de gestão de riscos, especialmente aquelas previstas na norma ABNT ISO 31000:2018, no framework COSO ERM, bem como na experiência metodológica desenvolvida pelos demais órgãos da Administração Pública Federal.

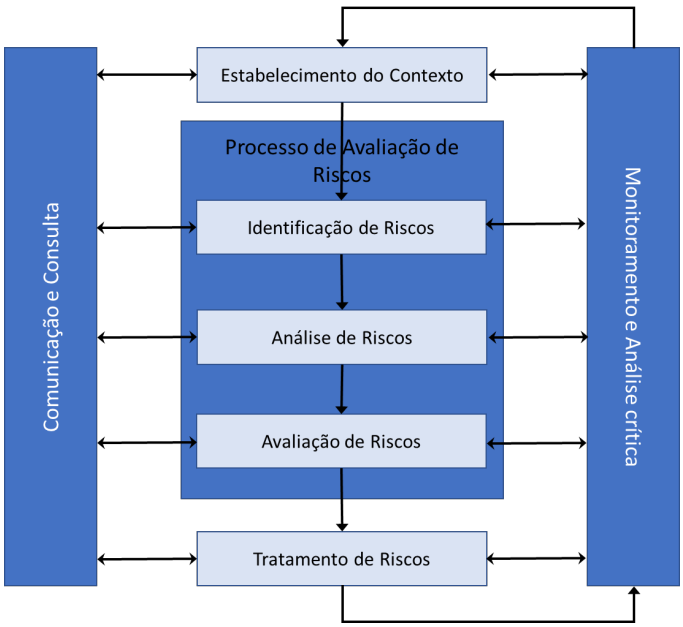
A metodologia foi estruturada a partir da integração de diferentes abordagens de gestão de riscos, aplicáveis aos distintos contextos organizacionais do Ministério, contemplando:

- riscos à integridade;
- riscos associados à avaliação de políticas públicas;
- riscos de processos organizacionais;
- riscos relacionados às contratações públicas;
- riscos da estratégia.

[1] https://www.gov.br/secretariageral/pt-br/estrutura/secretaria_de_controle_interno/arquivos/normativos/portaria-cgu-1089-2018.pdf

Essa estrutura integrada busca assegurar linguagem comum, padronização metodológica e coerência institucional na aplicação da gestão de riscos no Ministério.

De forma geral, o processo de gestão de riscos compreende as seguintes etapas:




*Adaptado - Processo de Gestão de Riscos – ABNT ISO 31000:2018*

Essas etapas permitem estruturar um processo sistemático de gestão das incertezas que podem impactar o alcance dos objetivos institucionais do Ministério.

## 2.5. Abrangência da Gestão de Riscos

O processo de gestão de riscos pode ser aplicado nos três níveis estruturais do ministério, a depender da relevância do objeto a ser avaliado e das necessidades identificadas, ou orientações de órgãos supervisores.

- **Nível estratégico -** Esses riscos normalmente são avaliados pela alta administração. Riscos que impactam:
  - missão institucional;
  - políticas públicas;
  - reputação institucional.

  Responsáveis:

  - alta administração;

  - comitê de governança;
- **Nível tático -** Riscos relacionados a:
  - Programas;
  - projetos;
  - áreas organizacionais.

  Responsáveis:

  - Gerentes e Diretores;
  - Coordenadores-Gerais.
- **Nível operacional** - É o nível onde ocorre a maior parte da identificação e tratamento de riscos. O nível operacional trata dos riscos associados aos:
  - Processos;
  - Atividades;
  - operações diárias.

  Responsáveis:

  - gestores de processo;
  - chefes de divisão e serviços;
  - equipes operacionais.

## • Instâncias de Gestão e Supervisão

O modelo utilizado e determinado pela CGU para aplicação pelos órgãos e entidades do Poder Executivo é o *Modelo de Três Linhas*[2], previsto na Instrução Normativa Conjunta MP/CGU Nº 01[3], de 2016.

Ele demonstra ser mais eficaz quando adaptado para se alinhar aos objetivos e circunstâncias do ministério. A forma como será estruturado e como os papéis são atribuídos, deve ser determinada pela gestão e pelo órgão de governança, mais especificamente o Comitê Estratégico de Governança do MPS.

[2] Instituto dos Auditores Internos do Brasil
[3] Publicação no Diário Oficial

O Comitê Estratégico de Governança do MPS pode estabelecer comitês ou outra estrutura para prestar supervisão adicional sobre aspectos de sua responsabilidade, como auditoria, riscos, finanças, planejamento e remuneração.


De forma geral, na gestão, é provável que haja arranjos funcionais e hierárquicos e uma tendência crescente à especialização, conforme as organizações aumentam em tamanho e complexidade.

## 3.1. Órgãos de Governança

Os órgãos de governança ministerial são responsáveis por garantir a eficiência e a transparência na gestão pública. O Comitê Estratégico de Governança (CEG), que é instância máxima de governança do Ministério, foi instituído pela Portaria MPS Nº 166[4], de 2 de fevereiro de 2026. Esse órgão tem caráter consultivo e deliberativo, com a finalidade de assessorar o Ministro de Estado da Previdência Social na execução da política de governança da administração pública federal, em consonância com os princípios, diretrizes e mecanismos estabelecidos pelo Decreto nº 9.203, de 22 de novembro de 2017.

[4] https://in.gov.br/en/web/dou/-/portaria-mps-n-166-de-2-de-fevereiro-de-2026-685369232.

Adicionalmente, com a finalidade de promover a interlocução entre as unidades vinculadas e o MPS para fins de subsidiar a atividade de supervisão ministerial quanto ao acompanhamento das recomendações emanadas pelos órgãos de controle interno e externo, bem como o alinhamento sobre assuntos voltados à integridade, transparência e gestão de riscos, foi instituído o Comitê de Controle Interno do Ministério da Previdência Social, pela Portaria MPS Nº 1.446[5], de 10 de julho de 2025.

Para a realidade dos ministérios e demais órgãos que compõem a Administração Pública Federal, a IN Conjunta MP/CGU nº 1/2016, adicionada a IN SFC/CGU nº 3[6]/2017, representam a base normativa de atuação das Três linhas.

### 3.2. Papéis da Primeira Linha – Unidades executoras

Responsável pela gestão operacional, é formada pelos próprios gestores e "equipes de negócio". Eles são os "donos" dos riscos: identificam, avaliam e respondem a eles no cotidiano por meio de controles internos inseridos nos processos. A responsabilidade é primária e direta — se um controle falha, é nessa linha que o problema emerge primeiro.

Os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio.

Exemplos práticos do papel da Primeira Linha no MPS:

- Liderar e dirigir ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da organização.
- Manter um diálogo contínuo com o órgão de governança e reportar: resultados planejados, reais e esperados, vinculados aos objetivos da organização; e riscos.
- Estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno).

[5] *https://www.in.gov.br/web/dou/-/portaria-mps-n-1.446-de-10-de-julho-de-2025-642213140.*
[6] https://www.gov.br/cgu/pt-br/assuntos/auditoria-e-fiscalizacao/links/Instrucao_Normativa_CGU_3_2017.pdf

- Garantir a conformidade com as expectativas legais, regulatórias e éticas.

No âmbito do MPS a primeira linha é composta pelas funções de gerência operacional responsáveis por monitorar e controlar os processos de trabalho, representada por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio do MPS. São as unidades organizacionais do MPS, representadas pelos seus respectivos dirigentes responsáveis pelos controles internos da sua área de atuação. Ex. Secretarias, Assessorias, Diretorias, Coordenações, Divisões, Serviços, Gerências, Conselhos e outras unidades correlatas do MPS.

### 3.3. Papéis da Segunda Linha - AECI

Responsável pelas funções de controle e conformidade, os papéis de segunda linha podem incluir monitoramento, assessoria, orientação, teste, análise e reporte sobre assuntos relacionados ao gerenciamento de riscos. Executam a supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance.

O papel é de supervisão e suporte: essas funções estabelecem políticas, monitoram a atuação da primeira linha quanto ao cumprimento das normas/regras e oferecem especialização técnica para o gerenciamento de riscos. Elas não eliminam a responsabilidade da primeira linha, mas atuam visando ampliar a capacidade de controle da organização.

Os papéis de segunda linha fornecem assistência à primeira linha no gerenciamento de riscos.

Exemplos práticos do papel da Segunda Linha no MPS:

- Fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo:
  - O Desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno).
  - O atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e

comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade.

- Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).

Conforme definido pela Controladoria Geral da União, na Instrução Normativa Nº03[7], de 09 de junho de 2017, *"os Assessores e Assessorias Especiais de Controle Interno (AECI) nos Ministérios integram a segunda linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações."*

## 3.4. Papéis da Terceira Linha - CGU

Responsável pela auditoria interna, ela atua com independência em relação às duas primeiras linhas. Sua função é fornecer garantia objetiva à alta direção de que o conjunto de controles das primeira e segunda linhas está funcionando adequadamente.

Constituída pelas auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha) e da supervisão dos controles internos (segunda linha).

Vale notar que, na atualização do modelo pelo IIA em 2020, o foco se ampliou para além de controles internos: o modelo passou a enfatizar a criação de valor e o alinhamento com os objetivos estratégicos da organização, não apenas a mitigação de riscos.

Exemplos práticos do papel da Terceira Linha no MPS:

- Mantém a prestação de contas primária perante o órgão de governança e a independência das responsabilidades da gestão.
- Comunica avaliação e assessoria independentes e objetivas à gestão e ao órgão de governança sobre a adequação e eficácia da governança e do gerenciamento de riscos (incluindo controle

[7] https://www.gov.br/cgu/pt-br/assuntos/auditoria-e-fiscalizacao/links/Instrucao_Normativa_CGU_3_2017.pdf

interno), para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua.

- Reporta ao órgão de governança prejuízos à independência e objetividade e implanta salvaguardas conforme necessário.

No âmbito do Poder Executivo, a Controladoria-Geral da União foi incumbida, como Órgão Central, da orientação normativa e da supervisão técnica dos órgãos que compõem o Sistema de Controle Interno do Poder Executivo Federal, conforme Decreto Nº 3.591[8], de 06 de setembro de 2000.

