MINISTÉRIO DO EMPREENDEDORISMO, DA MICROEMPRESA E DA EMPRESA DE PEQUENO PORTE

Assessoria Especial de Controle Interno – AECI

GUIA METODOLÓGICO PARA GESTÃO DE RISCOS MEMP

Portaria MEMP nº 390, de 16 de dezembro de 2025

Versão | 2026

MINISTÉRIO DO EMPREENDEDORISMO, DA MICROEMPRESA E DA EMPRESA DE PEQUENO PORTE

MINISTÉRIO DO EMPREENDEDORISMO, DA MICROEMPRESA E DA EMPRESA DE PEQUENO PORTE

Ministro de Estado
Paulo Henrique Rodrigues Pereira

Secretário-Executivo
Tiago Nicácio Pereira

Secretária-Executiva Adjunto
Tatiana Severino de Vasconcelos

Secretário Nacional de Inclusão Socioprodutiva, Artesanato e Microempreendedor Individual
Daniel Papa Garcia

Secretário Nacional de Ambiente de Negócios
Maurício Pinto Pereira Juvenal

Chefe da Assessoria Especial de Controle Interno
Luis Eduardo Delmont

Elaboração Técnica
Assessoria Especial de Controle Interno

Equipe Técnica

Luis Eduardo Delmont
Ana Carla de Melo Franco Vasconcelos
Poliany Pereira Gomes

Diagramação
Assessoria de Comunicação Social – ASCOM

MINISTÉRIO DO
EMPREENDEDORISMO,
DA MICROEMPRESA E DA
EMPRESA DE PEQUENO PORTE

SUMÁRIO

APRESENTAÇÃO

Este Guia Metodológico para Gestão de Riscos do Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte (MEMP) foi elaborado pela Assessoria Especial de Controle Interno (AECI) com o objetivo de orientar as equipes do Ministério na implementação estruturada, gradual e efetiva da gestão de riscos institucional.

Esta versão incorpora, com maior profundidade técnica e orientação prática, os preceitos dos seguintes referenciais internacionais e nacionais:

- ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes, com destaque para a integração da gestão de riscos à governança, os oito princípios orientadores e o processo iterativo de gestão;
- ABNT NBR ISO 31010:2021 – Técnicas para o Processo de Avaliação de Riscos, ampliando o leque de técnicas disponíveis para identificação, análise e avaliação;
- Referencial Básico de Gestão de Riscos do Tribunal de Contas da União (TCU, 2018), incorporando o modelo de maturidade em gestão de riscos, o roteiro básico de implementação e as dimensões Ambiente-Processos-Parcerias-Resultados;
- Modelo das Três Linhas do IIA (2013/2020), com detalhamento dos papéis, responsabilidades e mecanismos de coordenação de cada linha de defesa; COSO ERM (2017) – Enterprise Risk Management: Integrating with Strategy and Performance, reforçando a integração entre risco e estratégia.

A gestão de riscos é uma responsabilidade de toda a organização e contribui para o fortalecimento da governança, da integridade e da entrega de resultados à sociedade empreendedora brasileira.

1. FUNDAMENTOS DA GESTÃO DE RISCOS

1.1 Base Legal e Normativa

Quadro 01 – Base legal e normativa

Normativo / Referencial	Objeto
Portaria MEMP nº 390/2025	Institui a Política de Gestão de Riscos do MEMP
Decreto nº 12.694/2025	Aprova a Estrutura Regimental do MEMP
Decreto nº 9.203/2017	Dispõe sobre a política de governança da administração pública federal
IN Conjunta MP/CGU nº 1/2016	Controles internos, gestão de riscos e governança no Poder Executivo federal
ABNT NBR ISO 31000:2018	Gestão de Riscos: Princípios e Diretrizes
ABNT NBR ISO 31010:2021	Técnicas para Avaliação de Riscos
ABNT NBR ISO 31073:2023	Gestão de Riscos: Vocabulário
COSO ERM (2017)	Gerenciamento de Riscos Corporativos: Estrutura Integrada
Referencial TCU (2018)	Referencial Básico de Gestão de Riscos do TCU
Modelo Três Linhas IIA (2020)	Modelo de Três Linhas para Governança e Gestão de Riscos

1.2 Conceitos Fundamentais

Quadro 02 - Conceitos

Conceito	Definição
Risco	Possibilidade de ocorrência de um evento que poderá prejudicar o cumprimento dos objetivos institucionais. (Portaria MEMP nº 390/2025).
Gestão de Riscos	Conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos, visando conferir razoável segurança quanto ao alcance dos objetivos (ISO 31000:2018).
Apetite ao Risco	Nível de risco que a organização está disposta a aceitar na busca de seus objetivos, definido pela Alta Administração (Portaria MEMP nº 390/2025).
Tolerância ao Risco	Variação aceitável no desempenho relativa ao alcance dos objetivos; resiliência da organização diante de desvios.

Conceito	Definição
Risco Inerente	Nível de risco existente antes da consideração de quaisquer ações gerenciais ou controles.
Risco Residual	Nível de risco remanescente após a implementação de controles e tratamentos (pode ainda exigir novo ciclo de tratamento).
Controles Internos	Conjunto de regras, procedimentos, diretrizes, protocolos e rotinas destinados a evitar, mitigar, transferir, compartilhar ou aceitar riscos e oferecer segurança razoável para a consecução da missão institucional. (Portaria MEMP nº 390/2025)
Objeto Prioritário (OP)	Qualquer projeto, processo, programa, política pública, contrato, sistema ou atividade institucional selecionado para submissão ao ciclo de gestão de riscos, com base em critérios de materialidade, criticidade, relevância ou inovação.
Maturidade em Gestão de Risco	Grau de desenvolvimento e institucionalização das práticas de gestão de riscos em uma organização, avaliado nas dimensões Ambiente, Processos, Parcerias e Resultados (TCU, 2018).

1.3 Princípios da Gestão de Riscos

Conforme o art. 4º da Portaria MEMP nº 390/2025, alinhado à ABNT NBR ISO 31000:2018 (cláusula 4), a gestão de riscos do MEMP observa os seguintes princípios:

Quadro 03 – Princípios

#	Princípio MEMP	Fundamento ISO 31000:2018
I	Alinhamento estratégico e proteção do interesse público	Criação e proteção de valor
II	Decisão baseada em evidências	Melhor informação disponível
III	Aderência à boa governança, integridade e liderança	Integrada (parte da governança)
IV	Abordagem estruturada e melhoria contínua	Estruturada e abrangente / Melhoria contínua
V	Integração e transversalidade	Integrada
VI	Proporcionalidade e relevância	Personalizada
VII	Base em informação qualificada e transparência	Melhor informação disponível
VIII	Cultura organizacional empreendedora	Fatores humanos e culturais
IX	Continuidade e tempestividade	Dinâmica

#	Princípio MEMP	Fundamento ISO 31000:2018
X	Agregação de valor e resiliência institucional	Criação e proteção de valor

📌 **Fundamento (ISO 31000:2018, §4):** *Os princípios são a base para gerenciar riscos e convém que sejam considerados ao estabelecer a estrutura e os processos de gestão de riscos, possibilitando à organização gerenciar os efeitos da incerteza nos seus objetivos.*

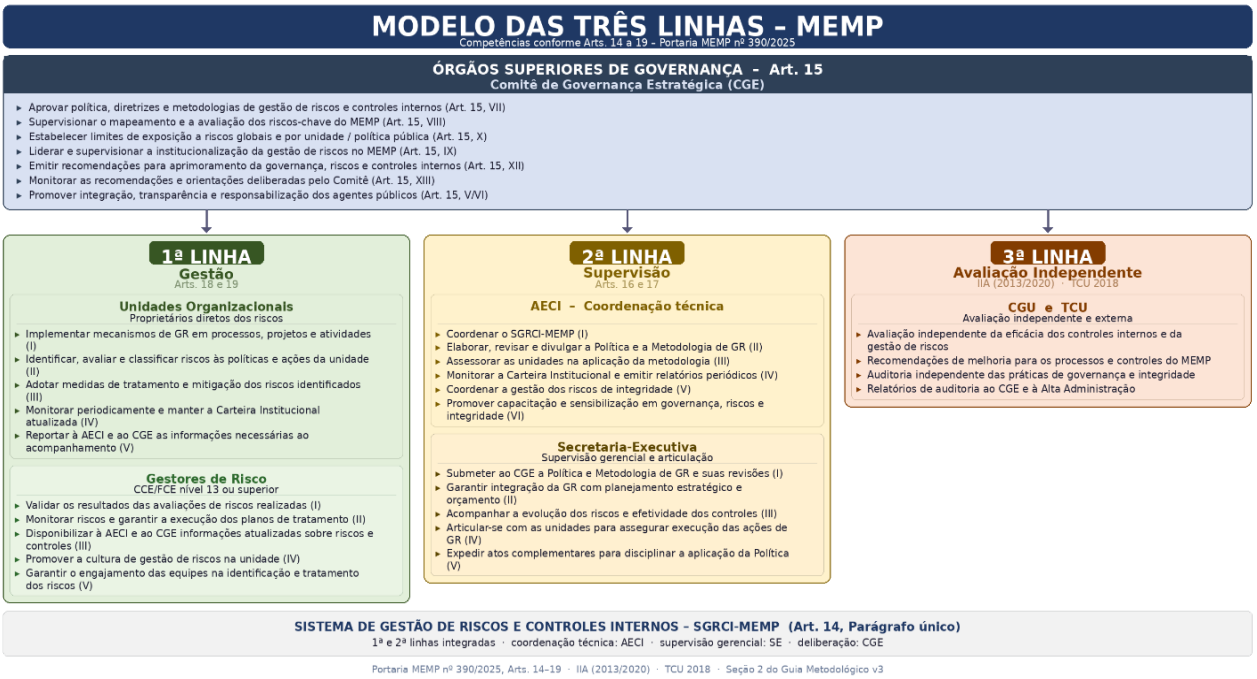
📌 **Fundamento (TCU, 2018):** *Adotar padrões e boas práticas estabelecidos em modelos reconhecidos é uma maneira eficaz de estabelecer uma abordagem sistemática, oportuna e estruturada para a gestão de riscos, que contribua para a eficiência e a obtenção de resultados consistentes.*

2. ESTRUTURA DE GOVERNANÇA: MODELO DAS TRÊS LINHAS

O MEMP adota o Modelo das Três Linhas proposto pelo Institute of Internal Auditors (IIA), referendado pelo TCU, para estruturar as responsabilidades relativas à gestão de riscos e controles internos (art. 14 da Portaria MEMP nº 390/2025). O modelo distingue claramente funções que gerenciam riscos, funções que supervisionam riscos e funções que proveem avaliação independente.

> 📌 **Fundamento (IIA, 2020):** *O Modelo de Três Linhas ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos. O modelo é aplicável a todas as organizações e foca na contribuição que o gerenciamento de riscos oferece para atingir objetivos e criar valor, bem como para a proteção de valor.*

Figura 01 – Modelo das três linhas



2.1 Detalhamento do Modelo de Três Linhas

2.1.1. Antes das Linhas: Órgãos de Governança e Alta Administração

A Alta Administração e os órgãos de governança têm, coletivamente, a responsabilidade pelo estabelecimento dos objetivos da organização, a definição de estratégias e o estabelecimento de estruturas e processos de governança para gerenciar os riscos durante a realização desses objetivos. Nenhuma das três linhas opera adequadamente sem o apoio ativo e a orientação desses órgãos.

No MEMP, o Comitê de Governança Estratégica (CGE) exerce esse papel, competindo-lhe, dentre outros:

- Aprovar a Política e a Metodologia de Gestão de Riscos e suas revisões;
- Estabelecer o apetite a riscos do MEMP e os respectivos limites de exposição a riscos, observadas as especificidades dos processos organizacionais;
- Supervisionar o mapeamento e a avaliação dos riscos-chave;
- Emitir recomendações para o aprimoramento da governança, da gestão de riscos e dos controles internos; e
- Monitorar as recomendações e orientações deliberadas pelo Comitê.