### 3.5. Controle Externo - TCU

Auditoria externa é o agente mais conhecido nesse papel. Diferente da auditoria interna (terceira linha), ela pode ser contratada por acionistas, no caso de empresas privadas, ou exigida por lei para emitir uma opinião independente sobre as demonstrações financeiras, no caso do setor público.

Cabe ressaltar que a auditoria interna serve à alta administração e ao comitê estratégico como ferramenta de melhoria contínua; a auditoria externa serve a partes externas como instrumento de confiança e transparência. Mais especificamente o Tribunal de Contas da União (TCU) é considerado auditor externo para o setor público, conforme Constituição Federal de 1988 arts. 70 a 73.

- O Controle externo presta avaliação adicional para:
  - Cumprir com as expectativas legislativas e regulatórias que servem para proteger os interesses dos stakeholders.
  - Atender aos pedidos da gestão e do órgão de governança para complementar as fontes internas de avaliação.

## • Referencial Normativo e Teórico

Relacionamos abaixo alguns dos principais normativos utilizados pelo MPS e pela administração pública, como referência metodológica e normativa, para condução do tema gestão de riscos, controles internos e governança.

[8] https://www.planalto.gov.br/ccivil_03/decreto/D3591.htm

### 4.1. ABNT NBR ISO 31000:2018 – Gestão de Riscos

A ISO 31000 é uma norma global que estabelece orientações e diretrizes para a administração de riscos, sendo aplicável a qualquer tipo de entidade, independentemente do tamanho ou ramo de atividade. Criada pela Organização Internacional de Normalização (ISO), fornece um método abrangente e genérico para identificar, analisar e administrar riscos que possam afetar os objetivos de uma organização, sejam eles financeiros, operacionais, de segurança ou de reputação.

Ela auxilia na gestão proativa de incertezas, na salvaguarda dos recursos da organização e na geração de valor, incentivando decisões mais conscientes e estratégicas.

### 4.2. Instrução Normativa Conjunta MP/CGU nº 1/2016

A Instrução Normativa Conjunta MP/CGU nº 1/2016 define orientações para controles internos, gerenciamento de riscos e governança no contexto do Poder Executivo Federal. Ela tem como objetivo assegurar que as entidades públicas implementem práticas estruturadas para a administração de riscos e a efetividade dos controles internos, incentivando o aprimoramento constante dos processos administrativos. A norma é essencial para garantir a transparência e a eficácia na implementação de políticas públicas, garantindo que as metas definidas sejam atingidas de maneira eficiente e econômica.

### 4.3. Instrução Normativa SFC/CGU nº 3/2017

Instrução Normativa SFC/CGU nº 3 aprova e institui o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, regras que devem ser observadas pelos órgãos e unidades que integram o Sistema de Controle Interno do Poder Executivo Federal.

### 4.4. Normas e diretrizes de Governança

O Decreto nº 9.203, de 22 de novembro de 2017, dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Este decreto estabelece diretrizes para a gestão e a transparência na administração pública, visando melhorar a eficiência e a eficácia dos serviços prestados.

O Decreto n° 6.029, de 1º de fevereiro de 2007, é competência da Comissão de Ética atuar como instância consultiva de dirigentes e servidores do MPS; aplicar o Código de Ética dos Servidores do Executivo, dirimir dúvidas a respeito da interpretação de suas normas; apurar conduta em desacordo com as normas éticas; recomendar, acompanhar e avaliar, no âmbito do MPS, a disseminação, capacitação e treinamento sobre as normas de ética e disciplina; representar o MPS nos eventos da Rede de Ética; e supervisionar a observância do Código de Conduta da Alta Administração.

## • Estrutura para a Gestão de Riscos

### 5.1. Metodologia

A Metodologia de Gestão de Riscos objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos no MPS, por meio da definição de um processo de gerenciamento de riscos.

Ela estabelece como o gerenciamento de riscos deve ser realizado de forma sistemática, padronizada e contínua, apoiando a tomada de decisão e a proteção dos resultados institucionais.

São necessárias, no mínimo, as seguintes etapas:

I – estabelecimento do contexto

II – Identificação de riscos

III – análise e avaliação de riscos

IV – tratamento dos riscos;

V – monitoramento dos riscos; e

VI – comunicação dos riscos.

### 5.2. Linguagem Única – Taxonomia de Riscos

A categorização de riscos refere-se a um sistema de classificação utilizado para agrupar uma variedade de itens, neste contexto, os riscos que podem impactar uma entidade, seus processos e metas estratégicas. Essa abordagem visa organizar, diferenciar e classificar riscos de maneira estruturada, estabelecendo uma terminologia comum que aprimora a comunicação, tanto interna quanto externa, a respeito dos riscos.

No âmbito do Ministério da Previdência Social estipulou-se uma base orientadora, constante no Anexo 1, de possíveis eventos dos riscos a que o ministério está exposto. Para o risco a integridade não foi feita definição dos eventos, pois será utilizada relação dos riscos divulgada pela CGU, com finalidade de alinhar o trabalho da terceira e segunda linha.

### 5.3. Política de Gestão de Riscos

Documento que estabelece princípios, objetivos, diretrizes, competências e responsabilidades para a implementação, o monitoramento e o aprimoramento contínuo da gestão de riscos e dos controles internos no âmbito do Ministério da Previdência Social a Política de Gestão de Riscos foi aprovada por meio da Resolução CEG/MPS nº 1, de 31 de março de 2026.

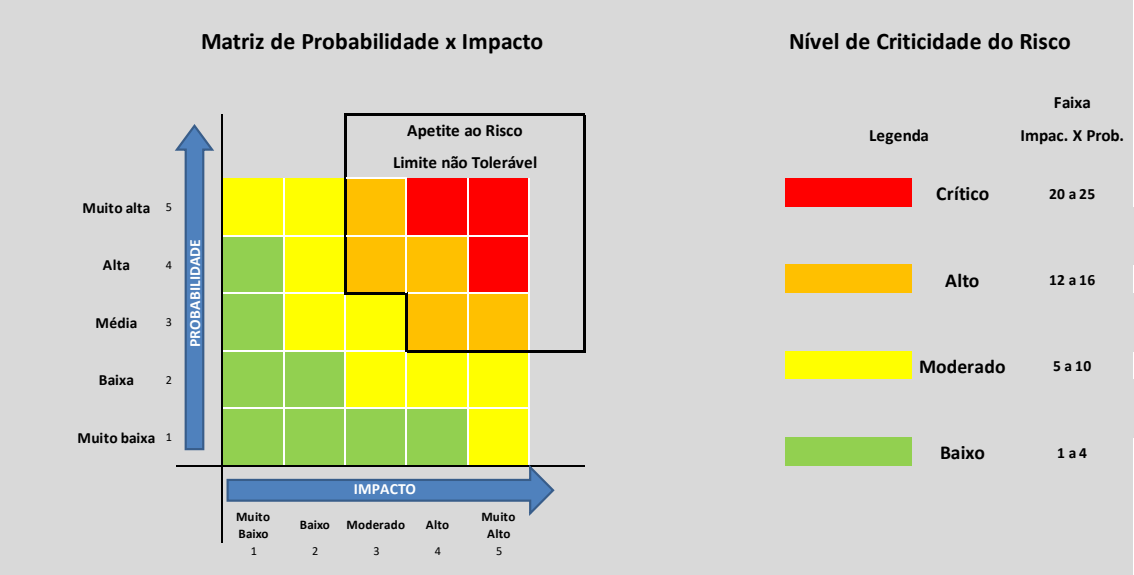
### 5.4. Apetite a Riscos

Apetite a risco é a quantidade e tipo de riscos que o MPS está disposto a buscar, reter ou assumir visando atingir seus objetivos organizacionais.

O apetite a riscos reflete o nível de risco, grau máximo de exposição que a instituição está disposta aceitar em suas atividades, projetos, iniciativas, e tem como propósito final, alcançar os objetivos estratégicos da Instituição.

A declaração de apetite a riscos, além de orientar a tomada de decisões relacionadas aos riscos institucionais, contribui para aprimorar a comunicação interna e externa acerca da forma como o MPS gerencia e responde aos riscos, podendo revisada e ajustada conforme as diretrizes estratégicas e o contexto definido pela alta administração.

Para o MPS, fica estabelecido o apetite a riscos moderado. Assim, os riscos classificados com criticidade baixa e moderada deverão ser objeto de monitoramento, enquanto os riscos classificados como altos e críticos deverão ter tratamento priorizado. Eventual adoção de entendimento diverso deverá ser devidamente justificada e submetida à aprovação da instância hierarquicamente superior ao gestor do risco.




### 5.5. Plano de Gestão de Riscos

É o documento que aborda os processos definidos como prioritários para o gerenciamento de riscos em determinado período.

É todo o planejamento e trabalhos necessários que antecedem a execução das etapas de gerenciamento de riscos. Para que se tenha êxito nas etapas posteriores é necessário que nessa etapa definam-se os seguintes pontos:

- Processos a serem gerenciados em determinado período;
- Unidade responsável pelo processo;
- Período de execução das atividades

## • Processo de Gestão de Riscos

O processo de gestão de riscos é a aplicação sistemática de políticas, procedimentos e

práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos, tendo como objetivo minimizar impactos negativos e maximizar oportunidades.

O Gestor de Risco é o responsável pelo processo organizacional da sua unidade, sendo a autoridade para gerenciar determinado risco da sua área de atuação e deve definir uma equipe para participar das etapas do processo de gerenciamento de riscos.

Essa equipe deve ser composta por servidores que conheçam o processo, seus objetivos, contextos, atores envolvidos, resultados e controles já existentes. A referida equipe será assessorada pelo Analista Setorial de Risco.

O Analista Setorial de Risco é o servidor indicado pelas unidades organizacionais para conduzir o processo de gestão de riscos, de acordo com as etapas estabelecidas na Metodologia de Gestão de Riscos do MPS, prestando apoio técnico e metodológico aos Gestores de Riscos no exercício de suas competências relacionadas à gestão de riscos.

### 6.1. Estabelecimento do Contexto

O estabelecimento do contexto é a etapa inicial e fundamental do processo de gestão de risco, é nessa etapa que o processo organizacional é conhecido e analisado levando-se em consideração o ambiente interno e externo do MPS, bem como do escopo de risco.

O escopo estabelece limites e abrangência do processo de gestão de riscos, ou seja, quais áreas, processos, projetos ou ativos serão considerados na identificação, análise e resposta aos riscos.

### 6.2. Identificar os riscos

A identificação de riscos visa construir uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos organizacionais ou das suas etapas críticas. A Identificação busca o reconhecimento e descrição dos riscos, mediante a identificação das categorias do risco, eventos, suas causas e suas consequências.

Os eventos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa.

Para a identificação das causas é importante uma análise das diversas fontes de riscos existentes.

Após a identificação dos riscos, causas e consequências, é necessário identificar quais controles estão presentes no processo e mitigam os riscos identificados.

### 6.3. Análise e Avaliação

Etapa que se analisa a natureza do risco, onde se determina o seu respectivo nível de criticidade, mediante a combinação da probabilidade de sua ocorrência e das consequências possíveis.

Se refere ao processo de avaliação do risco, com finalidade de identificar se o nível de criticidade do risco é aceitável ou não tolerável, conforme o apetite a riscos, definido no item 5.4 para a priorização e otimização das respostas ao risco.

### 6.4. Tratamento

Tratamento é o processo responsável em modificar o risco de modo a evitar, transferir, mitigar ou aceitar.

Os controles mitigatórios são medidas, processos ou ferramentas implementadas com objetivo de reduzir a probabilidade de um risco ocorrer ou minimizar o impacto negativo caso ele venha a se concretizar. Eles são etapas no processo, necessários quando um risco está acima do limite definido no apetite a risco, servindo como uma camada de proteção para manter o risco dentro de um nível aceitável.

Os controles podem ser:

- Controles Preventivos: Atuam na causa para evitar que o problema aconteça. Exemplo: Controle de autorização, como o uso de senhas fortes e autenticação em duas etapas para evitar acessos indevidos.
- Controles Detectivos: Identificam o problema logo após ele ocorrer, permitindo uma resposta rápida. Exemplo: Um sistema de monitoramento que dispara um alerta quando há uma tentativa de invasão.
- Controles Corretivos: Executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Focam em limitar o dano e restaurar a normalidade após o incidente. Exemplo: A existência de um backup atualizado para recuperar dados após um ataque de vírus.

### 6.5. Monitoramento

Etapa de verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. O monitoramento garante a efetividade da gestão de riscos, nessa etapa pode-se incluir, o acompanhamento de planos de tratamento, análise da evolução dos riscos, revisão periódica da matriz de riscos e avaliação da efetividade dos controles. O monitoramento, a depender da maturidade em gestão de riscos, deve ser feito por meio de KRI (Key Risk Indicator), ou seja, indicadores que servirão para monitorar e avaliar.

### 6.6. Comunicação

Etapa que fornece, compartilha ou obtêm informações relativas ao risco e ao seu tratamento com as partes interessadas, ou seja, todos aqueles que possam influenciar ou ser influenciados por esse risco, com vistas a prevenir sua materialização.

## • Como Fazer na prática

A presente Metodologia disponibiliza, em anexos, as ferramentas de apoio que podem ser utilizadas pelo analista setorial de risco desenvolver as atividades de gestão de riscos. Adicionalmente, a metodologia propõe modelos de indicadores de gestão de riscos para fins de monitoramento. Quaisquer dúvidas devem ser direcionadas à Assessoria Especial de Controle Interno do MPS.

### 7.1. Priorização dos processos de gestão de riscos

O processo de gestão de riscos é relativamente de fácil aplicação, contudo necessita ser aplicado com direcionamento. Dessa forma, disponibilizamos uma ferramenta, inspirada no Método de Priorização de Processos do Ministério do Planejamento de 2017, para que as unidades, gestores e analistas de risco estabeleçam quais os objetos prioritários para o gerenciamento dos riscos.

Os objetos são avaliados em 5 aspectos, e ponderados por pesos.

**Impacto na Estratégia - Peso 20%**

Nota 1 - O Objeto NÃO impacta os objetivos estratégicos, táticos ou operacionais.

Nota 2 - O Objeto tem pouco impacto, não impede o atingimento dos objetivos estratégicos, táticos ou operacionais.

Nota 3 - O Objeto tem grande impacto e pode impedir o atingimento dos objetivos estratégicos, táticos ou operacionais.

**Impacto no Orçamento - Peso 20%**

Nota 1 - O Objeto NÃO impacta o orçamento.

Nota 2 - O Objeto tem baixo impacto no orçamento.

Nota 3 - O Objeto tem grande impacto orçamentário.

**Avaliado por Órgãos de Controle - TCU ou CGU - Peso 20%**

Nota 1 - O Objeto foi objeto de análise e POSSUI recomendações.

Nota 2 - O Objeto foi objeto de análise, mas NÃO possui recomendações.

Nota 3 - O Objeto NÃO foi objeto de análise por órgãos de controle.

**Maturidade do Objeto - 10%**

Nota 1 - O Objeto POSSUI fluxos definidos E análise dos riscos e controles.

Nota 2 - O Objeto POSSUI fluxos definidos OU análise dos riscos e controles.

Nota 3 - O Objeto NÃO possui fluxos definidos, e NÃO possui análise de risco e controles.

**Reclamações Registradas na Ouvidoria - Peso 30%**

Nota 1 - Não Existe registro de reclamação registrada na Ouvidoria.

Nota 3 - Existe registro de reclamação registrada na Ouvidoria.

Após o registro de avaliação os objetos recebem uma nota, que por meio dela faz-se a classificação seguindo a orientação abaixo:

| Faixas de Classificação de Priorização de Objetos | |
|---|---|
| **P - Prioritário** | Resultado maior ou igual a 2,2 |
| **R - Relevante** | Resultado maior ou igual a 1,6 e menor que 2,2 |
| **M - Moderado** | Resultado menor que 1,6 |

A partir dessa classificação os gestores de riscos podem priorizar a avaliação dos objetos que possuírem maior nota, conforme orientação da AECI/MPS.

| Objetos | Avaliação | | | | | | |
|---|---|---|---|---|---|---|---|
| | Fatores de Análise dos Objetos | | | | | Nota | Classificação |
| | Impacto na Estratégia | Impacto no Orçamento | Avaliado por Órgãos de Controle - TCU ou CGU | Maturidade do Objeto | Reclamações Registradas na Ouvidoria | | |
| | 20% | 20% | 20% | 10% | 30% | 100% | |
| Objeto 1 | 2 | 2 | 2 | 2 | 3 | 2,3 | P |
| Objeto 2 | 2 | 2 | 1 | 2 | 3 | 2,1 | R |
| Objeto 3 | 1 | 2 | 1 | 2 | 1 | 1,3 | M |

Para objetos que estão ligados diretamente a implementação de políticas públicas, ou outro projeto estratégico, recomenda-se fazer a avaliação de riscos desses objetos, independente da avaliação acima.

## 7.2. Estabelecimento do Contexto

A análise de contexto refere-se ao levantamento e registro dos aspectos externos e internos, que compõem o ambiente onde o ministério está inserido, visando o atingimento dos seus objetivos, sejam eles estratégicos, táticos, ou operacionais, a depender em que nível organizacional a gestão de riscos esteja sendo realizada. A análise ambiental permite a compreensão clara do contexto do ministério, proporcionando uma visão abrangente dos fatores que podem influenciar sua capacidade em atingir os resultados planejados.

O ambiente interno envolve aspectos como governança, estrutura organizacional, funções, alçadas e responsabilidades, políticas, estratégias, capacidades, competência, sistemas de informação, processos decisórios, cultura organizacional.

O ambiente externo envolve aspectos como social, político, legal, regulatório, financeiro, tecnológico, econômico, ambiental, relações com partes interessadas externas e suas percepções e valores.

Para análise de contexto, destaca-se a tradicional ferramenta Análise SWOT (Strengths, Weaknesses, Opportunities, Threats), que auxilia a análise sobre os pontos fortes e fracos do ambiente interno e as oportunidades e ameaças do ambiente externo. Os insumos para a estruturação da Análise SWOT podem ser levantados por meio da utilização de uma tempestade de ideias (Brainstorming) – técnica para compartilhamento espontâneo de ideias – que poderá ser realizada em sessões de oficinas com a equipe responsável pelo processo de trabalho, sendo importante especificar o seu objetivo, a fim de identificar os fatores internos e externos que apoiam ou dificultam o seu alcance.


Fonte: Curso ENAP-Implementando a Gestão de riscos no setor público

### 7.2.1.Análise interna

A análise interna é o reflexo das forças e fraquezas, são aspectos pelos quais o ministério é responsável pelo seu aparecimento, assim ele o poder de agir, bem como o controle de mudanças.

Desta forma, todos os fatores sobre os quais há possibilidade de intervir são parte do ambiente interno; como seus colaboradores, maquinário, políticas internas, tecnologias empregadas, softwares e sistemas de gestão, frotas de veículos, rede de unidades descentralizadas, capacidade de investimento etc.

- Strengths (forças) - As forças são os **pontos positivos** da organização, as vantagens que ela possui em comparação às outras instituições. Isso pode ser identificado, principalmente, na análise dos diferenciais oferecidos, seja pela qualidade do atendimento, pelo desempenho das estratégias, das finanças e orçamento, da agilidade na prestação de serviços.
- Weaknesses (fraquezas) – Com certeza que uma organização também tenha fraquezas, pontos fracos que podem ser controlados internamente.

### 7.2.2. Análise externa

A análise externa envolve a identificação das oportunidades e ameaças no setor em que a instituição está inserida.

- Opportunities (oportunidades) - As oportunidades são fontes externas que podem influenciar positivamente a sua organização, mas que não podem ser controladas. As oportunidades são ocasiões que a organização tem para se desenvolver e atingir suas estratégias.
- Threats (ameaças) – As ameaça são todas as forças externas, e que também não se pode controlar, mas que impactam negativamente na organização.