2.1.2. Primeira Linha – Gestão Operacional (Unidades e Gestores de Risco)

Como primeira linha de defesa, os gestores operacionais gerenciam os riscos e têm propriedade sobre eles. São os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

> 📌 **Fundamento (IIA, 2020):** *Os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização. Incluem liderar e dirigir ações, inclusive o gerenciamento de riscos, e a aplicação de recursos para atingir os objetivos da organização. A responsabilidade pelo gerenciamento de riscos é parte integrante dos papéis de primeira linha e permanece dentro do escopo da gestão, mesmo quando papéis de segunda linha fornecem apoio e monitoramento complementares.*

Competências das Unidades Organizacionais (Primeira Linha):

- Implementar mecanismos de gestão de riscos em seus processos, projetos e atividades;
- Identificar, avaliar e classificar riscos que possam comprometer as políticas e ações sob sua responsabilidade;
- Adotar medidas de tratamento e mitigação dos riscos identificados;
- Monitorar periodicamente os riscos e manter registros atualizados na Carteira Institucional de Riscos do MEMP; e
- Reportar à AECI e ao CGE as informações necessárias ao acompanhamento.

Competências dos Gestores de Risco (chefes de unidades):

- Validar os resultados das avaliações de riscos realizadas em sua unidade;
- Monitorar os riscos e garantir a execução dos planos de tratamento;
- Disponibilizar à AECI e ao CGE informações atualizadas sobre riscos e controles;
- Promover a cultura de gestão de riscos em suas equipes; e
- Garantir o engajamento das equipes nas etapas de identificação e tratamento dos riscos.

2.1.3. Segunda Linha – Supervisão e Conformidade (AECI / Secretaria-Executiva)

A segunda linha estabelece, facilita e monitora a implementação de práticas eficazes de gestão de riscos por parte da primeira linha. A 2ª linha integra a estrutura de gestão do Ministério e, por isso, não exerce avaliação independente, que é papel reservado à 3ª linha (CGU e TCU). Sua função é supervisionar e apoiar, não auditar.

> 📌 **Fundamento (IIA, 2013):** *Os papéis de segunda linha fornecem assistência no gerenciamento de riscos. Podem se concentrar em objetivos específicos, como: conformidade com leis, regulamentos e comportamento ético; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade. Como alternativa, podem abranger uma responsabilidade mais ampla pelo gerenciamento de riscos corporativos (ERM). A responsabilidade pelo gerenciamento de riscos, no entanto, segue fazendo parte dos papéis de primeira linha e dentro do escopo da gestão.*

Competências da AECI (coordenação técnica da 2ª linha):

- Coordenar o Sistema de Gestão de Riscos e Controles Internos do MEMP (SGRCI-MEMP);
- Elaborar, revisar e divulgar a Política e a Metodologia de Gestão de Riscos;
- Assessorar as unidades na aplicação da metodologia;
- Monitorar a carteira institucional de riscos e emitir relatórios periódicos;
- Identificar questões emergentes e alertar sobre mudanças no cenário regulatório e de riscos;
- Coordenar a gestão dos riscos de integridade; e
- Promover ações de capacitação e sensibilização em governança, riscos e integridade.

Competências da Secretaria-Executiva (supervisão gerencial da 2ª linha):

- Submeter ao CGE a Política e a Metodologia de Gestão de Riscos e suas revisões;
- Garantir a integração da gestão de riscos com o planejamento estratégico, o orçamento e as principais iniciativas do MEMP;
- Acompanhar a evolução dos níveis de risco e a efetividade dos controles, a partir de relatórios elaborados pela AECI;
- Articular-se com as unidades organizacionais para assegurar a execução das ações de gestão de riscos;
- Expedir atos complementares para disciplinar a aplicação da Política de Gestão de Riscos; e
- Apoiar a tomada de decisões estratégicas sobre riscos críticos, atuando como elo entre a AECI e a Alta Administração.

2.1.4. Terceira Linha – Auditoria Interna e Controle Externo

Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização. Esse alto nível de independência não está disponível na segunda linha de defesa.

> 📌 **Fundamento (IIA, 2013):** *A auditoria interna presta avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Isso é feito através da aplicação competente de processos sistemáticos e disciplinados, expertise e conhecimentos. Uma característica determinante dos papéis de terceira linha é a independência em relação à gestão.*

O escopo da terceira linha cobre:

- A eficiência e eficácia das operações; a salvaguarda de ativos; a confiabilidade dos processos de reporte; e a conformidade com leis, regulamentos, políticas, procedimentos e contratos;
- Todos os elementos da estrutura de gerenciamento de riscos e controle interno (identificação, avaliação, resposta, informação, comunicação e monitoramento); e
- A organização como um todo, incluindo unidades, processos de negócio e funções de suporte.

No contexto do MEMP, exercem a terceira linha a CGU e o TCU, com papéis complementares e distintos: a CGU atua de forma mais próxima ao papel de auditoria interna descrito no Modelo do IIA, pois opera dentro do Poder Executivo, tem acesso contínuo às organizações e produz recomendações orientadas à melhoria da gestão, enquanto o TCU exerce o controle externo em sentido estrito, com função jurisdicional e base constitucional (art. 71 da Constituição Federal). A referência do IIA à "Auditoria Interna" como terceira linha deve, portanto, ser lida no contexto do modelo federal brasileiro como a função desempenhada por essas duas instituições, e não como uma unidade própria do MEMP.

3. O CICLO DE GESTÃO DE RISCOS DO MEMP

O processo de gestão de riscos do MEMP é estruturado em três momentos interconectados, conforme art. 21 da Portaria MEMP nº 390/2025 e alinhado com a ABNT NBR ISO 31000:2018. Embora frequentemente apresentado como sequencial, na prática o processo é iterativo, devendo ser revisado e ajustado continuamente à medida que novos riscos emergem ou o contexto se altera.

> 📌 **Fundamento (ISO 31000:2018, §6.1):** *O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto, avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos. Embora frequentemente apresentado como sequencial, na prática ele é iterativo.*

Quadro 06 – Visão geral do ciclo de gestão de riscos

Quadro 07 – Ciclo de Gestão de Riscos do MEMP

Momento	Pergunta Central	Quem Lidera	Periodicidade	Produto
M1: Escolha dos OPs	Em que vamos aplicar a gestão de riscos este ano?	Unidades + Gestores de Risco + CGE	Anual	Formulário de OPs aprovado pelo CGE
M2: Gerenciamento	Quais são os riscos e o que faremos com eles?	Unidades (1ª linha) + apoio AECI (2ª linha)	Contínuo no ciclo	Matriz de Riscos + Plano de Resposta
M3: Monitoramento e Reporte	Está funcionando? O que precisamos ajustar?	Unidades → AECI → CGE	Contínuo / semestral /anual	Relatório Gerencial + Deliberação CGE

Momento	Pergunta Central	Quem Lidera	Periodicidade	Produto
Os momentos são interconectados e iterativos: o M3 alimenta o próximo M1; novos riscos identificados no M3 podem reabrir o M2 a qualquer tempo. O processo não termina.				

3.1 Momento 1 – Escolha dos Objetos Prioritários (OPs)

As unidades do MEMP (Secretarias Nacionais, Diretorias, Departamentos e unidades de suporte) devem anualmente selecionar os Objetos Prioritários que serão submetidos ao ciclo de gestão de riscos.

Um Objeto Prioritário é **aquilo sobre o qual a unidade vai fazer gestão de riscos** em determinado ciclo anual. É a resposta à pergunta: *"Dentre tudo que fazemos, em que vamos concentrar nossa atenção de gestão de riscos este ano?"*

A palavra **"prioritário"** carrega dois sentidos importantes:

Primeiro, de **seleção** — a unidade não aplica a metodologia em tudo, mas escolhe onde o esforço trará mais retorno, com base nos critérios de materialidade, criticidade, relevância e inovação. Essa seleção deve estar alinhada aos objetivos estratégicos definidos no Plano Estratégico MEMP 2024–2027, garantindo que os riscos gerenciados sejam aqueles com maior potencial de impacto sobre os resultados que o Ministério se comprometeu a entregar.

Segundo, de **foco** — uma vez selecionado, o OP recebe atenção estruturada e documentada: análise de contexto, identificação de riscos, avaliação, tratamento e monitoramento. Sem essa seleção, o risco é que a gestão de riscos fique dispersa e superficial.

3.1.1. O que é um Objeto Prioritário?

Quadro 08 – Tipos de objetos prioritários

Tipo de OP	Descrição
Projeto	Projeto é um esforço único, temporário e progressivo empreendido para criar um produto, serviço ou resultado exclusivo. Geralmente possui início, meio e fim delimitados e contribui com objetivos do Plano Estratégico MEMP 2024-2027.
Processo	Sequência de atividades inter-relacionadas que são realizadas para transformar insumos em produtos e serviços. Podem ser finalísticos (ex.: habilitação, licenciamento, fomento) ou de suporte (ex.: compras, gestão de pessoas, TI).
Programa	Conjunto coordenado de ações e projetos com objetivos comuns, orientado a resultados de médio e longo prazo. Ex.: Programa Acredita.
Política Pública	Política de fomento, regulação ou apoio ao empreendedorismo e ao desenvolvimento das micro e pequenas empresas sob responsabilidade do

Tipo de OP	Descrição
	MEMP. Os riscos são predominantemente de natureza estratégica, regulatória e de impacto social.
Contrato ou Parceria	Contratos de grande vulto, convênios, termos de execução descentralizada ou parcerias estratégicas com alto potencial de risco de execução, financeiro ou reputacional.
Sistema de Informação	Sistema crítico que suporta cadastros, habilitações, transferências ou processos decisórios do MEMP, especialmente relevante no contexto da LGPD e da segurança da informação.
Atividade Institucional	Qualquer outra atividade relevante não enquadrada nas categorias anteriores, incluindo decisões estratégicas específicas, reestruturações organizacionais ou mudanças normativas de grande impacto.

3.1.2. Critérios para Seleção dos OPs

A seleção dos Objetos Prioritários não é arbitrária, ela deve ser justificada com base em pelo menos um dos quatro critérios estabelecidos neste Guia. Essa exigência garante que o esforço de gestão de riscos se concentre onde a exposição institucional é maior e onde os resultados são mais relevantes para o MEMP.

Os critérios não são excludentes, ou seja, um mesmo OP pode atender a mais de um deles simultaneamente, o que reforça sua pertinência para o ciclo. O Gestor de Risco deve indicar, no Formulário de Seleção (Anexo I), qual ou quais critérios fundamentam a escolha, com breve justificativa.

Quadro 09 – Critérios para seleção dos OPs

Critério	Descrição
I – Materialidade	OP que envolve volume significativo de recursos financeiros em sua execução.
II – Criticidade	OP com registro recorrente de irregularidades ou impropriedades apontadas pelos órgãos de controle ou pelas próprias unidades.
III – Relevância	OP relacionado diretamente aos objetivos e/ou projetos estratégicos contidos no Plano Estratégico MEMP 2024-2027.
IV – Inovação	OP com natureza transformadora que requer alto grau de inovação.

Recomenda-se que, especialmente para unidades em fase inicial de implementação, seja selecionado apenas um ou dois OPs por ciclo, de modo que as equipes adquiram familiaridade com a metodologia e os instrumentos disponíveis.

3.1.3. Procedimento de Seleção e Validação

1. A unidade (Secretaria ou Diretoria) analisa seus processos organizacionais e seleciona os OPs mais adequados aos critérios.

2. Preenche o Formulário de Indicação de Objetos Prioritários (Anexo I).
3. O Gestor de Risco (Chefe da unidade) valida o OP indicado.
4. O processo com o Formulário preenchido é encaminhado à AECI.
5. A AECI registra os OPs e os apresenta na reunião subsequente do CGE.

3.2 Momento 2 – Processo de Gerenciamento de Riscos

O Processo de Gerenciamento de Riscos (Momento 2) é o núcleo técnico do ciclo. É aqui que a unidade aplica o processo estruturado de gerenciamento de riscos para cada OP selecionado, identificando o que pode dar errado, avaliando a gravidade de cada risco, verificando se os controles existentes são suficientes e definindo as ações de tratamento necessárias.

O processo segue as etapas previstas no art. 21 da Portaria MEMP nº 390/2025, alinhadas à ABNT NBR ISO 31000:2018 e ao Referencial Básico de Gestão de Riscos do TCU, e se orienta por três características essenciais:

- **Iteratividade** - as etapas são apresentadas em sequência, mas na prática o processo é cíclico. Uma nova informação pode exigir retorno a uma etapa anterior. Isso não é falha, é o funcionamento esperado de um processo que lida com incerteza (ISO 31000:2018, Seção 5).
- **Proporcionalidade** - o nível de detalhamento deve ser compatível com a complexidade do OP. Forçar o mesmo nível de detalhe para todos os objetos gera burocracia sem agregar valor (ISO 31000:2018, Seção 5).
- **Colaboração** - o processo não deve ser feito pelo Gestor de Risco sozinho. Quem executa o objeto conhece os riscos reais melhor do que qualquer documento formal. Envolver essas pessoas é condição para que o resultado reflita a realidade (ISO 31000:2018, §6.2).