O estabelecimento do contexto é uma precondição à identificação de riscos, à análise e avaliação e ao tratamento de riscos. Basicamente, é uma etapa/fase de definição da estratégia de gestão de riscos que se concretiza com a definição de diversos elementos, tais como:

- definição de parâmetros internos e externos;
- equipe responsável;
- metodologias e normas específicas a serem utilizadas;
- ferramentas, relatórios, modelos e formulários a serem utilizados;
- tolerância ao risco;
- escopo de aplicação, acompanhamento e monitoramento.

Caso seja necessário, consta no Anexo III, formulário para produção e documentação dos dados levantados na análise ambiental.

## 7.3. Identificação dos Riscos

O processo de identificar um risco inclui, segundo a ISO 31.000, "a identificação das causas e fontes do risco, eventos, situações ou circunstâncias que poderiam ter um impacto material sobre os objetivos com o propósito de identificar o que poderia acontecer ou quais situações poderiam existir que poderiam afetar o alcance dos objetivos da Instituição".

A identificação de riscos é a etapa de maior relevância na gestão de riscos corporativos, pois envolve o reconhecimento, descrição e registro dos possíveis eventos de risco, com a identificação dos seus fatores (causas e fontes), e impactos e consequências (efeitos).

Como orientação, utilizamos a definição dos conceitos, extraídos e compilados das normas: ABNT ISO 31000:2018 e a ABNT ISO/IEC Guia 73, os quais devem nortear a atuação do responsável pela identificação e avaliação dos riscos.

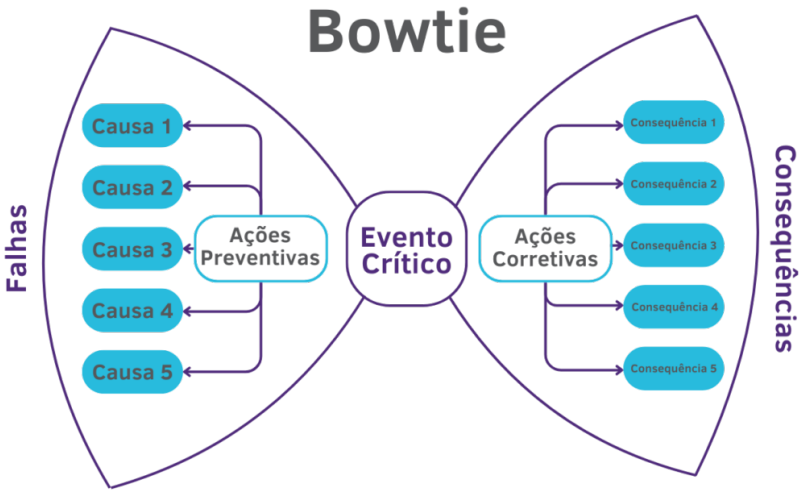
a) **Evento de Riscos** - Um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a implementação da estratégia e a realização de objetivos de modo negativo, positivo ou ambos.

*b)* **Causa Geradora** - Busca evidenciar o estado ou condição no processo que está levando a materialização do risco. Geralmente evidenciada por adjetivos negativos como: Falta, Ausência, Insuficiente, Inadequado, Ineficiente, Deficiente, Impreciso, Incorreto, entre outros. Por exemplo: *quantidade insuficiente de servidores; sistema ineficiente; processos inadequados.*

**Fonte de risco**- Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco. Por exemplo:

- Pessoas - Relacionam-se à competência, conduta ética e desempenho das suas atribuições;
- Processos - Fluxos e etapas do desenvolvimento de produtos e serviços e condução de atividades da organização, definição dos normativos internos e aderência à legislação;
- Sistemas - Infraestrutura e arquitetura de TI, disponibilidade de armazenamento, processamento e rede;
- Eventos Externos - Relacionados com as ocorrências do meio ambiente, do ambiente social e do ambiente regulatório do país.

c) **Consequência ou Impacto** - Efeito resultante da ocorrência do evento de risco.




Para favorecer a identificação de eventos de riscos utilizando as técnicas e ferramentas propomos a utilização das perguntas orientadoras abaixo, as quais permitem obter as informações necessárias para se construir o Plano de Respostas aos Riscos.

Para saber se foi feita uma identificação alinhada com a realidade do objeto avaliado, aplica-se a seguinte expressão de racionalidade:

**Devido a <CAUSAS/FONTES>, poderá acontecer <EVENTO DE RISCO>,**

**o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA/EFEITO>**

**impactando no/na <DIMENSÃO DE OBJETIVO> >>IMPACTADA>.**

Adaptado TCU, 2013

### 7.3.1. Insumos e Ferramentas

Para ser realizada a identificação de riscos, recomenda-se a utilização de ferramentas e direcionadores abaixo, ficando o analista setorial de risco responsável em identificar a melhor ferramenta que atenda suas necessidades.

- Brainstorming/entrevistas com especialistas (Anexo IV);
- Análise do fluxo de processos;
- Bow Tie
- Análise de incidentes históricos.

**IDENTIFICAÇÃO DE RISCOS**

**Análise dos Riscos Mapeados**

Devido a <**CAUSA/FONTE**>,
poderá acontecer <**EVENTO DE RISCO**>,
o que poderá levar a <**EFEITO/CONSEQUÊNCIAS**>
impactando no/na <**OBJETIVO/ENTREGA DO PROJETO**>

| CAUSA | | | EVENTO DE RISCO | | CONSEQUÊNCIA | |
|---|---|---|---|---|---|---|
| FONTE | CAUSA GERADORA | CONTROLE PREVENTIVO | CATEGORIA | DESCRIÇÃO | CONTROLE DETECTIVO/ CORRETIVO | IMPACTO |
| Fonte 1 | Causa 1 - Risco 1 | | Estratégico | Evento de Risco Identificado 1 | | Impacto 1 - Risco 1 |
| Fonte 2 | Causa 2 - Risco 1 | | | | | Impacto 2 - Risco 1 |
| Fonte 3 | Causa 3 - Risco 1 | | | | | Impacto 3 - Risco 1 |
| Fonte 4 | Causa 4 - Risco 1 | | | | | Impacto 4 - Risco 1 |
| Fonte 1 | Causa 1 - Risco 2 | | Operacional | Evento de Risco Identificado 2 | | Impacto 1 - Risco 2 |
| Fonte 2 | Causa 2 - Risco 2 | | | | | Impacto 2 - Risco 2 |
| Fonte 3 | Causa 3 - Risco 2 | | | | | Impacto 3 - Risco 2 |
| Fonte 4 | Causa 4 - Risco 2 | | | | | Impacto 4 - Risco 2 |
| Fonte 1 | Causa 1 - Risco 3 | | Imagem ou Reputação | Evento de Risco Identificado 3 | | Impacto 1 - Risco 3 |
| Fonte 2 | Causa 2 - Risco 3 | | | | | Impacto 2 - Risco 3 |
| Fonte 3 | Causa 3 - Risco 3 | | | | | Impacto 3 - Risco 3 |
| Fonte 4 | Causa 4 - Risco 3 | | | | | Impacto 4 - Risco 3 |
| Fonte 1 | Causa 1 - Risco 4 | | Legal ou Conformidade | Evento de Risco Identificado 4 | | Impacto 1 - Risco 4 |
| Fonte 2 | Causa 2 - Risco 4 | | | | | Impacto 2 - Risco 4 |
| Fonte 3 | Causa 3 - Risco 4 | | | | | Impacto 3 - Risco 4 |
| Fonte 4 | Causa 4 - Risco 4 | | | | | Impacto 4 - Risco 4 |
| Fonte 1 | Causa 1 - Risco 5 | | Financeiro/Orçamentário | Evento de Risco Identificado 5 | | Impacto 1 - Risco 5 |
| Fonte 2 | Causa 2 - Risco 5 | | | | | Impacto 2 - Risco 5 |
| Fonte 3 | Causa 3 - Risco 5 | | | | | Impacto 3 - Risco 5 |
| Fonte 4 | Causa 4 - Risco 5 | | | | | Impacto 4 - Risco 5 |
| Fonte 1 | Causa 1 - Risco 6 | | Integridade | Evento de Risco Identificado 6 | | Impacto 1 - Risco 6 |
| Fonte 2 | Causa 2 - Risco 6 | | | | | Impacto 2 - Risco 6 |
| Fonte 3 | Causa 3 - Risco 6 | | | | | Impacto 3 - Risco 6 |
| Fonte 4 | Causa 4 - Risco 6 | | | | | Impacto 4 - Risco 6 |

## 7.4. Análise

### 7.4.1.Probabilidade

Probabilidade refere-se à possibilidade de um risco se materializar. A avaliação da probabilidade deve considerar o conhecimento técnico e as experiências adquiridas pelos especialistas, levando em consideração,

critérios qualitativos e/ou sempre que viável, fatores como a frequência observada, histórica ou projetada dos riscos e de suas origens.

| Escala de Probabilidade | | |
|---|---|---|
| **Probabilidade** | **Descrição** | **Peso** |
| Muito baixa | Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade. **<10%** | 1 |
| Baixa | Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. **> = 10% e < = 30%** | 2 |
| Média | Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. **> = 30% e < = 50%** | 3 |
| Alta | Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. **> = 50% e < =90%** | 4 |
| Muito alta | Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade. **> 90%** | 5 |

### 7.4.2. Impacto

A consequência, se um risco se concretizar, está ligada às implicações que isso pode gerar em áreas significativas. Assim, será analisado de acordo com as repercussões em setores determinados, como perda de recursos ou baixa eficiência do procedimento, violação de normas legais, prejuízos financeiros e danos à reputação.

| Escala de Impacto | | |
|---|---|---|
| **Impacto** | **Descrição** | **Peso** |
| Muito baixo | Mínimo impacto nos objetivos. | 1 |
| Baixo | Pequeno impacto nos objetivos. | 2 |