O Processo de Gerenciamento de Riscos estrutura-se em duas etapas transversais, que permeiam todo o processo, e cinco etapas sequenciais, que compõem o núcleo técnico:

- **Etapas Transversais:**

  - Comunicação e Consulta - diálogo permanente com as partes interessadas; e
  - Monitoramento e Análise Crítica - verificação contínua da eficácia do processo e dos controles.

- **Etapas Sequenciais:**

  - Estabelecimento do Contexto - levantamento do ambiente interno e externo do OP;
  - Identificação de Riscos - reconhecimento dos eventos que podem impactar os objetivos do OP;
  - Análise de Riscos - cálculo do Risco Inerente (RI = Probabilidade × Impacto) e avaliação dos controles existentes;
  - Avaliação de Riscos - comparação do Risco Residual com o apetite ao risco e priorização das respostas; e
  - Tratamento de Riscos - seleção e implementação das respostas: evitar, mitigar, transferir, aceitar ou explorar.

As etapas são apresentadas em sequência, mas o processo é iterativo, onde uma nova informação pode exigir o retorno a uma etapa anterior a qualquer momento.

3.2.1 Comunicação e Consulta (Transversal a todas as etapas)

A comunicação e consulta é um processo contínuo e transversal, que deve acompanhar todas as fases do gerenciamento de riscos. Visa assegurar o diálogo permanente entre as partes interessadas, garantindo que informações sobre riscos, controles e decisões sejam compartilhadas de forma tempestiva e transparente.

> 📌 **Fundamento (ISO 31000:2018, §6.2):** *O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão.*

A comunicação e consulta visam a:

- Reunir diferentes áreas de especialização para cada etapa do processo de gestão de riscos;
- Assegurar que pontos de vista diferentes sejam considerados ao se definirem critérios de risco e ao se avaliarem riscos;
- Fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisão; e
- Construir senso de inclusão e propriedade entre os afetados pelo risco.

Instrumentos recomendados: reuniões de equipe, oficinas de brainstorming, painéis de monitoramento, relatórios gerenciais, plataformas colaborativas internas.

3.2.2 Monitoramento e Análise Crítica (Transversal a todas as etapas)

O monitoramento e a análise crítica constituem a segunda etapa transversal do processo de gerenciamento de riscos. Enquanto a Comunicação e Consulta (item 3.2.1) cuida do diálogo com as partes interessadas, o Monitoramento e Análise Crítica verifica, de forma contínua, se o próprio processo está funcionando como esperado e se as condições que o originaram permanecem válidas.

> 📌 **Fundamento (ISO 31000:2018, §6.6):** *O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Convém que o monitoramento contínuo e a análise crítica periódica ocorram em todos os estágios do processo de gestão de riscos.*

No contexto do Momento 2, o monitoramento atua em dois níveis distintos e complementares:

- Monitoramento interno ao processo: verifica se as etapas estão sendo executadas corretamente, se as análises permanecem atualizadas e se novos riscos emergiram durante o ciclo. É de responsabilidade da própria unidade e do Gestor de Risco.

- Análise crítica da qualidade: avalia se os resultados de cada etapa, especialmente a identificação e a avaliação de riscos, refletem a realidade do OP ou se precisam ser revisados diante de mudanças no contexto externo ou interno.

Importante distinguir este monitoramento do monitoramento institucional descrito na Seção 4 (Momento 3): aqui o foco é a qualidade e atualidade do processo técnico; lá, o foco é o acompanhamento dos planos de tratamento e o reporte à AECI e ao CGE.

3.2.3 Estabelecimento do Contexto

Estabelecimento do Contexto é a etapa que antecede qualquer identificação de risco. Antes de perguntar o que pode dar errado, é necessário responder em que ambiente este OP existe e com que parâmetros vamos avaliar os riscos que encontrarmos. Sem esse alicerce, a análise de riscos fica descolada da realidade do objeto e os resultados se tornam genéricos ou irrelevantes.

O contexto se desdobra em três dimensões complementares:

O contexto externo mapeia os fatores do ambiente fora do controle direto da unidade que podem criar ou ampliar riscos, tais como mudanças regulatórias, restrições orçamentárias do Governo Federal, demandas dos órgãos de controle, instabilidade política, expectativas dos beneficiários etc. O Gestor de Risco não precisa esgotar todos os fatores externos possíveis, mas deve identificar aqueles com maior capacidade de influenciar o OP no ciclo em questão.

O contexto interno mapeia as condições dentro da própria unidade e do MEMP que afetam o OP, tais como equipe disponível, processos formalizados ou não, sistemas utilizados, cultura organizacional, histórico de problemas, restrições de prazo, entre outros. É nesta dimensão que o Gestor de Risco tem mais capacidade de agir, pois os fatores internos são, em geral, controláveis.

Os critérios de risco definem a régua com que os riscos serão medidos e julgados ao longo de todo o ciclo. A Portaria MEMP nº 390/2025 atribui ao CGE a competência para definir o apetite ao risco e à AECI a responsabilidade pela coordenação metodológica. Os critérios técnicos operacionais estão definidos neste Guia Metodológico e devem ser referendados pelo CGE. Definir esses critérios nesta etapa garante que todas as unidades usem o mesmo padrão, tornando os resultados comparáveis e a Carteira Institucional de Riscos coerente.

A ferramenta recomendada para estruturar o levantamento de contexto é a

SWOT (ou FOFA - Forças, Oportunidades, Fraquezas e Ameaças), que organiza os fatores internos e externos de forma visual e facilita a posterior identificação de riscos. Os dados devem ser registrados na Planilha para Gestão de Riscos (Anexo II).

> 📌 **Fundamento (ISO 31000:2018, §6.3):** *O propósito do estabelecimento do escopo, contexto e critérios é personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado. O contexto externo e interno é o ambiente no qual a organização procura definir e alcançar seus objetivos.*

Quadro 10 – Contextos

Dimensão	Descrição	Ferramentas / Fontes
Contexto Externo	Fatores políticos, econômicos, sociais, tecnológicos, ambientais e legais (PESTEL) que podem afetar o alcance dos objetivos do OP.	Análise PESTEL, relatórios setoriais, normativos, dados de mercado.
Contexto Interno	Estrutura organizacional, cultura, recursos humanos, processos, sistemas, competências e valores do MEMP que influenciam o risco.	Plano Estratégico MEMP 2024-2027, organograma, processos mapeados.
Critérios de Risco	Definição do escopo, critérios de risco, apetite e tolerância ao risco, partes interessadas relevantes.	Portaria MEMP nº 390/2025, deliberações do CGE.

3.2.4 Identificação de Riscos

A identificação de riscos é a etapa em que a equipe do OP sistematicamente busca, reconhece e descreve os eventos que podem impedir ou facilitar o alcance dos objetivos. Ela parte do contexto levantado na etapa anterior e transforma as ameaças e incertezas identificadas em registros estruturados, prontos para análise.

Para cada risco identificado, devem ser descritos: o evento de risco, suas causas prováveis, as possíveis consequências sobre o OP e os controles que já existem para reduzi-lo. Esse conjunto de informações é registrado na Planilha para Gestão de Riscos (Anexo II) e constitui a base de toda a etapa seguinte.

Um ponto importante: a identificação não deve se restringir a ameaças óbvias ou já conhecidas. A ISO 31000:2018 recomenda que a organização identifique riscos independentemente de suas fontes estarem ou não sob seu controle. Os riscos externos, riscos de integridade, riscos tecnológicos e riscos decorrentes de inação também devem ser considerados.

> 📌 **Fundamento (ISO 31000:2018, §6.4.2):** *O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. A organização pode usar uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos.*
>
> 📌 **Fundamento (ISO 31000:2018, §6.4.2):** *Convém que a organização identifique os riscos independentemente de suas fontes estarem ou não sob seu controle. Pode haver mais de um tipo de resultado, o que pode resultar em uma variedade de consequências tangíveis ou intangíveis.*

3.2.4.1. Categorias de Risco

Para orientar a varredura e evitar lacunas, o MEMP adota as seguintes categorias de risco. Ao percorrer cada categoria, a equipe aumenta a chance de identificar riscos que passariam despercebidos em uma análise livre.

Quadro 11 – Categorias de Risco

Categoria	Descrição
Estratégico	Eventos que impactam os objetivos estratégicos definidos no Plano Estratégico MEMP 2024-2027.
Operacional	Eventos que podem comprometer as atividades do MEMP, associados a falhas de processos, pessoas, infraestrutura ou sistemas.
Conformidade (Legal)	Eventos derivados de alterações legislativas ou normativas que possam comprometer as atividades do MEMP.
Financeiro/Orçamentário	Eventos que comprometam a capacidade do MEMP de dispor dos recursos necessários à realização de suas atividades.
Imagem/Reputação	Eventos que possam comprometer a confiança da sociedade na capacidade do MEMP em cumprir sua missão institucional.
Integridade	Eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta.
Tecnologia da Informação	Eventos relacionados à segurança da informação, indisponibilidade de sistemas e proteção de dados pessoais (LGPD).
Risco Registral e Normativo	Eventos decorrentes de falhas na supervisão técnica das Juntas Comerciais, de inconsistências nas Instruções Normativas do DREI, de decisões em recursos administrativos com potencial de nulidade, de irregularidades em atos de arquivamento ou autenticação com repercussão erga omnes, e de mudanças normativas no Direito Empresarial que impactem os padrões registrais vigentes.

3.2.4.2. Técnicas de Identificação

A escolha da técnica depende do contexto e da complexidade do OP. A ISO 31010:2021 apresenta um amplo catálogo. O MEMP recomenda as seguintes técnicas como ponto de partida, podendo a equipe combiná-las conforme necessário.

Quadro 12 – Técnicas de Identificação de Risco

Técnica	Descrição Aplicada	Melhor para
Brainstorming	Dinâmica coletiva para obtenção de riscos sem censura inicial, seguida de análise estruturada.	OPs em fase inicial; equipes multidisciplinares
Entrevistas estruturadas	Conversa dirigida com especialistas e partes interessadas para identificar riscos específicos.	Riscos técnicos e de conformidade
Análise de Causa Raiz (ACR)	Investigação das causas fundamentais de um evento de risco para atacar a origem, não o sintoma.	Riscos recorrentes; lições aprendidas
Análise SWOT	Mapeamento de forças, fraquezas, oportunidades e ameaças relacionadas ao OP.	Estabelecimento do contexto; identificação inicial
Análise de Cenários	Elaboração de cenários plausíveis de futuro para identificar riscos emergentes e de baixa frequência.	Riscos estratégicos e de longo prazo
Checklists	Listas padronizadas de riscos conhecidos para conferência sistemática.	OPs semelhantes a ciclos anteriores
Delphi	Consulta iterativa a especialistas para convergência de opiniões sobre riscos.	Riscos de difícil quantificação; incertezas elevadas
Análise Bow Tie	Diagrama que conecta causas a consequências por meio do evento central, mapeando controles preventivos e mitigadores.	Riscos críticos e de alta complexidade

3.2.5 Análise e Avaliação de Riscos

A análise de riscos avalia a probabilidade de ocorrência e o impacto potencial de cada risco identificado. A avaliação compara o nível de risco com os critérios de apetite e tolerância definidos pela Alta Administração, classificando-os por prioridade.

> 📌 **Fundamento (ISO 31000:2018, §6.4.3):** *O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco. A análise envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. As técnicas podem ser qualitativas, quantitativas ou combinadas.*

3.2.5.1 Análise do Risco Inerente

O Risco Inerente é o nível de risco existente antes da consideração de quaisquer controles ou medidas de mitigação. Ele é calculado pela combinação da probabilidade de ocorrência do evento com a magnitude do seu impacto sobre os objetivos do OP, expressando o grau de exposição natural da organização àquele risco. Quanto maior o risco inerente, maior a necessidade de controles robustos para reduzi-lo a um nível aceitável.

O Risco Inerente (RI) é calculado sem a consideração de quaisquer controles existentes:

RI = Probabilidade (P) × Impacto (I)

Quadro 13 – Escala de Probabilidade[1]

Magnitude	Nota	Descrição
Muito Baixo	1	Evento improvável de ocorrer. Excepcional.
Baixo	2	Evento raro. Pode ocorrer de forma inesperada.
Médio	5	Evento possível. Há elementos que indicam moderadamente essa possibilidade.
Alto	8	Evento provável. Esperado que ocorra, com elementos consistentes.
Muito Alto	10	Evento praticamente certo. Inequivocamente ocorrerá.

Quadro 14 – Escala de Impacto[2]

Magnitude	Nota	Descrição
Muito Baixo	1	Causa impactos mínimos nos objetivos de prazo, custo, qualidade ou imagem.
Baixo	2	Causa impactos pequenos nos objetivos, com recuperação facilmente possível.
Médio	5	Interrompe parcialmente operações, com impactos significativos, porém recuperáveis.
Alto	8	Interrompe operações com impactos de reversão muito difícil nos objetivos.
Muito Alto	10	Paralisa operações, causando impactos irreversíveis ou catastróficos nos objetivos.

[1] A escala não linear adotada pelo MEMP busca ampliar a diferenciação entre riscos moderados e riscos críticos, favorecendo a priorização gerencial e a tomada de decisão.
[2] A escala não linear adotada pelo MEMP busca ampliar a diferenciação entre riscos moderados e riscos críticos, favorecendo a priorização gerencial e a tomada de decisão.

Quadro 15 – Resultado dos Riscos Inerentes

Nível de Risco	Pontuação (P × I)	Orientação de Resposta
Baixo	Até 9	Risco aceitável com monitoramento periódico.
Médio	10 a 39	Requer atenção e pode demandar ações de controle.
Alto	40 a 79	Requer plano de tratamento e acompanhamento frequente.
Extremo	80 a 100	Requer ação imediata da Alta Administração.

Pode-se ainda representar o produto das variáveis e os níveis de risco visualmente através de uma tabela com os resultados (Mapa de Calor):

Figura 1 – Mapa de Calor do Risco Inerente.

As cores indicam o nível de risco resultante da combinação de Probabilidade e Impacto.

3.2.5.2 Avaliação dos Controles Existentes

Os controles internos da gestão são regras, procedimentos, práticas e sistemas que minimizam a probabilidade ou o impacto do risco. São os controles que a unidade ou o Ministério possui que têm a força de reduzir de algum modo o risco residual. O conjunto desses controles deve ser então avaliado segundo o quanto é confiável, no sentido de ser capaz de mitigar os riscos respectivos.

Para cada risco, devem ser listados os controles existentes e avaliada sua eficácia:

Quadro 16 – Escala de Avaliação dos Controles

Avaliação	Risco de Controle (RC)	Descrição
Inexistente	1,00	Controle não existe, não funciona ou não está implementado.
Fraco	0,80	Controle não institucionalizado; realizado de forma manual e informal. Confiança de 20%.
Mediano	0,60	Controle razoavelmente institucionalizado, mas pode falhar. Confiança de 40%.
Satisfatório	0,40	Controle institucionalizado e sustentado por ferramentas adequadas. Confiança de 60%.
Forte	0,20	Controle institucionalizado, em nível de melhor prática, mitigando o risco em todos os aspectos relevantes. Confiança de 80%.

3.2.5.3 Cálculo do Risco Residual

O Risco Residual (RR) é o nível de risco que permanece após a consideração dos controles existentes. Enquanto o Risco Inerente mede a exposição bruta ao risco, o Risco Residual mede a exposição real, que é aquela com a qual a organização efetivamente convive. É ele que orienta a decisão sobre tratamento: se o RR estiver dentro do apetite ao risco definido pela Alta Administração, o risco pode ser aceito com monitoramento; se estiver acima, exige plano de tratamento.

O cálculo multiplica o Risco Inerente pelo Risco de Controle (RC), que reflete a eficácia dos controles existentes. Quanto mais forte o controle, menor o RC e, consequentemente, menor o RR. A tabela abaixo classifica o resultado em quatro níveis de atenção, cada um com uma orientação de resposta distinta.

RR = RI (Risco Inerente) × RC (Risco de Controle)

Quadro 17 – Risco Residual

Nível	Pontuação RR	Sinalização	Orientação
Baixo	Até 9	Verde	Risco dentro do apetite. Monitorar periodicamente.

Médio	10 a 39	Amarelo	Avaliar necessidade de novos controles. Monitorar com maior frequência.
Alto	40 a 79	Laranja	Plano de tratamento obrigatório. Acompanhamento mensal.
Extremo	80 a 100	Vermelho	Ação imediata. Reportar à Alta Administração.

Os riscos cujo nível residual supere o apetite ao risco definido pela Alta Administração deverão ser submetidos a planos de tratamento. Riscos dentro do apetite poderão ser aceitos formalmente, com monitoramento regular.

> 📌 **Fundamento (TCU, 2018):** *Considerando que não existe risco zero, ao final da adoção das medidas mitigadoras restam riscos residuais que precisam ser monitorados e mantidos dentro de limites compatíveis com os critérios de risco estabelecidos.*

As metodologias de mensuração e classificação de riscos possuem caráter orientativo e destinam-se a apoiar a análise, priorização e tomada de decisão, não substituindo o julgamento técnico, a análise contextual e a avaliação crítica das unidades responsáveis, da AECI e da Alta Administração.

3.2.6 Definição do Apetite ao Risco

O apetite ao risco é o nível de risco que o MEMP está disposto a assumir na busca de seus objetivos institucionais. Sua definição é competência do CGE, devendo orientar todas as decisões sobre tratamento e aceitação de riscos em todas as unidades do Ministério.

> 📌 **Fundamento (ISO 31000:2018, §6.3.4):** *Convém que a organização especifique a quantidade e o tipo de risco que podem ou não assumir em relação aos objetivos. Convém também que estabeleça critérios para avaliar a significância do risco e para apoiar os processos de tomada de decisão. Os critérios de risco devem refletir os valores, objetivos e recursos da organização.*

O apetite ao risco não é tolerância zero. Toda organização convive com algum nível de risco. O que o apetite define é o limite a partir do qual o risco deixa de ser aceitável e passa a exigir ação obrigatória. Riscos abaixo desse limite podem ser aceitos formalmente com monitoramento regular e riscos acima dele exigem plano de tratamento.

3.2.7 Tratamento de Riscos

O tratamento de riscos é a etapa em que a análise se converte em ação. Após identificar o Risco Residual de cada evento e compará-lo com o apetite ao risco definido pelo CGE, a unidade deve decidir o que fazer com cada risco que ultrapasse esse limiar e registrar formalmente essa decisão, independentemente da estratégia escolhida.

O processo não é linear, ou seja, a implementação de uma medida pode reduzir o RR a um nível aceitável, mas pode também introduzir novos riscos que precisarão ser identificados e tratados.

Por isso, a tabela abaixo não deve ser lida como um cardápio sequencial, mas como um conjunto de opções que podem ser combinadas para o mesmo risco.

Como escolher a estratégia adequada

A escolha depende de três fatores: o nível do RR, a viabilidade de controle e a proporcionalidade entre o custo do tratamento e o benefício esperado. Em geral:

- Riscos com RR extremo e sem possibilidade de controle efetivo dentro do prazo do ciclo devem ser **evitados** - a atividade que os origina precisa ser descontinuada ou redesenhada.
- Riscos com RR alto ou extremo, mas com controles possíveis dentro da capacidade da unidade, devem ser **mitigados** - é a estratégia mais adequada no contexto do MEMP.
- Riscos que envolvam alto impacto financeiro ou operacional e que possam ser redistribuídos por meio de parcerias, convênios ou acordos interinstitucionais podem ser **transferidos ou compartilhados**. No setor público, essa estratégia não se traduz em seguros comerciais, ela se materializa em acordos de cooperação, termos de parceria e compartilhamento de responsabilidades com outros órgãos ou entes federativos.
- Riscos com RR dentro do apetite ao risco podem ser formalmente **aceitos**, desde que essa decisão seja registrada na planilha e comunicada à AECI. Aceitar um risco não é ignorá-lo, é uma decisão consciente e documentada de conviver com ele sob monitoramento.
- Riscos que, em vez de ameaças, revelem oportunidades de melhoria ou inovação no OP podem ser **explorados** - a unidade adota medidas para maximizar o resultado positivo associado à incerteza.

> 📌 **Fundamento (ISO 31000:2018, §6.5.1):** *O tratamento de riscos envolve um processo iterativo de: formular e selecionar opções de tratamento; planejar e implementar o tratamento; avaliar a eficácia deste tratamento; decidir se o risco remanescente é aceitável; e, se não for, realizar tratamento adicional.*

Quadro 18 - Tratamento de Riscos

Estratégia	Descrição	Quando aplicar
Evitar	Eliminar a atividade ou processo que dá origem ao risco, quando os custos ou impactos potenciais superem os benefícios.	Riscos extremos sem mitigação viável
Mitigar	Adotar medidas para reduzir a probabilidade de ocorrência e/ou a magnitude do impacto do risco.	Riscos altos ou extremos com controles possíveis
Transferir / Compartilhar	Redistribuir a probabilidade ou o impacto por meio de parcerias, contratos, seguros ou terceirização.	Riscos com alto impacto financeiro ou operacional
Aceitar	Não adotar medida alguma quando o risco residual estiver dentro do apetite ou o custo de tratamento superar o benefício. Requer registro formal e ciência da Alta Administração.	Riscos baixos ou dentro do apetite

Estratégia	Descrição	Quando aplicar
Explorar (oportunidade)	Reconhecer o risco como oportunidade de inovação ou melhoria e adotar medidas para maximizar o resultado positivo.	Riscos que revelam oportunidades estratégicas

Para cada risco não aceito, ou seja, todo risco com RR acima do apetite deve ser elaborado um Plano de Resposta ao Risco (Anexo III). O plano é o instrumento formal que traduz a estratégia escolhida em ações concretas, com responsável, prazo, indicador de acompanhamento e custo estimado. Sem o Plano de Resposta, a decisão de tratamento existe apenas no papel e não há compromisso nem possibilidade de monitoramento.

Um ponto importante: o Plano de Resposta pode, por si só, introduzir novos riscos. Uma ação de mitigação que envolva contratação de terceiros, por exemplo, cria riscos de conformidade e de gestão contratual que precisarão ser avaliados. Esse é o caráter iterativo do tratamento de riscos previsto na ISO 31000:2018, §6.5.1.

> 📌 **Fundamento (ISO 31000:2018, §6.5.3):** *O propósito dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos e o progresso em relação ao plano possa ser monitorado. O tratamento de riscos também pode introduzir novos riscos que precisem ser gerenciados.*

4. MONITORAMENTO, REVISÃO E REPORTE

O monitoramento abordado nesta seção é distinto do monitoramento transversal descrito no item 3.2.2. Aquele verifica, em tempo real, se o processo técnico de gerenciamento de riscos está sendo conduzido corretamente, ou seja, se as análises estão atualizadas, se novos riscos emergiram e se os controles continuam válidos.

Este, do Momento 3, tem foco institucional: acompanha se os planos de tratamento estão sendo executados, consolida o perfil de risco do MEMP e reporta os resultados à Alta Administração e ao CGE. Os dois são complementares e igualmente necessários. Sem o primeiro, o processo técnico perde qualidade e sem o segundo, os resultados não chegam a quem decide.

> 📌 **Fundamento (ISO 31000:2018, §6.6):** *O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. O monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados devem ser uma parte planejada do processo, com responsabilidades claramente estabelecidas.*

Quadro 19 - Nível de Monitoramento

Nível de Monitoramento	Responsável	Frequência	Produto
1º Nível - Operacional	Unidades Organizacionais e Gestores de Risco	Trimestral	Matriz de Riscos atualizada; registros no SEI
2º Nível - Supervisão	AECI	Semestral (Relatório) e pontual quando necessário	Relatório Gerencial de Riscos; alertas à Alta Administração
3º Nível - Governança	CGE	Semestral (reunião de monitoramento)	Ata de reunião / Resolução / Deliberação

4.1 Periodicidade do Ciclo de Gestão de Riscos

A gestão de riscos não é um evento único. A periodicidade definida neste item estabelece o ritmo mínimo esperado de cada atividade do ciclo, garantindo que as informações sobre riscos permaneçam atualizadas, que os planos de tratamento sejam acompanhados e que o CGE disponha de subsídios suficientes para suas deliberações. O não cumprimento dos prazos não é apenas uma falha procedimental, é um sinal de que o sistema de gestão de riscos está perdendo efetividade.