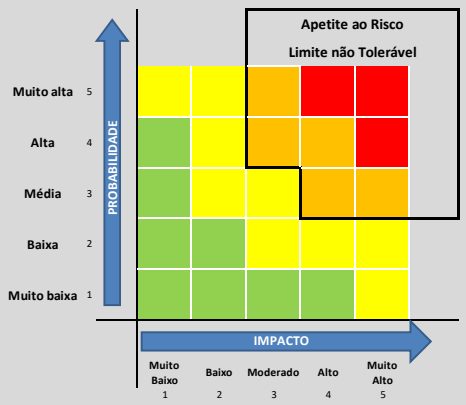
| | | |
|---|---|---|
| Moderado | Moderado impacto nos objetivos, de fácil recuperação ou de baixo custo, pode ser gerenciado em circunstâncias normais. | 3 |
| Alto | Significativo impacto nos objetivos, de moderada recuperação ou com moderado custo, com a devida gestão pode ser suportado. | 4 |
| Muito alto | Catastrófico impacto nos objetivos, de complexa recuperação com alto custo, com potencial para levar o negócio/serviço ao colapso. | 5 |

## 7.5. Avaliação

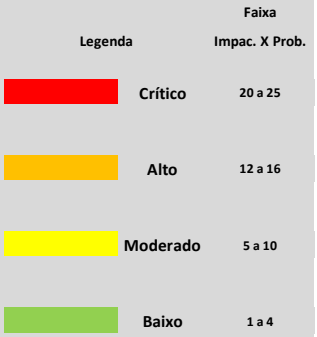
A avaliação de riscos envolve a comparação dos resultados da análise de riscos com o apetite a riscos estabelecido para a organização, a fim de determinar se eles são aceitáveis, qual sua priorização e auxiliar na decisão sobre o tratamento a ser adotado. O resultado da criticidade é obtido pela multiplicação dos pesos, probabilidade x impacto.

| Classificação da Criticidade do Risco | |
|---|---|
| **Classificação** | **Peso** |
| Baixo | 1 a 4 |
| Moderado | 5 a 10 |
| Alto | 12 a 16 |
| Crítico | 20 a 25 |

**Matriz de Probabilidade x Impacto**




**Nível de Criticidade do Risco**



O Cálculo do nível de risco deve ser realizado pensado em dois cenários distintos:

**1. Risco inerente** – A equipe técnica deve imaginar o processo em questão sem nenhum mecanismo de controle implementado.

**2. Risco residual** – A equipe técnica deve imaginar o processo em questão com os atuais mecanismos de controle implementados.

A diferença entre o valor do risco inerente e o risco residual demonstrará a atual eficácia dos controles implementados na mitigação dos riscos identificados. Essa informação auxiliará a etapa "Avaliação dos Controles Processuais" na identificação de melhorias possíveis nos controles atuais.

### 7.6. Priorização e Tratamento

Nesta etapa, devem ser considerados os valores dos níveis de riscos calculados na etapa anterior para a priorização e otimização das respostas. A faixa de classificação do risco deve ser considerada para a definição da atitude da unidade em relação à priorização para tratamento. A seguir orientamos as possíveis respostas e tratamento, quais ações devem ser adotadas em relação ao risco residual.

| Tratamento | Descrição |
|---|---|
| Evitar | Implica em descontinuar as atividades ou processos que geram esses riscos. Evitar sugere que nenhuma das demais opções de resposta tenham sido identificada seja capaz de reduzir o impacto e a probabilidade do risco a um nível aceitável. |
| Compartilhar<br>Transferir | Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco, como a terceirização de uma atividade ou a contratação de seguros. |
| Mitigar | São adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou mesmo ambos. Para a CGU, mitigar o risco significa implementar controles, de acordo com a avaliação do custo x benefício. |
| Aceitar | Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos. Aceitar indica que o risco já esteja dentro do apetite a riscos, contudo deve ser monitorado para garantir que permaneça nos níveis aceitáveis. |

Considerando que os riscos Baixo e Moderado estão dentro dos limites aceitáveis de apetite do MPS, não há que ser tomar atitudes adicionais além de monitoramento, a fim de evitar seu agravamento.

Para os demais riscos, altos e críticos, serão necessárias ações adicionais ao monitoramento, a exemplo de mitigar ou compartilhar/transferir, a depender da avaliação do gestor dos riscos, sob assessoramento da AECI.

Caso a opção seja mitigar o risco, orienta-se implementar controles previstos no item 6.5, sejam preventivos, detectivos ou corretivos, isolada ou cumulativamente, podendo também avaliar outras medidas para correção, levando-se em conta a capacidade operacional e custo-benefício, a exemplo de aplicação de novos sistemas, ou a inovação do processo.

Com finalidade de auxiliar e dar suporte na definição dos controles utilize os dados registrados no Bow-Tie, disponibilizado no Anexo V.

**Plano de Gestão de Riscos**
**Ações de Mitigação e Monitoramento**

| Porque? | | | O que? | Onde? | Quem? | | Como? | Quando? | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ID. | Evento de Risco | Fator de Risco | Descrição da Ação | Área Responsável pela Implementação | Responsável Implementação | Intervenientes | Como será Implementado | Data do Início | Data da Conclusão | Status |
| 1 | Evento de Risco Identificado 1 | Causa 1 - Risco 1 | | | | | | | | Atrasado |
| | | Causa 2 - Risco 1 | | | | | | | | Concluído |
| | | Causa 3 - Risco 1 | | | | | | | | Em andamento |
| | | Causa 4 - Risco 1 | | | | | | | | Concluído |
| 2 | Evento de Risco Identificado 2 | Causa 1 - Risco 2 | | | | | | | | Não Iniciado |
| | | Causa 2 - Risco 2 | | | | | | | | Concluído |
| | | Causa 3 - Risco 2 | | | | | | | | Concluído |
| | | Causa 4 - Risco 2 | | | | | | | | Concluído |

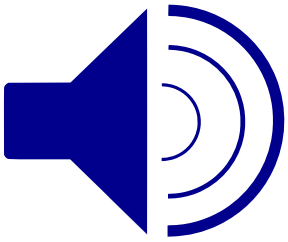
## 7.7. Monitoramento

O modelo orientado é estruturado em KRI (Key Risk Indicators), vinculado à Taxonomia de Riscos do MPS, a fim de proporcionar a estruturação de dados institucionais, implementação de plataforma de Governança, Riscos e Compliance - GRC e painéis analíticos.

No Anexo II, disponibilizamos propostas de indicadores de monitoramento por categoria de riscos, ficando a opção de sua aplicação sob responsabilidade

do gestor do risco, com auxílio do analista setorial de risco e assessoria da AECI.

### 7.8. Comunicação e Reporte



O processo de comunicação e reporte iniciará com às partes interessadas sobre os pontos relevantes do processo de gestão de riscos realizado. A AECI, posteriormente reportará ao Comitê Estratégico de Governança.

A comunicação de riscos deve assegurar transparência e compartilhamento de informações relevantes entre as instâncias de governança.

Relatórios institucionais de riscos:

- Relatório de riscos;
- Painel institucional de riscos;

## • Particularidades

### 8.1. Riscos da Estratégia

A gestão de riscos da estratégia tem por finalidade apoiar a alta administração na identificação de riscos que possam comprometer o alcance dos objetivos estratégicos da organização.

Esses riscos geralmente estão associados a fatores externos e a mudanças no ambiente institucional.

#### 8.1.1. Premissas em políticas públicas

Premissas são as condições consideradas verdadeiras quando uma política pública ou estratégia é formulada. O risco da estratégia surge quando uma premissa deixa de ser válida.

- desenho da política;
- escala de atuação;
- modelo de governança;
- alocação orçamentária;
- indicadores de sucesso.

**Exemplo:**

Uma política pública é desenhada com a premissa de que:
"Haverá cooperação permanente dos municípios."
Se essa premissa falhar:

- a política não escala;
- metas não são atingidas;
- surgem riscos de inefetividade e desperdício.

### 8.1.2. Identificação de eventos de risco da estratégia

- Quais eventos ou condições incertas que podem impedir o órgão ou entidade de cumprir sua missão institucional, executar políticas públicas ou alcançar seus objetivos estratégicos?

### 8.1.3. Identificação das causas - Análise PESTEL

- **Político:** ciclos eleitorais, governabilidade, alinhamento entre entes
    - O que está mudando fora do ministério que pode afetar nossa estratégia atual?
    - Como nossas decisões estratégicas podem ser percebidas pelos stakeholders?
- **Econômico:** restrições fiscais, dívida pública
    - A estratégia é financiável ao longo do tempo?
- **Social:** demandas sociais crescentes, desigualdades
    - O que pode gerar perda de efetividade das políticas públicas?
- **Tecnológico:** transformação digital, proteção de dados
    - Temos capacidade real de executar o que foi planejado?
- **Ambiental:** eventos climáticos, sustentabilidade
    - Quais eventos podem afetar a implementação das políticas públicas?
- **Legal:** novos marcos legais, judicialização
    - Existe risco de a estratégia se tornar inviável juridicamente?
    - Nossa estratégia parte de premissas válidas e atualizadas?

### 8.1.4. Avaliação dos riscos

Os riscos são avaliados considerando probabilidade e impacto sobre os objetivos estratégicos.

### 8.1.5. Consequências do evento de risco

- Entrega de valor público;
- Continuidade de serviços essenciais;
- Aderência ao mandato legal e às prioridades de governo;
- Interrupção de serviços essenciais;
- Perda de recursos já investidos;
- Frustração da sociedade;
- Risco elevado à imagem institucional;
- Potenciais questionamentos do controle externo.

### 8.1.6. Controles e Monitoramento

Faz-se o controle de riscos da estratégia para que Administração Pública proteja com razoável segurança sua missão institucional, garantir a efetividade das políticas públicas e dar racionalidade às decisões da alta gestão em ambientes de incerteza.