Quadro 20 - Periodicidade do Ciclo

Atividade	Periodicidade	Responsável	Produto
Seleção de OPs	Anual	Unidades Organizacionais	Formulário de Indicação de OPs (Anexo I)

Atividade	Periodicidade	Responsável	Produto
Atualização da Matriz de Riscos	Mínimo semestral	Unidades e Gestores de Risco	Planilha para Gestão de Riscos (Anexo II)
Relatório Gerencial da AECI	Semestral	AECI	Relatório Gerencial de Riscos
Reunião de monitoramento no CGE	Semestral	CGE	Ata de reunião / Resolução
Revisão da Política de Gestão de Riscos	A cada 2 anos ou quando houver mudança significativa	AECI / SE	Nova versão da Portaria ou IN

4.2 Monitoramento pelas Unidades

O monitoramento das unidades é o primeiro nível do Momento 3. Ele se concretiza nos **Pontos de Controle,** que são reuniões periódicas da equipe do OP, conduzidas pelo Gestor de Risco, para verificar o andamento dos planos de tratamento e a evolução do perfil de risco.

Os Pontos de Controle devem ocorrer no mínimo semestralmente, coincidindo com o calendário do Relatório Gerencial da AECI. Para OPs com riscos Altos ou Extremos, recomenda-se periodicidade mensal. Participam o Gestor de Risco, os responsáveis pelas ações de tratamento e, quando pertinente, a autoridade superior da unidade.

Em cada Ponto de Controle, a equipe deve verificar:

- O cumprimento do cronograma das ações de tratamento;
- Surgimento de novos riscos desde o último monitoramento;
- A eficácia dos controles existentes, podendo ser revistos ou não;
- A tempestividade informada à Alta Administração; e
- Informações atualizadas no processo SEI.

Os resultados de cada Ponto de Controle devem ser registrados no processo SEI do OP, com indicação da data, dos participantes e das deliberações. Esse registro é a evidência que a AECI utilizará para consolidar o Relatório Gerencial e que os órgãos de controle poderão consultar em eventual avaliação.

Riscos que se materializam fora do ciclo regular

Se um risco identificado na matriz se materializar ou se um risco novo e grave surgir entre dois Pontos de Controle, a unidade não deve aguardar o próximo ciclo. O Gestor de Risco deve comunicar imediatamente a AECI, que avalia a necessidade de acionar a Alta Administração e o CGE em caráter extraordinário. Riscos Extremos não materializados que apresentem sinais de agravamento também justificam comunicação imediata, sem aguardar o próximo Ponto de Controle.

4.3 Supervisão pela AECI e Reporte ao CGE

O Relatório Gerencial de Riscos é elaborado semestralmente pela AECI e constitui o principal instrumento de reporte ao CGE. Ele transforma as informações descentralizadas das unidades em uma visão consolidada e priorizada do perfil de risco do MEMP, subsidiando as deliberações do Comitê.

O Relatório Gerencial deve conter, no mínimo:

- **Sumário executivo:** síntese dos principais riscos do ciclo, destacando os que sofreram agravamento ou foram materializados no período.
- **Carteira consolidada:** quantitativo de riscos por nível (Baixo, Médio, Alto, Extremo), por categoria e por unidade.
- **Status dos planos de tratamento:** proporção de ações concluídas, em andamento e atrasadas, com identificação dos responsáveis pelos atrasos.
- **Riscos transversais:** riscos semelhantes identificados em mais de uma unidade, com análise das causas comuns e recomendação de tratamento coordenado.
- **Riscos materializados no período:** descrição dos eventos ocorridos, impactos verificados e lições aprendidas.
- **Recomendações ao CGE:** ações estruturantes que dependem de deliberação da Alta Administração, tais quais: revisão do apetite ao risco, alocação de recursos e definição de responsabilidades transversais.
- **Evolução da maturidade:** comparativo com o ciclo anterior, quando disponível.

> 📌 **Fundamento (ISO 31000:2018, §6.7):** *O registro e o relato visam: comunicar atividades e resultados de gestão de riscos em toda a organização; fornecer informações para a tomada de decisão; melhorar as atividades de gestão de riscos; e auxiliar a interação com as partes interessadas. O relato é parte integrante da governança da organização.*

4.4 Carteira Institucional de Riscos

A Carteira Institucional de Riscos é a visão consolidada de todos os riscos gerenciados pelo MEMP em determinado ciclo. Mantida e atualizada pela AECI, ela reúne em um único instrumento os riscos identificados por todas as unidades em seus respectivos OPs, permitindo uma leitura global do perfil de risco do Ministério.

A carteira serve três funções principais: (a) subsidiar o Relatório Gerencial semestral da AECI ao CGE, com uma visão consolidada e priorizada dos riscos mais críticos do MEMP; (b) identificar riscos transversais, que são riscos semelhantes que aparecem em múltiplas unidades com causas comuns, como dependência de um sistema crítico, restrição orçamentária estrutural ou mudança regulatória que afeta as secretarias, permitindo tratamento coordenado; e (c) alimentar as deliberações do CGE com informação organizada por nível de criticidade, categoria e status dos planos de tratamento.

No ciclo inaugural, a carteira pode ser mantida em planilha eletrônica consolidada pela AECI, com uma aba por unidade e uma aba de visão geral com todos os riscos ordenados por nível residual. Com o avanço da maturidade organizacional, pode evoluir para sistemas mais robustos de gestão

e monitoramento. A carteira deve ser atualizada minimamente a cada Ponto de Controle semestral e sempre que um risco extremo for identificado fora do ciclo regular.

5. MODELO DE MATURIDADE EM GESTÃO DE RISCOS

O modelo de maturidade é uma forma de medir **em que estágio de desenvolvimento** o Ministério está na implementação da gestão de riscos e para onde precisa evoluir.

O MEMP adota o modelo de maturidade em gestão de riscos descritos no capítulo 7 do Referencial Básico de Gestão de Riscos do TCU (2018), desenvolvido com referência nas boas práticas do COSO GRC, ABNT NBR ISO 31000, Orange Book e IN-MP/CGU Nº 1/2016. O modelo avalia o grau de desenvolvimento e institucionalização das práticas de gestão de riscos em quatro dimensões: Ambiente, Processos, Parcerias e Resultados.

> 📌 **Fundamento (TCU, 2018):** *Como forma de contribuir com o monitoramento, a revisão e a melhoria contínua dos modelos de gestão de risco adotados pela administração pública, o TCU desenvolveu um modelo de avaliação da maturidade organizacional em gestão de riscos. Tal modelo tem por referência boas práticas preconizadas pelo COSO GRC, ABNT NBR ISO 31000 e Orange Book, bem como pela IN-MP/CGU Nº 1/2016.*

5.1 Dimensões do Modelo de Maturidade

O modelo de maturidade não avalia a gestão de riscos como um bloco único e sim em quatro dimensões complementares, cada uma medindo um aspecto diferente do desenvolvimento institucional. Essa estrutura permite identificar onde estão as lacunas, ou seja, uma organização pode ter política formalmente aprovada (Ambiente bem avaliado) mas ainda não executar o ciclo de forma consistente (Processos em estágio inicial). A avaliação por dimensão é o que transforma o diagnóstico de maturidade em um instrumento útil de planejamento, pois aponta exatamente onde concentrar os esforços de melhoria no ciclo seguinte.

Quadro 21 - Dimensões do Modelo de Maturidade

Dimensão	Aspecto Avaliado	Itens Chave
Ambiente	Liderança	Comprometimento da Alta Administração; comunicação dos objetivos de GR; recursos alocados
Ambiente	Políticas e Estratégias	Existência e qualidade da política de GR; alinhamento estratégico; apetite ao risco definido
Ambiente	Pessoas	Capacitação; cultura de risco; papéis e responsabilidades definidos
Processos	Identificação e análise de riscos	Sistematização da identificação; qualidade das análises; técnicas utilizadas
Processos	Avaliação e resposta a riscos	Priorização de riscos; planos de tratamento; monitoramento dos planos
Processos	Monitoramento e comunicação	Periodicidade do monitoramento; qualidade dos relatórios; comunicação às partes interessadas
Parcerias	Integração e coordenação	Articulação entre linhas de defesa; coordenação com órgãos de controle; benchmarking

Dimensão	Aspecto Avaliado	Itens Chave
Resultados	Efetividade	Evidências de melhoria; redução de riscos materializados; aprendizado organizacional

5.2 Níveis de Maturidade

Os níveis de maturidade descrevem uma trajetória e não um julgamento. Nenhuma organização começa no nível 5, e estar no nível 1 ou 2 não significa falha de gestão, mas sim o reconhecimento honesto do ponto de partida. O que importa é que cada nível seguinte seja alcançado com base em evidências concretas de mudança, e não apenas por declaração formal. A tabela a seguir descreve as características de cada nível para que a AECI, a SE e as unidades possam identificar com objetividade em qual estágio o MEMP se encontra e o que é necessário para avançar.

Quadro 22 - Níveis de Maturidade

Nível	Denominação	Características
1	Inicial / Ad hoc	Práticas informais e não sistematizadas. A gestão de riscos depende de iniciativas individuais. Sem política formal.
2	Em desenvolvimento	Política de gestão de risco existente, mas implementação parcial. Algumas unidades adotam práticas. Metodologia em construção.
3	Definido	Metodologia formalizada e aplicada de forma consistente. Papéis definidos. Relatórios periódicos produzidos.
4	Gerenciado	Gestão de risco integrada ao planejamento e às decisões. Monitoramento sistemático. Indicadores de desempenho estabelecidos.
5	Otimizado	Gestão de risco dinâmica e em melhoria contínua. Cultura organizacional consolidada. Benchmarking e inovação em práticas de risco.

5.3 Trajetória de Maturidade do MEMP

A AECI realizará anualmente a autoavaliação de maturidade em gestão de riscos do MEMP, com base no modelo TCU. Os resultados subsidiarão o planejamento de melhorias e a definição de prioridades para o ciclo subsequente.

Quadro 23 - Ciclo de Autoavaliação da Maturidade

Ciclo	Meta de Maturidade	Ações Prioritárias
2026 (Ciclo Inaugural)	Nível 2 – Em desenvolvimento	Institucionalização da metodologia; capacitação das unidades; primeiros ciclos de OPs
2027	Nível 3 – Definido	Expansão para todas as unidades; relatórios consolidados; avaliação de eficácia dos controles

Ciclo	Meta de Maturidade	Ações Prioritárias
2028	Nível 4 – Gerenciado	Integração com planejamento e orçamento; indicadores de GR nos relatórios de gestão; melhoria contínua

A trajetória acima cobre o horizonte do ciclo inaugural de implementação da gestão de riscos no MEMP (2026–2028). A partir de 2029, as metas de maturidade serão definidas anualmente pela AECI com base nos resultados da avaliação do ciclo anterior, apresentadas ao CGE para deliberação e incorporadas ao plano de trabalho da Assessoria. Essa autonomia de planejamento é, em si, um indicador de maturidade e significa que o sistema não depende mais de uma tabela prescritiva para se orientar

5.4 Avaliação Anual da Maturidade

A avaliação anual de maturidade é o instrumento pelo qual o MEMP verifica, de forma sistemática e baseada em evidências, o estágio de desenvolvimento de suas práticas de gestão de riscos. Ela é conduzida anualmente pela AECI e pela Secretaria-Executiva (SE), de forma independente, com os resultados consolidados e apresentados ao CGE.

> 📌 **Fundamento (Referencial TCU, 2018, Cap. 7):** *Como forma de contribuir com o monitoramento, a revisão e a melhoria contínua dos modelos de gestão de risco, o TCU desenvolveu um modelo de avaliação da maturidade organizacional que tem por referência boas práticas preconizadas pelo COSO GRC, ABNT NBR ISO 31000 e Orange Book, bem como pela IN-MP/CGU nº 1/2016.*

A avaliação utiliza a seguinte escala de pontuação, aplicada a cada pergunta do Questionário de Maturidade (Anexo IV):

Quadro 24 - Avaliação de Maturidade

Nota	Nível	Significado
1	Inexistente	Prática não existe ou nunca foi implementada.
2	Inicial	Prática existe de forma isolada e informal.
3	Em desenvolvimento	Prática existe e está sendo estruturada, mas ainda incompleta.
4	Definido	Prática formalizada e aplicada consistentemente.
5	Otimizado	Prática consolidada, monitorada e em melhoria contínua.

O questionário completo, as orientações de preenchimento e o modelo de consolidação dos resultados estão no Anexo IV deste Guia.