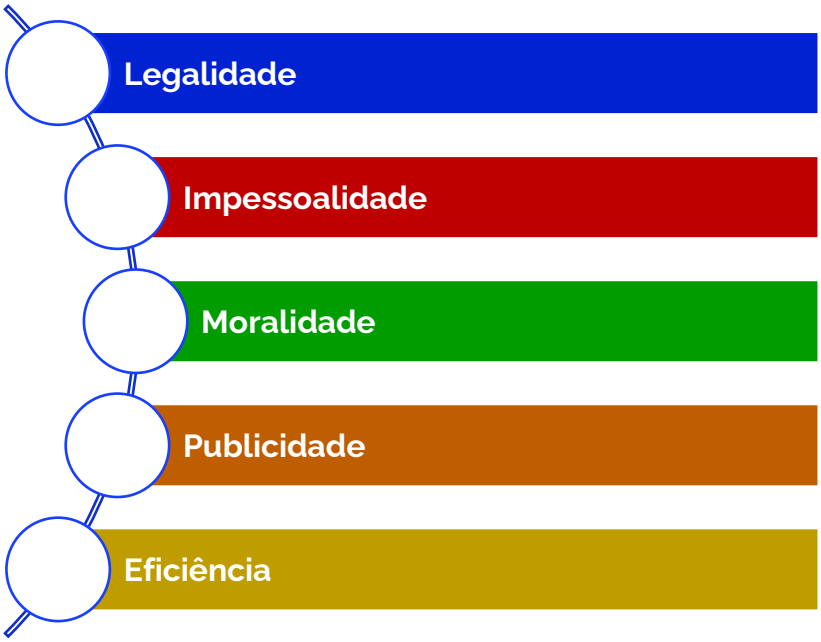
Avaliar se os riscos de estratégia estão adequadamente tratados por mecanismos de governança.

- Direção e Liderança (Tone at the top) - Avalia se a alta administração assume e direciona o risco da estratégia.
- Institucionalização da Estratégia - Avalia se a estratégia sobrevive a mudanças de pessoas e contextos políticos.
- Governança e Papéis Institucionais - Avalia se há arranjos claros de governança.
- Monitoramento e Desempenho Estratégico - Avalia se a gestão acompanha resultados, não só atividades.
- Análise e Revisão de Premissas - Avalia se a estratégia é adaptável à realidade.
- Sustentabilidade Orçamentária - Avalia se a estratégia é financeiramente viável ao longo do tempo.
- Capacidade Estatal - Avalia se a organização tem meios reais de executar a estratégia.
- Transparência e Accountabiity - Avalia riscos de reputação, legitimidade e controle social.

## 8.2. Riscos a Integridade

Consideramos que riscos a integridade são situações ou fatores que podem favorecer desvios de conduta, como corrupção, fraude, abuso de poder ou outras práticas que ferem os princípios da administração pública. Eles afetam diretamente a confiança da sociedade, a qualidade dos serviços públicos e a legalidade dos atos administrativos.

Riscos à integridade são possibilidades de ocorrência de atos que violem valores éticos, legais e institucionais, especialmente:




Eles não significam que o problema já ocorreu, mas que existem vulnerabilidades que aumentam a chance de ocorrer.

Embora os riscos existam em toda a administração, algumas áreas são mais vulneráveis:

- Licitações e contratos;
- Compras e aquisições;
- Concessão de benefícios, licenças e autorizações;
- Fiscalização e regulação;
- Gestão de pessoas (nomeações, cargos de confiança);
- Transferências de recursos e convênios.

A identificação dos riscos à integridade deverá considerar, entre outros aspectos:

I. exposição à interação com agentes privados;
II. grau de discricionariedade decisória;
III. acesso a informações sensíveis ou dados pessoais;
IV. histórico de irregularidades;
V. achados de auditorias e recomendações de órgãos de controle.

O tratamento dos riscos à integridade poderá envolver:

I. aprimoramento normativo e procedimental;
II. segregação de funções e fortalecimento de controles;
III. ações de capacitação e comunicação;
IV. adoção de controles tecnológicos.

### 8.3. Riscos em Contratações Públicas

A gestão de riscos nas contratações públicas visa garantir maior transparência, integridade e eficiência no uso dos recursos públicos. Aplicável ao ciclo completo de contratação pública.

Etapas analisadas:

- Planejamento da contratação;
- Seleção do fornecedor;
- Gestão do contrato.

A análise pode ocorrer em três níveis:

- Macroprocesso de contratação - Essa abordagem analisa o sistema de governança das contratações como um todo. São avaliados:
    - planejamento das contratações
    - estrutura organizacional
    - capacitação dos agentes públicos
    - instrumentos de governança.
- Processos organizacionais de contratação - Nesta etapa são avaliados os riscos associados às diferentes fases do ciclo de contratação:
    - planejamento;
    - seleção do fornecedor;
    - gestão do contrato.

- Processos específicos de contratação

Quando necessário, poderá ser realizada análise de processo de contratação específico, a critério da Secretaria-Executiva ou do Gabinete do Ministro. A demanda poderá ser encaminhada à AECI para análise, com o apoio técnico das unidades responsáveis pela contratação. Nesses casos, deverá ser observada a capacidade operacional da AECI, de modo a não comprometer a execução das atividades ordinárias e a qualidade dos trabalhos desempenhados. Assim, as contratações específicas deverão ser caracterizadas como relevantes sob, ao menos, um dos seguintes aspectos:

1. valor da contratação – contratações de alto vulto; e
2. relevância estratégica para o MPS ou unidades vinculadas.

## • Conclusão

A implementação de uma metodologia integrada de gestão de riscos representa avanço significativo para o fortalecimento da governança no Ministério da Previdência Social.

Ao integrar diferentes abordagens de gestão de riscos — da estratégia, operacionais, de integridade, de processos, de políticas públicas e de contratações — o Ministério estabelece bases sólidas para aprimorar sua capacidade de decisão, prevenir falhas institucionais e ampliar a geração de valor público.

Essa abordagem contribui para:

- maior racionalidade na tomada de decisões;
- melhor utilização dos recursos públicos;
- fortalecimento da integridade institucional;
- melhoria contínua das políticas públicas previdenciárias.

## Referências

Associação Brasileira de Normas Técnicas. (2018). ABNT NBR ISO 31000:2018. *Gestão de riscos — Diretrizes*. Rio de Janeiro, RJ, Brasil: Associação Brasileira de Normas Técnicas.

Associação Brasileira de Normas Técnicas. (2021). ABNT NBR IEC 31010:2021. *Gestão de riscos — Técnicas para o processo de avaliação de riscos*. Rio de Janeiro, RJ, Brasil: Associação Brasileira de Normas Técnicas.

Associação Brasileira de Normas Técnicas. (2022). ABNT NBR ISO 31073:2022. *Gestão de riscos — Vocabulário*. Rio de Janeiro, RJ, Brasil: Associação Brasileira de Normas Técnicas.

Controladoria-Geral da União. (2018). *Metodologia de Gestão de Riscos.* Fonte: Governança - Gestão de Riscos: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf

Ministério da Fazenda. (s.d.). *Guia Referencial de Gestão Integral de Riscos.* Fonte: Gestão de Riscos: https://www.gov.br/fazenda/pt-br/assuntos/gestao-de-riscos/documentos/cgrci-guia-referencial-de-gestao-integral-de-riscos-versao-1.pdf

Ministério da Gestão e da Inovação em Serviços Públicos. (s.d.). *Guia de Gestão de Riscos do MGI.* Fonte: Comitê de Integridade, Transparência, Acesso à Informação, Riscos e Controle | CITARC: https://www.gov.br/gestao/pt-br/acesso-a-informacao/estrategia-e-governanca/estrutura-de-governanca/citarc/guia_gr_mgi.pdf

Ministério da Previdência Social. (Abril de 2026). *Governança - Integridade.* Fonte: Guia de Prevenção e Enfrentamento a Assédios e Discriminação: https://www.gov.br/previdencia/pt-br/acesso-a-informacao/governanca/integridade/guia-de-prevencao-e-enfrentamento-a-assedios-e-discriminacao/guia-de-prevencao-enfrentamento-assedio_mps_online.pdf

Ministério das Cidades. (2025). *Metodologia de Gestão de Riscos e Controles Internos aplicada às Contratações Públicas.* Fonte: Governança - Gestão de Riscos e Controles Internos: https://www.cidades.gov.br/images/stories/ArquivosCidades/ArquivosPDF/Metodologia_de_Gesto_de_Riscos_e_Controles_Internos_aplicada_s_Contrataes_Pblicas.pdf

Ministério das Cidades. (2025). *Metodologia de Gestão de Riscos e Controles Internos aplicada às Políticas Públicas.* Fonte: Governança - Gestão de Riscos e Controles Internos: https://www.gov.br/cidades/pt-br/acesso-a-informacao/acoes-e-programas/governanca/gestao-de-riscos-e-controles-internos/arquivos/METODOLOGIAAPLICADASPOLTICASPBLICAS.pdf

Ministério das Cidades. (2025). *Metodologia de Gestão de Riscos e Controles Internos de Processos Organizacionais.* Fonte: Governança - Gestão de Riscos e Controles Internos: https://www.gov.br/cidades/pt-br/acesso-a-informacao/acoes-e-programas/governanca/gestao-de-riscos-e-controles-internos/arquivos/METODOLOGIA_DE_GESTAO_DE_RISCOS_DE_PROCESSOS_ORGANIZACIONAIS___3__EDICAO___2025___ATUALIZADO_EM_17.01.pdf

Presidência da República. (s.d.). *Decreto nº 9.203, de 22 de novembro de 2017*. Brasília, DF.

Presidência da República/Controladora Geral da União. (10 de maio de 2016). *Instrução Normativa Conjunta MP/CGU nº 1.* Fonte: Diário Oficial de União - Imprensa Nacional: https://www.in.gov.br/web/dou/-/instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197

Tribunal de Contas da União. (2020). *Referencial Básico de Governança Organizacional 3ª Edição.* Fonte: Governança: https://portal.tcu.gov.br/data/files/FB/B6/FB/85/1CD4671023455957E18818A8/Referencial_basico_governanca_organizacional_3_edicao.pdf

ANEXO I - Taxonomia de Riscos

1. **Riscos da Estratégia - Risco relacionado a eventos que podem comprometer o alcance da missão institucional, dos objetivos estratégicos ou da efetividade das políticas públicas.**

1.1. Mudanças no ambiente

- Interrupção de políticas públicas prioritárias
- Falta de coordenação interinstitucional
- Mudança abrupta no cenário macroeconômico
- Perda de legitimidade institucional
- Dependência excessiva de atores externos

1.2. Tomada de decisões estratégicas inadequadas

- Falha na definição da estratégia institucional
- Falta de priorização de iniciativas estratégicas
- Análise inadequada de riscos

1.3. Execução da estratégia

- Desalinhamento entre planejamento estratégico e execução
- Falha na implementação de políticas públicas
- Planejamento estratégico desatualizado
- Inconsistência entre objetivos estratégicos e recursos disponíveis
- Inadequada gestão de portfólio de programas
- Falha na comunicação da estratégia institucional

2. **Riscos Operacionais - Risco decorrente de falhas em processos internos, pessoas, sistemas ou eventos externos, que podem comprometer a eficiência das operações.**

2.1. Riscos em Processos - Risco relacionado a falhas na execução dos processos internos.

- Falhas em processos organizacionais
- Ausência de padronização de processos
- Dependência excessiva de conhecimento individual
- Erros operacionais humanos
- Falhas de supervisão
- Interrupção de atividades críticas
- Falha na gestão de documentos
- Falta de segregação de funções
- Sobrecarga operacional de servidores
- Falta de controle sobre atividades terceirizadas

- Ineficiência na execução de processos
- Falha na continuidade de serviços
- Falha no controle de prazos
- Falta de monitoramento de desempenho
- Inadequada gestão de rotinas administrativas

2.2. Riscos Tecnológicos e de Informação - Risco relacionado a falhas em sistemas de informação, infraestrutura tecnológica ou segurança da informação, podendo comprometer dados e serviços digitais.

- Falhas em sistemas de informação
- Indisponibilidade de sistemas críticos
- Ataques cibernéticos
- Vazamento de dados sensíveis
- Perda de dados institucionais
- Falhas em backups
- Obsolescência tecnológica
- Falhas na gestão de acessos
- Uso indevido de sistemas
- Inconsistência em bases de dados
- Dependência de sistemas legados
- Falta de governança de TI
- Falha em projetos de tecnologia
- Interrupção de infraestrutura tecnológica
- Falhas de integração entre sistemas

2.3. Riscos Externos e Ambientais - Risco decorrente de fatores externos fora do controle direto da organização, capazes de impactar a execução de políticas públicas ou serviços.

- Desastres naturais;
- Crises sanitárias;
- Crises econômicas;
- Crises sociais;
- Instabilidade política;
- Mudanças políticas que alterem prioridades institucionais;
- Mudanças legislativas inesperadas;
- Falhas em infraestrutura pública;
- Interrupção de serviços essenciais;
- Dependência de fornecedores críticos;
- Crises internacionais;
- Mudanças tecnológicas disruptivas;
- Falhas em cadeias de suprimentos;

- Pandemias;
- Eventos climáticos extremos;
- Mudanças demográficas.

3. **Riscos Financeiros e Orçamentários - Risco relacionado à gestão inadequada de recursos financeiros e orçamentários, podendo gerar perdas, desperdícios ou irregularidades.**

3.1. Riscos ligados à fase de planejamento, estimativa e à autorização legal para gastar. Eles afetam a capacidade da organização de cumprir suas metas programadas.

- Execução inadequada do orçamento;
- Falhas na previsão orçamentária;
- Inexecução orçamentária;
- Contingenciamento inesperado de recursos.
- Falta de transparência orçamentária;
- Dependência excessiva de transferências externas.

3.2. Riscos dizem respeito à movimentação real de caixa, ao controle das saídas de dinheiro, à contabilidade e à prestação de contas.

- Pagamentos indevidos;
- Baixa eficiência na aplicação de recursos;
- Falhas no controle de despesas;
- Falhas em prestações de contas;
- Inconsistência em registros contábeis;
- Falha na gestão de convênios.

4. **Riscos de Integridade - Quaisquer vulnerabilidades de um indivíduo, de uma instituição ou de um processo de trabalho que aumente a probabilidade de ocorrência de comportamentos que possam ter efeitos negativos no desenvolvimento de uma cultura de integridade. (CGU)**

4.1. Abuso de posição ou poder em favor de interesses privados

- concessão de cargos ou vantagens em troca de apoio ou auxílio;
- esquivar-se do cumprimento de obrigações;
- falsificação de informação para interesses privados; e
- outras formas de favorecimento – a outros ou a si mesmo.

4.2. Nepotismo

- contratação de familiares para cargos em comissão e função de confiança;

- contratação de familiares para vagas de estágio e de atendimento a necessidade temporária de excepcional interesse público;
- contratação de pessoa jurídica de familiar por agente público responsável por licitação;
- contratação de familiares para prestação de serviços terceirizados;
- nomeações, contratações não previstas expressamente no decreto.

4.3. Conflitos de interesses

- uso de informação privilegiada;
- relação de negócio com pessoa física ou jurídica que tenha interesse em decisão;
- atividade privada incompatível com o cargo;
- atuar como intermediário junto à administração;
- praticar ato em benefício de pessoa jurídica (em que participe o servidor ou parente);
- receber presente de quem tenha interesse em decisão;
- prestar serviços a pessoa jurídica sob regulação do órgão.

4.4. Pressão interna ou externa para influenciar atos ilegais ou antiéticos de agentes públicos

- influência sobre funcionários subordinados para violar sua conduta devida;
- ações de retaliação contra possíveis denunciantes.
- lobby realizado fora dos limites legais ou de forma antiética;
- pressões relacionadas a tráfico de influência.

4.5. Solicitação ou recebimento de vantagem indevida

- qualquer tipo de enriquecimento ilícito;
- solicitação ou recebimento de propina;
- cobrança de vantagem indevida

4.6. Utilização de recursos públicos em favor de interesses privados

- apropriação indevida;
- irregularidades em contratações públicas; e
- outras formas de utilização de recursos públicos para uso privado (ex: carros, tempo de trabalho, equipamentos do escritório, etc.).

4.7. Assédio Moral

- humilhar, ridicularizar ou constranger a pessoa, publicamente ou em particular;

- desqualificar de forma reiterada o trabalho, a capacidade ou a competência profissional;
- impor metas ou prazos impossíveis, com a finalidade de constranger ou desestabilizar;
- retirar tarefas sem justificativa ou sobrecarregar injustificadamente;
- isolar, ignorar ou excluir deliberadamente a pessoa do convívio profissional;
- espalhar boatos, fofocas ou informações que atinjam a reputação;
- ameaçar, de forma velada ou explícita, a permanência no trabalho;
- tratar a pessoa com desprezo, hostilidade ou desrespeito constante.

4.8. Assédio Sexual

- Insinuações, comentários ou piadas de conotação sexual indesejadas;
- convites insistentes, mesmo após recusa;
- envio de mensagens, imagens ou conteúdos de natureza sexual;
- comentários sobre o corpo, a aparência ou a vida íntima;
- toques, aproximações físicas ou contatos sem consentimento;
- exposição de material pornográfico no ambiente de trabalho;
- promessas de vantagens ou ameaças relacionadas à aceitação de investidas sexuais.

4.9. Discriminação

- Racismo - tratamento desigual, estigmatização, piadas, exclusões ou desvalorização com base em raça ou cor;
- Gordofobia - comentários, piadas, estigmatização ou restrições associadas ao peso ou à aparência física;
- Machismo e sexismo - desqualificação, interrupções constantes, estereótipos de gênero ou limitação de oportunidades;
- LGBTQIA+fobia - constrangimentos, piadas, desrespeito à identidade ou orientação sexual;
- Capacitismo - barreiras, exclusões ou negação de adaptações razoáveis para pessoas com deficiência;
- Etarismo - preconceito ou discriminação em razão da idade, atingindo especialmente idosas.

**5. Riscos de Contratações Públicas - Risco relacionado a falhas nos processos de licitação, contratação e gestão de contratos, que podem resultar em prejuízos financeiros ou jurídicos.**

5.1. Riscos relacionados à etapa de Planejamento

- Planejamento inadequado de contratações
- Ausência/deficiência de Matriz de Riscos
- Editais com falhas técnicas
- Direcionamento de licitação
- Atraso em processos licitatórios
- Inadequada análise de preços
- Ausência de planejamento de compras

5.2. Riscos relacionados à etapa de Contratação

- Contratação de fornecedores inidôneos
- Restrição indevida à competitividade
- Dependência excessiva de fornecedores

5.3. Riscos relacionados à etapa de Gestão Contratual

- Interrupção no fornecimento de serviços, bens e materiais
- Falha na fiscalização de contratos
- Aditivos contratuais indevidos ou abusivos
- Entregas de baixa qualidade
- Descumprimento contratual
- Contratações emergenciais indevidas

**6. Riscos Jurídicos e Regulatórios – Conformidade - Risco decorrente do descumprimento de leis, regulamentos ou decisões judiciais, podendo gerar sanções, litígios ou responsabilização institucional.**

6.1. Riscos relacionados ao Ambiente Regulatório

- Decisões judiciais desfavoráveis
- Multas ou sanções regulatórias
- Insegurança jurídica
- Litígios institucionais
- Mudanças regulatórias inesperadas

6.2. Riscos relacionados ao processo de avaliação de decisões e sua execução

- Interpretação jurídica inadequada
- Normas internas inconsistentes
- Falta de conformidade regulatória
- Responsabilização administrativa
- Responsabilização civil
- Responsabilização penal

6.3. Riscos relacionados aos processos de gestão administrativa para aplicação das normas/leis

- Descumprimento de legislação
- Falhas na elaboração de normas
- Falha na gestão de processos judiciais
- Falhas na análise de contratos

**7. Riscos de Imagem e Reputação - Risco associado a eventos que possam comprometer a credibilidade, a confiança pública ou a reputação institucional.**

7.1. Riscos relacionados à percepção que a Sociedade possui do MPS

- Crise de imagem institucional
- Divulgação negativa na mídia
- Falha no atendimento ao cidadão
- Escândalos institucionais
- Perda de legitimidade social
- Baixa reputação institucional
- Repercussão negativa de decisões administrativas
- Falhas na gestão de crises

7.2. Riscos relacionados à percepção que APF e Órgãos de Controle Interno possuem do MPS

- Falta de transparência pública
- Comunicação institucional inadequada
- Informações públicas incorretas
- Desinformação institucional
- Críticas de órgãos de controle
- Falhas em prestação de contas públicas