A periodicidade e os responsáveis pela avaliação seguem a seguinte lógica:

Quadro 25 - Periodicidade e Responsáveis pela Avaliação da Maturidade

Ciclo	Quem avalia	Periodicidade	Produto
Inaugural (2026)	AECI e SE, de forma independente. Unidades não respondem neste ciclo.	Único (antes do 1º ciclo de OPs)	Diagnóstico de linha de base apresentado ao CGE
A partir de 2027	Unidades que completaram ao menos um ciclo completo de OPs + SE + AECI, de forma independente.	Anual	Diagnóstico atualizado + Plano de Melhoria apresentado ao CGE

6. RISCOS DE INTEGRIDADE

Os riscos de integridade merecem atenção especial no âmbito do MEMP, por envolverem condutas que comprometem a ética, a probidade e a confiança pública. Sua gestão é coordenada pela AECI em articulação com o Programa Empreendendo Integridade.

Os riscos de integridade constituem uma categoria especial dentro do sistema de gestão de riscos do MEMP. Ao contrário dos riscos operacionais, estratégicos ou financeiros, que em geral decorrem de falhas, incertezas ou fatores externos, os riscos de integridade envolvem comportamentos intencionais que comprometem a ética, a probidade e a confiança pública, tais como: corrupção, fraude, nepotismo, conflito de interesses e desvios de conduta. Essa natureza específica exige atenção redobrada e tratamento diferenciado.

A gestão dos riscos de integridade no MEMP é coordenada pela AECI em articulação com o Programa Empreendendo Integridade, conforme previsto na Portaria MEMP nº 390/2025. Essa articulação é intencional, ou seja, os riscos de integridade não devem ser tratados apenas no âmbito do Programa de Integridade de forma isolada. Eles precisam integrar a Matriz de Riscos de cada OP onde forem identificados, seguindo o mesmo processo de identificação, análise, avaliação e tratamento descrito neste Guia.

Nem todo OP apresentará riscos de integridade. A questão que o Gestor de Risco deve fazer durante a etapa de identificação é: *"Existe neste OP alguma situação em que uma pessoa poderia se beneficiar pessoalmente de uma decisão irregular, ou em que recursos públicos poderiam ser desviados ou mal utilizados?"* OPs que envolvam contratos, licitações, concessão de benefícios, habilitações, acesso a dados sensíveis ou decisões discricionárias com impacto financeiro relevante têm maior propensão a apresentar riscos de integridade. OPs essencialmente técnicos, tais como elaboração de normas, estudos analíticos ou capacitações internas sem envolvimento de recursos tendem a apresentar exposição menor ou nenhuma.

A tabela a seguir apresenta as categorias de risco de integridade reconhecidas no contexto do setor público federal. Ela serve como lista de verificação e não como obrigação de preencher todas as linhas. O que é obrigatório é a verificação ativa, ou seja, o Gestor de Risco deve percorrer as categorias, avaliar se alguma se aplica ao OP e documentar a conclusão, seja ela positiva ou negativa. Ignorar essa verificação é o verdadeiro problema, pois os riscos de integridade raramente aparecem espontaneamente nas Matrizes porque são desconfortáveis de nomear. Nomeá-los é o primeiro passo para gerenciá-los.

Quando um risco de integridade for identificado com RR acima do apetite ao risco, a unidade deve comunicar imediatamente a AECI, que avaliará a necessidade de acionar os mecanismos do Programa Empreendendo Integridade e, se cabível, os órgãos de controle competentes.

Quadro 26 - Riscos de Integridade

Risco de Integridade	Evento Relacionado
Uso ou manipulação indevida de dados/informações	Acesso ou restrição indevida, alterações, divulgações confidenciais ou uso irregular de dados e informações.

Risco de Integridade	Evento Relacionado
Desvio ou usufruto indevido de recursos materiais	Subtração ou desvio de finalidade de bens e recursos logísticos da Administração Pública.
Desvio de recursos humanos	Exercício de funções incompatíveis com o cargo ou atribuições de maior complexidade sem acréscimo salarial.
Corrupção, fraude e uso irregular de verbas públicas	Atos lesivos ao patrimônio público, atentatórios aos princípios da Administração ou aos compromissos internacionais do Brasil.
Nepotismo	Uso do poder do cargo para nomear, contratar ou favorecer parentes.
Conflito de interesses	Situações em que interesses privados influenciam de forma imprópria o desempenho da função pública.
Ameaças à isenção técnica	Interferências prejudiciais na autonomia técnica dos servidores.
Assédio ou discriminação	Condutas abusivas que degradem o ambiente de trabalho ou atentem à dignidade das pessoas.

7. DOCUMENTAÇÃO, INSTRUMENTOS E FLUXO PROCESSUAL

7.1. Instrumentos do Ciclo de Gestão de Riscos

A gestão de riscos só existe institucionalmente se estiver documentada. Registros atualizados, instrumentos padronizados e rastreabilidade processual são o que transforma análises informais em evidências válidas para fins de auditoria, prestação de contas e melhoria contínua. Esta seção descreve os instrumentos que compõem o ciclo de gestão de riscos do MEMP, o fluxo processual no SEI e as orientações para proteção das informações produzidas. Todos os instrumentos listados aqui estão disponibilizados em formato eletrônico pela AECI e devem ser utilizados de forma padronizada por todas as unidades, garantindo que os resultados sejam comparáveis e consolidáveis na Carteira Institucional de Riscos.

Quadro 27 - Instrumentos do Ciclo de Gestão de Riscos

Instrumento	Descrição
Formulário de Indicação de OPs (Anexo I)	Registro formal da indicação do OP pela unidade, com fundamentação da escolha e validação do Gestor de Risco.
Planilha para Gestão de Riscos (Anexo II)	Instrumento central do processo, com abas para: análise SWOT e Matriz de riscos.
Plano de Resposta ao Risco (Anexo III)	Documento de formalização das ações de tratamento, com responsável, prazo, indicador e custo estimado.
Relatório Gerencial de Riscos (AECI)	Relatório semestral consolidado com o status da carteira de riscos do MEMP e recomendações ao CGE.
Resolução/Ata do CGE	Registro das deliberações sobre gestão de riscos nas reuniões do Comitê de Governança Estratégica.

7.2. Fluxo Processual no SEI

Toda a documentação relativa ao ciclo de gestão de riscos deverá ser registrada em processo SEI específico para cada OP selecionado. A estrutura documental mínima de cada processo SEI deve conter:

a) Formulário de Indicação do OP (com ciência do Gestor de Risco);
b) Planilha para Gestão de Riscos preenchida (com aba SWOT e Matriz de Riscos);
c) Plano de Resposta ao Risco (se aplicável, com validação do Gestor de Risco);
d) Atualizações periódicas do monitoramento (a cada Ponto de Controle da unidade); e
e) Relatório Gerencial semestral da AECI (referência ao processo da unidade).

7.3. Proteção das Informações

A Carteira Institucional de Riscos, os Planos de Resposta e demais documentos do ciclo de gestão de riscos podem conter informações sensíveis sobre vulnerabilidades institucionais, controles internos em operação e exposições a riscos ainda não mitigados. A divulgação indevida dessas informações pode comprometer a eficácia dos próprios controles ou expor o MEMP a riscos adicionais.

Recomenda-se que todos os processos SEI relativos à gestão de riscos sejam autuados com nível de acesso **Restrito**, com a hipótese legal "Documento Preparatório" (art. 7º, § 3º, da Lei nº 12.527/2011 – Lei de Acesso à Informação), durante todo o ciclo de gestão. Essa hipótese aplica-se porque a Carteira de Riscos e os Planos de Resposta constituem instrumentos de trabalho interno que subsidiam decisões ainda em curso, não configurando ato decisório final.

O nível de acesso Restrito garante que somente servidores com permissão expressa – integrantes da unidade responsável, Gestores de Risco, AECI e membros do CGE – possam visualizar e editar os documentos. O compartilhamento com outros servidores deverá ser feito mediante concessão de acesso individual no próprio SEI, com registro do motivo.

Após a deliberação do CGE e a publicação do Relatório Gerencial semestral, a AECI poderá produzir versão resumida do Relatório com nível de acesso Público, para fins de transparência ativa, preservando as informações operacionais sensíveis nos processos restritos de origem.

A definição do nível de acesso é responsabilidade do servidor que autua o processo, cabendo à AECI orientar as unidades em casos de dúvida quanto à classificação adequada.

8. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31010:2021 – Gestão de Riscos: Técnicas para o Processo de Avaliação de Riscos. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31073:2023 – Gestão de Riscos: Vocabulário. Rio de Janeiro: ABNT, 2023.

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: DOU, 2017.

BRASIL. Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte. Portaria MEMP nº 390, de 16 de dezembro de 2025. Institui a Política de Gestão de Riscos no âmbito do MEMP. Brasília: DOU, 2025.

BRASIL. Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte. Plano Estratégico MEMP 2024-2027. Brasília: MEMP, 2024.

BRASIL. Ministério do Planejamento, Orçamento e Gestão; Controladoria-Geral da União. Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016. Brasília: DOU, 2016.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise Risk Management – Integrating with Strategy and Performance. 2017.

INSTITUTE OF INTERNAL AUDITORS (IIA). Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. Janeiro de 2013.

INSTITUTE OF INTERNAL AUDITORS (IIA). Modelo das Três Linhas do IIA. 2020.

TRIBUNAL DE CONTAS DA UNIÃO. Referencial Básico de Gestão de Riscos. Brasília: TCU, SEGECEX/COGER, abril de 2018.

9. ANEXOS

ANEXO I – FORMULÁRIO DE INDICAÇÃO DE OBJETOS PRIORITÁRIOS

FORMULÁRIO DE INDICAÇÃO DE OBJETOS PRIORITÁRIOS – MEMP	
Ciclo de Gestão de Riscos: _____ / _____	Data de Preenchimento: ___/___/_____
Campo	**Preenchimento**
1. Unidade Administrativa Responsável ( ) Secretaria Nacional: _____ ( ) Diretoria: _____ ( ) Departamento / Outra unidade: _____	
2. Nome do OP (projeto ou processo):	
3. Tipo de OP:	( ) Projeto ( ) Processo ( ) Programa ( ) Política Pública ( ) Contrato/Parceria ( ) Sistema ( ) Atividade Institucional ( ) Outro: _____
4. Objetivo do OP:	
5. Relação com o Plano Estratégico MEMP 2024-2027:	
6. Critério(s) aplicável(is): ( ) I – Materialidade ( ) II – Criticidade ( ) III – Relevância ( ) IV – Inovação	
7. Justificativa da escolha:	
8. Responsável pelo preenchimento: Nome: _____ Cargo/Função: _____	
9. Validação do Gestor de Risco (CCE/FCE nível 13 ou superior): Nome: _____ Assinatura: _____ Data: _____/_____/_____	

ANEXO II – PLANILHA PARA GESTÃO DE RISCOS (ESTRUTURA)

A Planilha para Gestão de Riscos é o instrumento central do processo e deverá ser disponibilizada pela AECI em formato de planilha eletrônica, garantindo que todas as unidades utilizem as mesmas escalas e fórmulas de cálculo automático. O preenchimento é de responsabilidade da própria unidade organizacional, com coordenação da equipe e validação obrigatória do Gestor de Risco antes de qualquer encaminhamento à AECI.

A AECI supervisiona a qualidade do preenchimento e consolida as informações na Carteira Institucional de Riscos do MEMP. A planilha é composta pelas seguintes abas:

Aba 1 – Identificação do OP e Análise SWOT

Campo	Orientação de Preenchimento
Nome e Descrição do OP	Descrever o projeto/processo selecionado e seu objetivo institucional.
Objetivo do OP	Descrever o objetivo principal do OP. (Exemplo: Conceder crédito aos MEIs, Microempresas e Empresas de Pequeno Porte)
Forças (Strengths)	Listar características internas favoráveis (recursos, competências, processos, cultura).
Fraquezas (Weaknesses)	Listar vulnerabilidades internas que podem amplificar riscos (lacunas de recursos, processos, sistemas, capacitação).
Oportunidades (Opportunities)	Listar fatores externos que podem ser aproveitados (tendências, parcerias, tecnologias).
Ameaças (Threats)	Listar fatores externos que podem introduzir dificuldades (mudanças regulatórias, fatores econômicos, sociais, políticos).

Aba 2 – Identificação e Análise de Riscos e Controles

Coluna	Descrição
A - Evento de Risco	Descrição do risco identificado (o que pode acontecer).
B - Categoria	Estratégico / Operacional / Conformidade / Financeiro / Imagem / Integridade / TI.
C - Fonte de Risco	Descrição das Fontes do Risco com base na aba "Fontes de Risco"
D - Possíveis Causas	Fontes e vulnerabilidades que podem originar o risco.
E - Possíveis Consequências	Impactos potenciais sobre o objetivo do OP.
F - Impacto (I)	Nota conforme escala: 1 (Muito Baixo), 2, 5, 8, 10 (Muito Alto).
G - Probabilidade (P)	Nota conforme escala: 1 (Muito Baixa), 2, 5, 8, 10 (Muito Alta).

Coluna	Descrição
H - Risco Inerente (RI)	Calculado automaticamente: RI = P × I.
I - Nível do RI	Classificação automática: Baixo / Médio / Alto / Extremo.
J - Controles Existentes	Listar políticas, procedimentos e sistemas que já mitigam o risco.
K/L – Avaliação Preliminar do Controle	Avaliação dos controles desenhados para o respectivo risco (Inexistente / Fraco / Mediano / Satisfatório / Forte).
I - Risco de Controle (RC)	Calculado automaticamente conforme escala de avaliação.
M - Risco Residual (RR)	Calculado automaticamente: RR = RI × RC.
N - Nível do RR	Classificação automática: Baixo / Médio / Alto / Extremo.
O - Apetite	Nível máximo de risco aceito pela unidade para o OP (Baixo / Médio / Alto / Extremo).
P - Opção de Tratamento	Aceitar / Mitigar / Evitar / Transferir / Explorar.

ANEXO III – PLANO DE RESPOSTA AO RISCO

PLANO DE RESPOSTA AO RISCO – MEMP					
Unidade: _____ OP: _____ Gestor de Risco: _____ Data de elaboração: ___/___/_____					
A – Evento de Risco	**B – Opção de Tratamento**	**C – Ações de Tratamento**	**D – Responsável**	**E – Início**	**F – Término**
(Descreva o risco)	(Mitigar / Evitar / Transferir / Explorar)	(Ações específicas, controles a implantar ou modificar)	(Área/servidor responsável)	(dd/mm/aa)	(dd/mm/aa)

G – Responsável pelo Monitoramento	**H – Periodicidade do Monitoramento**	**I – Comprovação da Implementação (links, normativos, sistemas)**
(Área/servidor)	(Mensal / Trimestral / Semestral)	(Registrar evidências)

Validação do Gestor de Risco: _____ Data: ___/___/_____

Ciência da Autoridade Superior: _____ Data: ___/___/_____

ANEXO IV – QUESTIONÁRIO DE AVALIAÇÃO DA MATURIDADE EM GESTÃO DE RISCOS

Este questionário deve ser respondido anualmente, de forma independente, pela Secretaria-Executiva (SE), pela AECI e pelas Unidades. No ciclo inaugural (2026), apenas SE e AECI respondem. A partir de 2027, as unidades que completaram ao menos um ciclo completo de OPs também respondem. Os resultados são consolidados pela AECI e apresentados ao CGE.

Identificação		Ciclo / Ano	
Unidade / Respondente:		Data de preenchimento:	___/___/_____
Papel do respondente:	( ) Unidade ( ) Secretaria-Executiva ( ) AECI		

Escala de Avaliação

Nota	Nível	Significado
1	Inexistente	Prática não existe ou nunca foi implementada.
2	Inicial	Prática existe de forma isolada e informal.
3	Em desenvolvimento	Prática existe e está sendo estruturada, mas ainda incompleta.
4	Definido	Prática formalizada e aplicada consistentemente.
5	Otimizado	Prática consolidada, monitorada e em melhoria contínua.

Instruções: Para cada pergunta, atribua uma nota de 1 a 5 conforme a escala acima. Registre na coluna 'Evidências / Observações' os documentos, sistemas ou fatos que sustentam a nota atribuída. Em caso de dúvida, atribua a nota mais conservadora.

DIMENSÃO 1 - AMBIENTE (Liderança, Políticas e Pessoas)

Nº / Pergunta de Avaliação	Unidade (1–5)	SE (1–5)	AECI (1–5)	Evidências / Observações
1.1 - A Alta Administração demonstra comprometimento formal com a gestão de riscos (declarações, participação em reuniões, cobrança de resultados)?				
1.2 - Existe política de gestão de riscos formalmente aprovada e divulgada para toda a unidade/MEMP?				

Nº / Pergunta de Avaliação	Unidade (1–5)	SE (1–5)	AECI (1–5)	Evidências / Observações
1.3 - Os papéis e responsabilidades relacionados à gestão de riscos estão claramente definidos e comunicados (inclusive Gestores de Risco e AECI)?				
1.4 - Os servidores receberam capacitação em gestão de riscos nos últimos 12 meses?				
1.5 - Existe cultura de reporte de riscos? Os servidores se sentem à vontade para identificar e comunicar riscos sem receio?				
SUBTOTAL (máximo 25 pontos)	___	___	___	

DIMENSÃO 2 - PROCESSOS (Identificação, Avaliação, Tratamento e Monitoramento)

Nº / Pergunta de Avaliação	Unidade (1–5)	SE (1–5)	AECI (1–5)	Evidências / Observações
2.1 - A unidade/MEMP realiza identificação sistemática de riscos para seus objetos prioritários (OPs)?				
2.2 - Os riscos identificados são analisados e avaliados com base em critérios de probabilidade e impacto?				
2.3 - Existem planos de resposta formalizados para os riscos classificados acima do apetite ao risco?				
2.4 - Os controles internos existentes são avaliados quanto à sua eficácia no processo de gestão de riscos?				
2.5 - O monitoramento dos riscos e dos planos de tratamento é realizado periodicamente e documentado?				
2.6 - Os resultados do processo de gestão de riscos são registrados em instrumentos formais (planilha, SEI)?				
SUBTOTAL (máximo 30 pontos)	___	___	___	

DIMENSÃO 3 - PARCERIAS (Integração e Coordenação)

Nº / Pergunta de Avaliação	Unidade (1–5)	SE (1–5)	AECI (1–5)	Evidências / Observações
3.1 - A unidade/MEMP articula-se com a AECI no ciclo de gestão de riscos (seleção de OPs, análises, relatórios)?				
3.2 - As informações de riscos são compartilhadas tempestivamente entre as três linhas de Gestão de Riscos?				
3.3 - As recomendações da CGU e do TCU são consideradas como insumo para identificação de riscos?				
3.4 - Há troca de experiências e boas práticas em gestão de riscos com outras unidades do MEMP ou outros órgãos?				
SUBTOTAL (máximo 20 pontos)	___	___	___	

DIMENSÃO 4 - RESULTADOS (Efetividade e Aprendizado)

Nº / Pergunta de Avaliação	Unidade (1–5)	SE (1–5)	AECI (1–5)	Evidências / Observações
4.1 - A gestão de riscos contribuiu para a prevenção de problemas ou irregularidades nos últimos 12 meses?				
4.2 - As lições aprendidas de riscos materializados são incorporadas ao processo de identificação no ciclo seguinte?				
4.3 - Os resultados da gestão de riscos são reportados à Alta Administração e ao CGE de forma regular?				
4.4 - A gestão de riscos influencia decisões estratégicas e operacionais da unidade/MEMP?				
SUBTOTAL (máximo 20 pontos)	___	___	___	

Consolidação dos Resultados

Dimensão	Total Unidade	Total SE	Total AECI	Média Unidade	Média SE/AECI
D1 — Ambiente	/25	/25	/25		
D2 — Processos	/30	/30	/30		
D3 — Parcerias	/20	/20	/20		
D4 — Resultados	/20	/20	/20		
TOTAL GERAL	**/95**	**/95**	**/95**		

Nível de Maturidade Global

Média Consolidada	Nível de Maturidade	Descrição
1,0 a 1,9	Nível 1 - Inicial	Práticas informais e não sistematizadas. Sem política ou metodologia formal.
2,0 a 2,9	Nível 2 - Em desenvolvimento	Política existente, implementação parcial. Metodologia em construção.
3,0 a 3,9	Nível 3 - Definido	Metodologia formalizada e aplicada consistentemente em toda a organização.
4,0 a 4,9	Nível 4 - Gerenciado	GR integrada ao planejamento. Indicadores de desempenho ativos e monitorados.
5,0	Nível 5 - Otimizado	Cultura consolidada. Benchmarking e inovação contínua. Melhoria sem indução externa.

Nível apurado neste ciclo: _____ Nível apurado no ciclo anterior: _____ Variação: _____

Plano de Melhoria para o Próximo Ciclo

Com base nas dimensões com menor pontuação, a unidade / SE / AECI devem registrar as ações prioritárias de melhoria para o próximo ciclo:

Dimensão com maior gap	Ação prioritária de melhoria	Responsável	Prazo

Validação da AECI: _____ Data: ___/___/_____

Ciência da SE: _____ Data: ___/___/_____

Apresentado ao CGE em: ___/___/_____ Reunião nº: _____

ANEXO V – Política de Gestão de Riscos

POLÍTICA DE GESTÃO DE RISCOS DO MEMP –

PORTARIA MEMP Nº 390, DE 16 DE DEZEMBRO DE 2025

Institui a Política de Gestão de Riscos no âmbito do Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte.

O MINISTRO DE ESTADO DO EMPREENDEDORISMO, DA MICROEMPRESA E DA EMPRESA DE PEQUENO PORTE, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição Federal, e considerando o disposto no Decreto nº 12.694, de 22 de outubro de 2025; no art. 19 do Decreto nº 9.203, de 22 de novembro de 2017; no Decreto nº 11.529, de 16 de maio de 2023; na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016; e no art. 1º da Portaria CGU nº 57, de 4 de janeiro de 2019, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Gestão de Riscos no âmbito do Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte (MEMP), com o intuito de estabelecer objetivos, princípios, diretrizes, conceitos, responsabilidades e mecanismos para integração da gestão de riscos aos processos organizacionais, em todos os níveis e áreas do Ministério.

Art. 2º Para os fins desta Portaria, considera-se:

I - Risco: possibilidade de ocorrência de um evento que poderá prejudicar o cumprimento dos objetivos institucionais;

II - Apetite ao Risco: nível de risco que a organização está disposta a aceitar na busca de seus objetivos;

III - Controles Internos da Gestão: conjunto de regras, procedimentos, diretrizes, protocolos e rotinas destinados a evitar, mitigar, transferir, compartilhar ou aceitar riscos e oferecer segurança razoável para a consecução da missão institucional;

IV - Gestão de Riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela Alta Administração, que sistematiza, estrutura e coordena as atividades de gerenciamento de riscos da organização;

V - Gerenciamento de Riscos: processo destinado a identificar, analisar, avaliar, tratar, monitorar e comunicar os potenciais eventos ou situações que possam impactar o alcance dos objetivos da instituição; e

VI - Plano de Respostas aos Riscos: documento que contém o conjunto de ações necessárias para adequar os níveis de riscos de determinado processo, considerando o custo-benefício da implantação dos controles.

CAPÍTULO II

DOS OBJETIVOS

Art. 3º A Política de Gestão de Riscos do MEMP tem por objetivo:

I - subsidiar a tomada de decisão com base em evidências e na análise sistemática de riscos, apoiando o alcance dos objetivos estratégicos e institucionais;

II - fortalecer os controles internos da gestão, contribuindo para a melhoria contínua dos processos e da integridade institucional;

III - promover uma cultura organizacional voltada à gestão proativa de riscos e oportunidades, envolvendo todas as unidades do Ministério;

IV - aprimorar a governança pública, assegurando transparência, accountability e sustentabilidade das políticas e programas;

V - facilitar a identificação e o tratamento de ameaças que possam comprometer a entrega de resultados à sociedade;

VI - reforçar a prevenção de riscos de integridade, privilegiando ações preventivas e educativas;

VII - aumentar a capacidade institucional de adaptação às mudanças do ambiente interno e externo;

VIII - agregar valor à gestão e às políticas públicas, melhorando o processo decisório e o tratamento de riscos;

IX - fomentar decisões baseadas em riscos e evidências, integrando a gestão de riscos aos processos de planejamento, financeiro, orçamentário, compras e monitoramento; e

X - promover a cultura da ética, integridade e respeito aos princípios da Administração Pública.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º A gestão de riscos do MEMP observará os seguintes princípios:

I - Alinhamento estratégico e proteção do interesse público: a gestão de riscos deve estar alinhada ao planejamento estratégico e aos objetivos institucionais do MEMP, protegendo o interesse público por meio da definição clara de apetite e tolerância a riscos que equilibrem inovação, efetividade e responsabilidade fiscal;

II - Decisão baseada em evidências: o mapeamento de riscos deve ser utilizado como ferramenta estratégica para subsidiar decisões, priorizar ações, orientar a alocação eficiente de recursos e aprimorar o desempenho institucional;

III - Aderência à boa governança, integridade e liderança: a gestão de riscos deve estar integrada às práticas de governança, com liderança ativa e comprometida da Alta Administração na implementação, monitoramento e aperfeiçoamento dos controles internos e da cultura de integridade;

IV - Abordagem estruturada e melhoria contínua: deve adotar metodologia sistemática, cíclica e oportuna, baseada nas melhores informações disponíveis, incorporando lições aprendidas e promovendo a evolução dos processos organizacionais;

V - Integração e transversalidade: a gestão de riscos deve ser parte integrante dos processos organizacionais, políticas públicas e atividades operacionais do Ministério, favorecendo a coerência entre planejamento, execução e monitoramento;

VI - Proporcionalidade e relevância: deve ser compatível com a natureza, a complexidade e o impacto dos riscos, priorizando aqueles que possam comprometer significativamente os resultados e objetivos institucionais;

VII - Base em informação qualificada e transparência: deve apoiar-se em dados e análises de qualidade, assegurando rastreabilidade, documentação adequada e comunicação clara aos tomadores de decisão;

VIII - Cultura organizacional empreendedora: deve valorizar os aspectos humanos, estimular a postura proativa, a inovação responsável, o aprendizado contínuo e a accountability em todos os níveis hierárquicos;

IX - Continuidade e tempestividade: deve ser realizada de forma contínua, preventiva e dinâmica, permitindo resposta rápida a mudanças no contexto interno e externo; e

X - Agregação de valor e resiliência institucional: deve agregar valor à atuação do MEMP, fortalecer os controles internos e aumentar a capacidade de adaptação e resiliência da instituição diante de incertezas e desafios.

CAPÍTULO IV

DAS DIRETRIZES

Art. 5º A gestão de riscos no âmbito do Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte - MEMP deverá ser integrada ao planejamento estratégico, ao Programa de Integridade, aos processos organizacionais, projetos, contratações e políticas públicas, de forma articulada e coerente com os objetivos institucionais.

Art. 6º A implementação da gestão de riscos será realizada de forma gradual e progressiva, observada a capacidade institucional das unidades organizacionais, priorizando:

I - processos finalísticos;

II - projetos estratégicos;

III - políticas públicas de maior impacto; e

IV - áreas com maior exposição a riscos ou fragilidades de controle identificadas.

Art. 7º O modelo de gestão de riscos e controles internos do MEMP deverá observar os princípios, conceitos e orientações:

I - do Committee of Sponsoring Organizations of the Treadway Commission (COSO);

II - da ABNT NBR ISO 31000:2018, da ABNT NBR ISO 31010 e da ABNT NBR ISO 31073;

III - da Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016; e

IV - do Referencial Básico de Gestão de Riscos do Tribunal de Contas da União (TCU).

Art. 8º O Comitê de Governança Estratégica (CGE) poderá propor ou deliberar sobre a inclusão de processos, temas ou projetos prioritários na agenda de gestão de riscos do MEMP, para fins de acompanhamento, monitoramento e priorização de controles.

Art. 9º A definição, revisão e comunicação do apetite e da tolerância ao risco são de responsabilidade da Alta Administração, devendo orientar o processo decisório, a priorização de ações e a alocação de recursos.

Art. 10. O desenvolvimento contínuo das competências relacionadas à gestão de riscos será promovido por meio:

I - do Plano de Desenvolvimento de Pessoas (PDP);

II - da oferta de cursos, trilhas de capacitação e oficinas internas; e

III - da articulação com escolas de governo, universidades e órgãos de controle.

Art. 11. A utilização de ferramentas de apoio à gestão de riscos deverá priorizar o uso de software livre ou Software Público Brasileiro ou, na sua ausência, soluções homologadas pela Secretaria Executiva e pela Assessoria Especial de Controle Interno.

Art. 12. Todas as etapas do processo de gestão de riscos deverão ser documentadas, registradas e atualizadas em matriz institucional, assegurando:

I - rastreabilidade;

II - transparência; e

III - disponibilidade das informações às instâncias competentes.

Art. 13. A gestão de riscos será orientada pela melhoria contínua, considerando os resultados de monitoramento, auditorias, avaliações de maturidade, lições aprendidas e mudanças no contexto institucional.

§ 1º A identificação, a análise, a avaliação, o tratamento e o monitoramento dos riscos deverão ocorrer de forma periódica, conforme metodologia aprovada, observada, no mínimo, a revisão anual dos riscos institucionais e estratégicos.

§ 2º O desempenho da gestão de riscos será mensurado por meio de indicadores definidos na metodologia institucional, considerando, entre outros aspectos, a efetividade dos controles e a evolução dos níveis de risco.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 14. O Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte (MEMP) adota o Modelo das Três Linhas de Governança, proposto pelo Institute of Internal Auditors (IIA) e referendado pelo Tribunal de Contas da União (TCU), para a definição das competências e responsabilidades relativas à gestão de riscos e aos controles internos.

Parágrafo único. São instâncias responsáveis pelo Sistema de Gestão de Riscos e Controles Internos do MEMP (SGRCI-MEMP):

I - o Comitê de Governança Estratégica (CGE);

II - a Secretaria-Executiva (SE);

III - a Assessoria Especial de Controle Interno (AECI);

IV - as Unidades Organizacionais; e

V - os Gestores de Risco.

Art. 15. Compete ao Comitê de Governança Estratégica (CGE), com o apoio da Secretaria Executiva e da AECI, nos termos do § 2º do art. 23 da Instrução Normativa Conjunta MP/CGU nº 1, de 2016:

I- promover práticas e princípios de conduta e padrões de comportamento;

II- institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;

III- promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;

IV- garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;

V- promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;

VI- promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;

VII- aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;

VIII- supervisionar o mapeamento e a avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;

IX- liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo o suporte necessário para sua efetiva implementação no órgão ou entidade;

X- estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada ao nível de unidade, política pública, ou atividade;

XI- aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;

XII- emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos; e

XIII- monitorar as recomendações e orientações deliberadas pelo Comitê.

Art. 16. Compete à Secretaria-Executiva (SE):

I - submeter ao CGE a Política e a Metodologia de Gestão de Riscos e suas revisões;

II - garantir a integração da gestão de riscos com o planejamento estratégico, o orçamento e as

principais iniciativas do MEMP;

III - acompanhar a evolução dos níveis de risco e a efetividade dos controles, a partir de relatórios elaborados pela AECI;

IV - articular-se com as unidades organizacionais para assegurar a execução das ações de gestão de riscos; e

V - expedir atos complementares para disciplinar a aplicação desta Política, observadas as diretrizes estabelecidas nesta Portaria.

Art. 17. Compete à Assessoria Especial de Controle Interno (AECI):

I - coordenar o Sistema de Gestão de Riscos e Controles Internos do MEMP;

II - elaborar, revisar e divulgar a Política e a Metodologia de Gestão de Riscos e Controles Internos;

III - assessorar as unidades na aplicação da metodologia de gestão de riscos;

IV - monitorar a carteira institucional de riscos e emitir relatórios periódicos de acompanhamento e recomendações;

V - coordenar a gestão dos riscos de integridade, em articulação com o Programa Empreendendo Integridade; e

VI - promover ações de capacitação e sensibilização em governança, riscos e integridade.

Art. 18. Compete às Unidades Organizacionais do MEMP:

I - implementar mecanismos de gestão de riscos em seus processos, projetos e atividades;

II - identificar, avaliar e classificar riscos que possam comprometer as políticas e ações sob sua responsabilidade;

III - adotar medidas de tratamento e mitigação dos riscos identificados;

IV - monitorar periodicamente os riscos e manter os registros atualizados na matriz institucional; e decisão.

V - reportar à AECI e ao CGE as informações necessárias ao acompanhamento e à tomada de

Art. 19. Compete aos Gestores de Risco:

I - validar os resultados das avaliações de riscos realizadas;

II - monitorar os riscos e garantir a execução dos planos de tratamento;

III - disponibilizar à AECI e ao CGE informações atualizadas sobre riscos e controles;

IV - promover a cultura de gestão de riscos no âmbito de sua unidade; e

V - garantir o engajamento das equipes nas etapas de identificação e tratamento dos riscos.

Parágrafo único. Os Gestores de Risco deverão ser ocupantes de CCE ou FCE de nível 13 ou superior, com autoridade para orientar e validar as ações de gestão de riscos em suas unidades.

Art. 20. Compete a todos os servidores do MEMP:

I - atuar com visão preventiva, identificando e comunicando riscos em suas atividades;

II - zelar pela observância dos princípios da gestão de riscos, integridade e controle interno; e

III - colaborar para o aperfeiçoamento contínuo da governança e da prestação de serviços públicos de qualidade.

CAPÍTULO VI

DO PROCESSO DE GESTÃO DE RISCOS

Art. 21. O processo de gestão de riscos do MEMP segue os princípios da ABNT NBR ISO 31000:2018 e do Referencial Básico de Gestão de Riscos do TCU, estruturando-se nas seguintes etapas:

I - Comunicação e Consulta: visa assegurar o diálogo permanente entre as partes interessadas, internas e externas, em todas as fases do processo de gestão de riscos, garantindo que as percepções e informações sobre riscos, controles e decisões sejam compartilhadas de forma tempestiva e transparente, fortalecendo o entendimento comum sobre responsabilidades e prioridades;

II - Estabelecimento do Contexto: define o ambiente interno e externo em que o MEMP atua, considerando fatores estratégicos, operacionais, legais, tecnológicos, econômicos, sociais e ambientais, sendo definidos, nessa etapa, os objetivos, os critérios de risco, o apetite e a tolerância ao risco, além dos limites de aceitação;

III - Identificação de Riscos: consiste em reconhecer e descrever os eventos potenciais que possam impactar a consecução dos objetivos institucionais, devendo ser considerados riscos estratégicos, operacionais, financeiros, de integridade, tecnológicos, ambientais e de imagem, com a indicação das causas, eventos, consequências e controles existentes;

IV - Análise de Riscos: avalia a probabilidade de ocorrência e a magnitude do impacto dos riscos identificados, levando em conta a eficácia dos controles atuais, resultando na determinação do nível de risco inerente (antes dos controles) e do nível de risco residual (após controles);

V - Avaliação de Riscos: compara o nível de risco residual com os critérios de apetite e tolerância definidos pela Alta Administração, classificando os riscos por prioridade (baixo, médio, alto, crítico) e selecionando aqueles que demandam planos de tratamento;

VI - Tratamento de Riscos: envolve a definição e a implementação de medidas para modificar o risco, por meio das seguintes estratégias:

a) evitar o risco;

b) reduzir a probabilidade ou o impacto;

c) transferir ou compartilhar (ex.: parcerias, seguros, contratos);

d) aceitar o risco, quando dentro dos limites definidos; ou

e) explorar o risco como oportunidade de inovação ou melhoria;

VII - Monitoramento e Revisão: corresponde à verificação contínua da efetividade dos controles, das ações e da evolução dos riscos ao longo do tempo, incluindo a revisão periódica das matrizes de risco, a atualização dos planos de ação e a comunicação de mudanças significativas ao Comitê de Governança Estratégica (CGE); e

VIII - Registro e Reporte: abrange o registro estruturado de todas as informações relativas ao processo de gestão de riscos, incluindo riscos identificados, análises, planos de ação, decisões e relatórios, devendo o reporte periódico ser encaminhado à AECI e ao CGE, e, quando aplicável, à Alta Administração.

Parágrafo único. As ações definidas na etapa de Tratamento de Riscos (inciso VI do caput) deverão ser formalizadas em Plano de Resposta ao Risco, contendo a indicação do responsável, o prazo de execução e o indicador de acompanhamento.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 22. A Política de Gestão de Riscos deverá ser revisada a cada dois anos, ou sempre que ocorrerem mudanças significativas no ambiente institucional.

Art. 23. Os casos omissos serão resolvidos pela Alta Administração, com o apoio técnico da AECI e do CGE.

Art. 24. Esta Portaria entra em vigor após decorridos 30 (trinta) dias de sua publicação.

Art. 25. Esta Portaria será disponibilizada no portal de governança do MEMP.