ANEXO II - Indicadores

## Riscos da Estratégia

### Falha na execução do planejamento estratégico

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Percentual de metas não atingidas | metas não cumpridas / metas totais | >15% | >30% |
| Índice de execução do plano | ações executadas / ações previstas | <85% | <70% |
| Desvios estratégicos identificados | número de desvios relevantes | >5 | >10 |

### Mudanças políticas impactando programas

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Programas interrompidos | programas suspensos / total | >5% | >15% |
| Alterações orçamentárias extraordinárias | número de revisões | >2 | >4 |
| Rotatividade de dirigentes | trocas por ano | >3 | >5 |

## Riscos Orçamentários e Financeiros

### Execução orçamentária inadequada

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Percentual de execução orçamentária | valor executado / orçamento | <70% | <50% |
| Restos a pagar acumulados | valor restos / orçamento | >10% | >20% |
| Reprogramações orçamentárias | número anual | >3 | >6 |

Irregularidades financeiras

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Achados de auditoria financeira | ocorrências | >2 | >5 |
| Percentual de despesas glosadas | glosas / despesas | >3% | >7% |
| Desvios identificados | valor de desvios | >R$100k | >R$500k |

**Riscos de Contratações Públicas**

Falhas em licitações

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Licitações anuladas | licitações anuladas / total | >5% | >10% |
| Impugnações em editais | número de impugnações | >3 | >6 |
| Tempo médio de licitação | dias | >120 | >180 |

**Riscos Operacionais**

Falhas em processos administrativos

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Retrabalho processual | processos devolvidos / total | >8% | >15% |
| Tempo médio de tramitação | dias | >30 | >60 |
| Processos pendentes | estoque | >100 | >300 |

Indisponibilidade de sistemas

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Disponibilidade de sistemas | uptime % | <99% | <97% |
| Incidentes críticos | número | >2 | >5 |
| Tempo médio de recuperação | horas | >3 | >8 |

### Ataques cibernéticos

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Tentativas de intrusão | número | >100 | >500 |
| Vulnerabilidades críticas | número | >5 | >10 |
| Incidentes de segurança | número | >1 | >3 |

## Riscos de Integridade

### Fraudes administrativas

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Processos disciplinares | número | >3 | >6 |
| Denúncias recebidas | número | >5 | >10 |
| Investigações abertas | número | >2 | >5 |

### Conflito de interesses

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Declarações de conflito | número | >5 | >10 |

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Casos confirmados | número | >1 | >3 |
| Servidores em função sensível | percentual | >20% | >40% |

### Conluio em licitações

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Número de participantes por licitação | média | <3 | <2 |
| Concentração de vencedores | contratos por fornecedor | >40% | >60% |
| Denúncias registradas | número | >1 | >3 |

## Riscos Regulatórios e Legais

### Descumprimento de normas

| Indicador | Fórmula | Alerta | Crítico |
|---|---|---|---|
| Autos de infração | número | >2 | >5 |
| Não conformidades | número | >10 | >20 |
| Processos judiciais | número | >5 | >15 |

## ANEXO III – Análise Ambiental – Matriz SWOT

| | |
|---|---|
| Órgão/Unidade | |
| Diretoria/Secretaria | |
| Coordenação | |
| Objeto Avaliado | |
| Autor | |

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. O que você faz melhor que a média?

**Pontos Fracos**

Descreva suas principais deficiências. Pontos a serem melhorados ou revistos. Onde você perde para seus pares?

## ANÁLISE DO AMBIENTE EXTERNO

**Oportunidades**

Descreva as principais oportunidades identificadas. Eventos potenciais que podem gerar grandes benefícios, mudanças no mercado, novas tecnologias, mudanças na legislação ou falhas de um "concorrente" que você pode explorar.

**Ameaças**

Descreva as principais ameaças identificadas. Eventos potenciais que podem causar um grande estrago ao projeto ou entrega. Crises econômicas, novos parceiros agressivos, mudanças repentinas no comportamento do cidadão ou riscos cibernéticos.

## 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.

| Cruzamento | Objetivo Estratégico | Pergunta-chave |
|---|---|---|
| Forças + Oportunidades | Estratégia de Ofensiva | Como usar minhas forças para aproveitar essa oportunidade? |
| Forças + Ameaças | Estratégia de Confronto | Como minhas forças podem minimizar o impacto desta ameaça? |

| Cruzamento | Objetivo Estratégico | Pergunta-chave |
|---|---|---|
| Fraquezas + Oportunidades | Estratégia de Reforço | Como posso corrigir essa fraqueza para não perder a oportunidade? |
| Fraquezas + Ameaças | Estratégia de Defesa | Como reduzir as fraquezas para evitar que a ameaça me derrube? |

## ANEXO IV – Entrevista/Brainstorming

| | |
|---|---|
| Órgão/Unidade | |
| Diretoria/Secretaria | |
| Coordenação | |
| Objeto Avaliado | |
| Autor | |

A entrevista, diferente do brainstorming, é realizada com uma única pessoa, interna ou externa ao objeto avaliado, que seja experiente nas respectivas áreas de atuação (compras, contratos, TI, entre outros), stakeholders e especialistas no assunto a ser analisado.

A mesma estrutura da entrevista, os questionamentos feitos, também podem ser utilizados em um brainstorming, contudo essa abordagem é aplicada em um grupo, focado principalmente na multirreferencialidade, na busca da pluralidade de perspectivas.

Para que a entrevista tenha maior efetividade procure seguir as orientações:

| **PLANEJAMENTO** |
|---|

- Defina a pauta (objetivos e tópicos do projeto a serem analisados): Criar um modelo para a tabulação dos dados coletados, preferencialmente utilize a Planilha Documentadora - Objeto;
- Identificar os entrevistados e convocá-los com a pauta;
- Se prepare para a entrevista, obtenha informações do projeto e as entregas previstas. Para identificar riscos em um projeto sugerimos seguir as perguntas do Roteiro abaixo.

## REALIZAÇÃO

- Procure esclarecer o objetivo da entrevista, caso o entrevistado tenha alguma dúvida;
- Tabular os dados coletados, preferencialmente utilize a Planilha Documentadora - Objeto;
- Caso não haja objeção por parte do entrevistado, recomenda-se gravar a entrevista, pois pode ser utilizada para facilitar a tabulação dos dados levantados.

## ACOMPANHAMENTO

- Analise os dados coletados e tabulados na planilha;
- Verifique a aderência das informações coletadas com o objetivo proposto inicialmente.

## AÇÕES DE MITIGAÇÃO

Defina os possíveis mitigadores das ameaças. Busque adotar ações específicas para cada causa identificada, ou para a consequência/impacto registrado.

**Expressão da Racionalidade do Risco**

Devido a <CAUSAS/FONTES>, poderá acontecer <DESCRIÇÃO DA INCERTEZA (Evento de Risco)>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA/EFEITO> impactando no/na <DIMENSÃO DE OBJETIVO IMPACTADA>.

# Roteiro

**Identificação de eventos de risco**

- O que poderia dar errado?
- Quais eventos podem EVITAR, ATRASAR, PREJUDICAR ou IMPEDIR o atingimento de um ou mais objetivos?
- O que tem gerado ou pode gerar perda?
- Quais atividades são mais complexas?
- Em que gastamos mais dinheiro?
- Temos ativos que podem ser usados facilmente por terceiros?
- Quais recursos existem para nos proteger (físico, informação, humano)?
- Quais atividades são reguladas?

**Identificação das causas que levam ao risco**

- Como e por que ocorreu a falha?
- Existe falha humana?
- Fragilidades em sistemas favoreceram a ocorrência do evento de risco?
- Como é possível alguém interromper nossas operações?
- Como alguém pode nos fraudar ou roubar?
- Onde estamos vulneráveis?

**Consequências se ocorrer (materializar) o evento de risco**

- Quais as consequências caso ocorra o evento?

**Controles**

- Que ações podemos realizar para evitar?
- O que devemos fazer para sermos bem-sucedidos?
- Em quais informações temos maior confiança?

- Quais as decisões que requerem maior discernimento?

## ANEXO V – Bow – Tie

| | |
|---|---|
| Órgão/Unidade | |
| Diretoria/Secretaria | |
| Coordenação | |
| Objeto Avaliado | |
| Autor | |

A análise bow tie é uma maneira esquemática simples de descrever e analisar os caminhos de um risco desde as causas até as consequências. Pode ser considerada uma combinação do raciocínio de árvore de falhas, que analisa a causa de um evento (representada pelo nó de um bow tie), com árvore de eventos, que analisa as consequências. Entretanto, o foco bow tie está nas barreiras entre as causas e o risco, e o risco e as consequências.


Fonte: http://www.arrudaconsult.com.br/2020/03/analise-de-risco-tecnica-bow-tie.html

**Para preencher o Diagrama Bow – Tie siga os seguintes passos:**

O diagrama Bow Tie é a base para confecção do Plano de Gestão de Riscos, onde se registra todos os dados levantados nas etapas de análise ambiental e identificação de riscos. Para tanto utilize como base o formulário na página seguinte.

Lembre-se da racionalidade do risco para confirmar se o que está levantando está aderente com o objeto avaliado.

**Devido a <CAUSAS/FONTES>, poderá acontecer <EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA/EFEITO> impactando no/na <DIMENSÃO DE OBJETIVO> >>IMPACTADA>.**

1. Identifique os eventos críticos: Coloque o evento crítico no centro do diagrama.
2. Identifique as causas: No lado esquerdo, liste as causas ou ameaças que podem desencadear o evento crítico.
3. Identifique as consequências: No lado direito, liste as consequências que podem resultar do evento crítico.
4. Identifique os controles ou barreiras de detectivas ou corretivas:

Esses passos ajudarão a estruturar o diagrama Bow Tie de forma eficaz, permitindo uma análise detalhada e uma abordagem focada para cada risco identificado.

| **DEVIDO A** | | **PODERÁ OCORRER** | | **QUE PODE LEVAR A** |
|---|---|---|---|---|
| CAUSA | CONTROLE | EVENTO DE RISCO | CONTROLE | IMPACTO/CONSEQUÊNCIA |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |