

Referencial de Gestão de Riscos

Conselho Nacional do Ministério Público



EXPEDIENTE

2026, Conselho Nacional do Ministério Público

Permitida a reprodução mediante citação da fonte.

COMPOSIÇÃO DO CNMP

Paulo Gustavo Gonet Branco, Presidente do Conselho Nacional do Ministério Público

Fernando da Silva Comin, Conselheiro do CNMP

Ivana Lúcia Franco Cei, Conselheira do CNMP

Edvaldo Nilo de Almeida, Conselheiro do CNMP

Fabiana Costa Oliveira Barreto, Conselheira do CNMP

Karen Luise Vilanova Batista de Souza, Conselheira do CNMP

Greice Fonseca Stocker, Conselheira do CNMP

Thiago Roberto Moraes Diaz, Conselheiro do CNMP

Gustavo Afonso Sabóia Vieira, Conselheiro do CNMP

José de Lima Ramos Pereira, Conselheiro do CNMP

Alexandre Magno Benites de Lacerda, Conselheiro do CNMP

Clementino Augusto Ruffeil Rodrigues, Conselheiro do CNMP

Márcio Barra Lima, Conselheiro do CNMP

Carl Olav Smith, Conselheiro do CNMP

SECRETARIA-GERAL DO CNMP

Carlos Vinicius Alves Ribeiro, Secretário-geral

Michel Betenjane Romano, Secretário-geral Adjunto

ELABORAÇÃO E REVISÃO

Diogo Moreira Chaves Cavalcante, Coordenadoria de Governança e Gestão Estratégica

Luísa de Moura Ferreira Dourado, Coordenadoria de Governança e Gestão Estratégica

Mateus Willig Araujo, Secretário de Governança e Gestão Estratégica Adjunto

Sávio Neves do Nascimento, Secretário de Governança e Gestão Estratégica

SUMÁRIO

1. INTRODUÇÃO.....	4
2. TERMOS, DEFINIÇÕES E TIPOLOGIA DE RISCOS.....	5
2.1 Categorias de riscos.....	6
3. OBJETIVO, ABRANGÊNCIA E PREMISSAS DE ATUALIZAÇÃO.....	7
3.1 Objetivo geral.....	7
3.2 Objetivos específicos.....	7
3.3 Abrangência.....	7
4. GOVERNANÇA DA GESTÃO DE RISCOS.....	8
4.1 Princípios de organização da governança.....	8
4.2 Matriz RACI referencial.....	9
5. METODOLOGIA E PROCESSO DE GESTÃO DE RISCOS.....	11
5.1 Mapa de Riscos.....	12
5.1.1 Uso de ferramentas institucionais e de inteligência artificial.....	12
5.2 Etapa I: Estabelecimento do contexto.....	13
5.3 Etapa II: Identificação dos riscos.....	13
5.4 Etapa III: Análise dos riscos.....	14
5.4.1 Escala de probabilidade.....	14
5.4.2 Escala de impacto.....	15
5.4.3 Nível de risco.....	15
5.4.4 Nível de risco residual.....	16
5.5 Etapa IV: Avaliação de riscos.....	17
5.5.1 Finalidade da avaliação de riscos.....	17
5.5.2 Comparação do risco residual com o apetite a risco.....	18
5.5.3 Avaliação por categoria de risco.....	18
5.5.4 Decisão quanto à resposta ao risco.....	19
5.5.5 Produto e registro da avaliação de riscos.....	19
5.6 Etapa V: Tratamento dos riscos.....	20
5.6.1 Tratamento de ameaças.....	20
5.6.2 Registro das medidas de tratamento no Mapa de Riscos.....	20
5.7 Etapa VI: Monitoramento e análise crítica.....	21
5.7.1 Painel Institucional de Riscos.....	21
5.8 Etapa VII: Comunicação e consulta.....	22
6. ABORDAGEM ESPECÍFICA PARA RISCOS ESTRATÉGICOS.....	23
6.1 Objeto da gestão de riscos estratégicos.....	23
6.2 Papéis e responsabilidades na gestão de riscos estratégicos.....	23
6.3 Abordagem para riscos positivos (oportunidades).....	24
6.3.1 Estabelecimento do contexto de riscos positivos.....	25
6.3.2 Identificação de risco positivo.....	25
6.3.3 Análise de risco positivo.....	25
6.3.4 Avaliação de risco positivo.....	27
6.3.5 Tratamento do risco positivo.....	27
6.3.6 Monitoramento e análise crítica de risco positivo.....	28
6.3.7 Comunicação e consulta de risco positivo.....	28
7. ABORDAGEM PARA AS DEMAIS CATEGORIAS DE RISCOS.....	30
7.1 Objetos de análise.....	30
7.2 Papéis e responsabilidades.....	31
8. INTEGRAÇÃO ENTRE A GESTÃO DE RISCOS E O PLANEJAMENTO INSTITUCIONAL.....	33
8.1 Integração com outros instrumentos institucionais.....	34
REFERÊNCIAS.....	35

1. INTRODUÇÃO

A gestão de riscos é uma ferramenta essencial para a governança do Conselho Nacional do Ministério Público (CNMP). Ela contribui para a integridade, a conformidade, a transparência e o alinhamento com os objetivos estratégicos da instituição. Mais do que cumprir normas, a gestão de riscos é uma prática contínua que ajuda a proteger e gerar valor público, melhorar a tomada de decisões e alcançar os objetivos institucionais.

Este Referencial de Gestão de Riscos aprofunda os conceitos trazidos na Política de Gestão de Riscos do CNMP e apresenta abordagem, os principais componentes, os instrumentos e os recursos necessários para aplicação prática. A Política foi instituída pela Portaria CNMP-PRESI nº 85, de 17 de março de 2026, que substituiu a Portaria nº 45, de 27 de abril de 2017.

Ademais, ele possibilita incorporar a gestão de riscos estratégicos, a integração com o Planejamento Estratégico do CNMP (PE-CNMP), a inclusão de riscos estratégicos e táticos, o uso do Painel Institucional de Riscos e a definição de ciclos de gestão alinhados ao monitoramento do PE-CNMP.

O Referencial mantém as práticas já consolidadas, com os ajustes necessários. Permanecem o processo de gestão de riscos, o uso de critérios de probabilidade e impacto, a realização de registro, comunicação, consulta, monitoramento e análise dos riscos, além da busca por melhoria contínua, com base em boas práticas como a ABNT NBR ISO 31000 e o COSO ERM.



2. TERMOS, DEFINIÇÕES E TIPOLOGIA DE RISCOS

Aplicam-se a este Referencial as definições previstas na Política de Gestão de Riscos do CNMP. Para uso prático, adotam-se as terminologias expostas na tabela a seguir:

Tabela 1: Termos e definições

TERMO	DEFINIÇÃO
Ameaça	Efeito negativo da incerteza sobre os objetivos institucionais.
Apetite a risco	Nível e tipo de risco que o CNMP se dispõe a aceitar, reter ou perseguir na busca por agregar valor aos serviços prestados.
Atitude perante o risco	Abordagem do CNMP para avaliar o risco e, a partir daí, decidir por evitá-lo, retê-lo, assumi-lo, persegui-lo ou dele se afastar, em função dos objetivos institucionais e do apetite a risco.
Causa	Fator ou condição que, isolado ou combinado, dá origem a um evento.
Consequência	Resultado de um evento que afeta os objetivos institucionais, podendo ser negativo ou positivo.
Critérios de risco	Padrão de referência para a avaliação dos riscos.
Evento	Ocorrência, conjunto de ocorrências ou mudança em circunstâncias que pode dar origem a risco.
Facilitador da gestão de riscos	Servidor designado pelo proprietário do risco, com a função de apoiar tecnicamente as atividades de identificação, análise, tratamento, monitoramento e reporte de riscos, sem prejuízo da responsabilidade final atribuída ao proprietário do risco.
Fonte de risco	Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.
Gestão de riscos	Conjunto de atividades coordenadas para subsidiar a tomada de decisão no que se refere a riscos.
Impacto	Magnitude da consequência de um evento sobre os objetivos institucionais.
Mapa de riscos da unidade	Documento que consolida os riscos identificados, analisados, avaliados e tratados no âmbito de cada unidade organizacional, apresentando seus níveis de exposição, causas, consequências, controles existentes, responsáveis e medidas de tratamento, servindo como base para monitoramento contínuo e para integração dos riscos da unidade ao Painel Institucional de Riscos.
Nível de risco	Grau resultante da combinação de probabilidade e impacto do risco, resultando nos níveis: baixo, médio, alto e crítico.
Oportunidade	Efeito positivo da incerteza sobre os objetivos institucionais, decorrente de evento capaz de potencializar resultados e agregar valor, especialmente na consecução dos objetivos estratégicos, caracterizando a face positiva do risco.
Painel institucional de riscos	Ferramenta corporativa que consolida, visualiza e monitora os riscos estratégicos e nos níveis de risco alto e crítico, alimentada pelos Mapas de Riscos das Unidades e por riscos estratégicos identificados pelas instâncias de governança, permitindo análise integrada da exposição institucional, acompanhamento de planos de tratamento, identificação de tendências, apoio à tomada de decisão e comunicação estruturada à Alta Administração.
Plano de gestão de riscos	Ferramenta da gestão de riscos que especifica e detalha a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos.
Probabilidade	Chance de ocorrência de um evento.
Processo de gestão de riscos	Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.
Proprietário do risco	Autoridade responsável pela gestão do risco em sua área de atuação, incumbida de implementar as medidas de tratamento e de reportar às instâncias de governança, podendo delegar a gestão de riscos específicos a responsáveis designados, sem prejuízo de sua responsabilidade final.
Risco	Efeito da incerteza sobre os objetivos institucionais, caracterizado pela possibilidade de ocorrência de eventos, atuais ou futuros, que possam impactar, positiva ou negativamente, o alcance dos objetivos do CNMP.
Risco de conformidade	Aquele decorrente de eventos que ocasionem o descumprimento das normas legais, constitucionais, regulamentares ou contratuais vigentes.
Risco de integridade	Aquele decorrente de eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que possam comprometer os valores e padrões preconizados pelo CNMP, classificando-se como risco reputacional os efeitos sobre a imagem institucional deles decorrentes.
Risco estratégico	Aquele decorrente de eventos que podem afetar a definição ou o alcance dos objetivos estratégicos, da visão e da missão do CNMP, seja de forma positiva, caracterizando uma oportunidade, seja de forma negativa, configurando uma ameaça.

TERMO	DEFINIÇÃO
Risco inerente	Nível de risco ao qual os objetivos estratégicos e táticos, as ações, projetos, iniciativas, ativos e processos de trabalho do CNMP estão sujeitos, desconsiderada a efetividade das medidas de controle ou de tratamento existentes.
Risco operacional	Aquele decorrente de eventos que podem comprometer as atividades do CNMP, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
Risco reputacional	Risco decorrente de eventos que possam comprometer a imagem, a credibilidade e a confiança da sociedade no CNMP.
Risco residual	Risco remanescente após a aplicação dos controles e das medidas de tratamento;
Risco secundário	Risco decorrente da adoção das medidas de controle para um risco inerente ou residual.
Risco tático	Aquele decorrente de eventos que podem afetar a consecução dos objetivos táticos estabelecidos nos painéis de contribuição das unidades, comprometendo a entrega de resultados intermediários necessários ao alcance dos objetivos estratégicos.
Tratamento de riscos	Seleção e implementação de uma ou mais opções para modificar o risco, compreendendo evitar, reduzir (mitigar), transferir ou compartilhar e reter o risco e, no caso de oportunidades, assumir ou aumentar o risco para persegui-las.
Vulnerabilidade	Propriedade intrínseca de algo, resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência.

2.1 Categorias de riscos

As categorias de riscos permitem organizar e classificar os eventos que podem afetar os objetivos institucionais do CNMP, facilitando sua identificação, análise, tratamento e monitoramento. O infográfico a seguir apresenta as principais categorias previstas na Política de Gestão de Riscos, com indicação de sua aplicação no contexto do CNMP e exemplos orientativos para apoiar a compreensão e a padronização da análise pelas unidades.

Figura 1: Categorias de Riscos



3. OBJETIVO, ABRANGÊNCIA E PREMISSAS DE ATUALIZAÇÃO

3.1 Objetivo geral

Estabelecer a metodologia institucional e o processo de gestão de riscos com instrumentos padronizados para identificar, analisar, avaliar, tratar, monitorar, comunicar e revisar riscos no âmbito do CNMP, assegurando alinhamento com a Política de Gestão de Riscos, com o Planejamento Estratégico, com os Painéis de Contribuição, com a integridade, com a conformidade, com os controles internos e com a tomada de decisão orientada a resultados.

3.2 Objetivos específicos

- Reduzir a probabilidade e o impacto de eventos com resultados negativos;
- Implementar procedimentos de contingência para reduzir impactos decorrentes da materialização de riscos;
- Padronizar conceitos, critérios, papéis, responsabilidades, fluxos de comunicação e modelos de registro;
- Integrar a gestão de riscos aos níveis estratégico, tático e operacional, com ênfase nos objetivos estratégicos e nos objetivos estratégicos prioritários definidos anualmente pela Presidência;
- Possibilitar a análise de oportunidades nos riscos estratégicos, quando o evento favorável puder potencializar resultados e agregar valor institucional;
- Assegurar que os Mapas de Riscos das Unidades alimentem o Painel Institucional de Riscos, especialmente quanto aos riscos de nível alto e crítico, às oportunidades e às medidas de tratamento;
- Garantir proporcionalidade, economicidade, rastreabilidade, *accountability* e transparência compatível com a natureza das informações; e
- Promover aprendizado institucional, capacitação continuada e aperfeiçoamento da maturidade em gestão de riscos.

3.3 Abrangência

- Todas as unidades da estrutura organizacional do CNMP, observadas suas competências regimentais e legais;
- Os níveis de gestão estratégico, tático e operacional;
- As categorias de risco estratégico, tático, operacional, de conformidade, de integridade e reputacional;
- As oportunidades, exclusivamente no nível estratégico, quando relacionadas à consecução dos objetivos estratégicos;
- Os objetivos estratégicos e objetivos estratégicos prioritários definidos no PE-CNMP;
- As ações, projetos e processos de trabalho das unidades;
- Os ativos institucionais, incluindo recursos humanos, tecnológicos, informacionais e de infraestrutura; e
- Outros elementos cuja criticidade ou impacto possam comprometer os objetivos institucionais.

4. GOVERNANÇA DA GESTÃO DE RISCOS

A governança da gestão de riscos do CNMP será exercida em três níveis (estratégico, tático e operacional), com papéis complementares, segregação de funções, fluxo de reporte compatível com a materialidade dos riscos e integração com planejamento, orçamento, integridade, conformidade, controles internos e auditoria.

4.1 Princípios de organização da governança

- A Alta Administração direciona, avalia e monitora a gestão de riscos, aprovando a Política, o Plano e o apetite institucional, conforme a governança formalmente estabelecida;
- Os Comitês Temáticos de Governança atuam no nível tático, integrando riscos a planejamento, orçamento e Plano de Gestão, propondo aperfeiçoamentos e acompanhando os riscos sob sua esfera temática;
- A Secretaria de Governança e Gestão Estratégica (SGE) coordena metodologicamente o processo, consolida informações, promove capacitação e assegura alinhamento dos riscos ao PE-CNMP;
- A Unidade Setorial de Integridade (USI) coordena o Programa de Integridade e orienta, articula e acompanha medidas voltadas à prevenção, detecção e mitigação de riscos de integridade, incluindo fraudes, corrupção, desvios éticos e outras situações que possam comprometer a ética, a probidade, a impessoalidade, a transparência e a confiança institucional.
- Os Proprietários de Riscos identificam, analisam, tratam, monitoram e reportam riscos em suas áreas de atuação, podendo designar facilitadores, sem prejuízo de sua responsabilidade final; e
- A Auditoria Interna (AUDIN) atua como avaliação independente, avaliando processos de gestão de riscos, integridade, conformidade, controles internos e governança.

Figura 2: Dimensões da estrutura de governança de gestão de riscos



A Figura 2 apresenta as dimensões da estrutura de governança da gestão de riscos no CNMP, evidenciando a organização dos papéis em nível estratégico, tático e operacional, bem como a atuação independente da Auditoria Interna. Essa representação descreve a lógica geral de funcionamento do modelo,

no qual a governança define diretrizes, prioridades e apetite a risco; as instâncias táticas coordenam, orientam e integram a aplicação da metodologia; e o nível operacional executa a gestão dos riscos nos objetos sob sua responsabilidade.

A partir dessa estrutura, a Tabela 2 detalha as instâncias e os atores funcionais envolvidos em cada dimensão, indicando suas responsabilidades no âmbito do Plano de Gestão de Riscos. Assim, enquanto a figura oferece uma visão panorâmica da arquitetura institucional de governança, a tabela explicita como essa arquitetura se traduz em atribuições práticas, distribuindo responsabilidades pela aprovação, coordenação, execução, monitoramento, reporte e avaliação independente do processo de gestão de riscos.

Tabela 2: Governança de Gestão de Riscos – Instâncias e Responsabilidades

NÍVEL	INSTÂNCIA / ATOR FUNCIONAL	RESPONSABILIDADE
Estratégico	Instância Superior de Governança e Presidência	Aprovar e revisar Política, Plano e apetite a risco; revisar Painel Institucional de Riscos; assegurar integração com o Planejamento Estratégico.
Tático	Comitês Temáticos de Governança	Integrar gestão de riscos aos processos de planejamento, orçamento e Plano de Gestão; propor revisão da Política, do Plano e do apetite; analisar riscos de maior exposição.
Tático	SGE	Coordenar elaboração dos planos de riscos estratégicos, táticos e operacionais; consolidar relatórios anuais; orientar metodologia; apoiar capacitação; assegurar alinhamento ao PE-CNMP.
Tático	USI	Acompanhar institucionalmente, como instância de segunda linha, medidas de prevenção, detecção e mitigação de riscos de integridade, sem prejuízo da responsabilidade das unidades gestoras pela gestão dos riscos sob sua governança.
Operacional	Proprietário de Risco	Identificar, analisar, tratar, monitorar e reportar riscos, elaborar planos de ação e escalar riscos quando necessário.
Operacional	Facilitador (da Gestão) de Riscos	Apoiar tecnicamente a unidade na aplicação da metodologia, registros, evidências, monitoramento e reporte.
Atuação independente	AUDIN	Avaliar, de forma independente, processos de gestão de riscos, integridade, conformidade e efetividade dos controles internos, emitindo recomendações.

4.2 Matriz RACI referencial

A matriz RACI apresentada a seguir possui caráter referencial e tem por finalidade orientar a distribuição de papéis e responsabilidades entre os atores envolvidos no processo de gestão de riscos.

A matriz RACI é uma ferramenta de apoio à definição de papéis e responsabilidades em processos, projetos ou atividades. Seu objetivo é deixar claro quem aprova, quem é responsável pela decisão ou tarefa, quem deve ser consultado e quem precisa ser informado ao longo de determinado fluxo de trabalho.

Sua aplicação deve observar as especificidades do objeto analisado, a complexidade do risco, as competências das unidades envolvidas e o arranjo de governança aplicável ao caso concreto. Assim, a matriz poderá ser ajustada sempre que necessário, desde que preservadas a clareza de responsabilidades, a segregação de funções, a rastreabilidade das decisões e a efetividade do processo de gestão de riscos.

Tabela 3: Matriz RACI referencial

ATIVIDADE	PROPRIETÁRIO DE RISCO	SGE	COMITÊ TEMÁTICO DE GOVERNANÇA	USI	AUDIN	INSTÂNCIA SUPERIOR
Estabelecer contexto	R	C	I	C¹	I	I
Identificar riscos	R	C	I	C¹	I	I
Analisar riscos	R	C	C	C¹	I	I
Avaliar riscos	R	C	C (quando alto/crítico)	C¹	I	I
Tratar riscos	R	C	C/A (quando alto/crítico)	C¹	I	A
Executar tratamento	R	I	I	I	I	I
Monitorar riscos	R	R	R	R¹	I	A
Consolidar Painel Institucional	C	R	C	C	I	I
Plano de Gestão de Riscos	I	R	C	C¹	C	A
Definir o Apetite a Riscos	I	R	A	C	C	A
Avaliação independente	I	C	I	C	R	I
Capacitar envolvidos	R	R	I	I	I	I

Legenda:

R = Responsável pela execução;

R¹ = Responsável, quando se tratar de riscos de integridade;

A = Aprovador;

C = Consultado;

C¹ = Consultado, quando se tratar de riscos de integridade;

I = Informado.



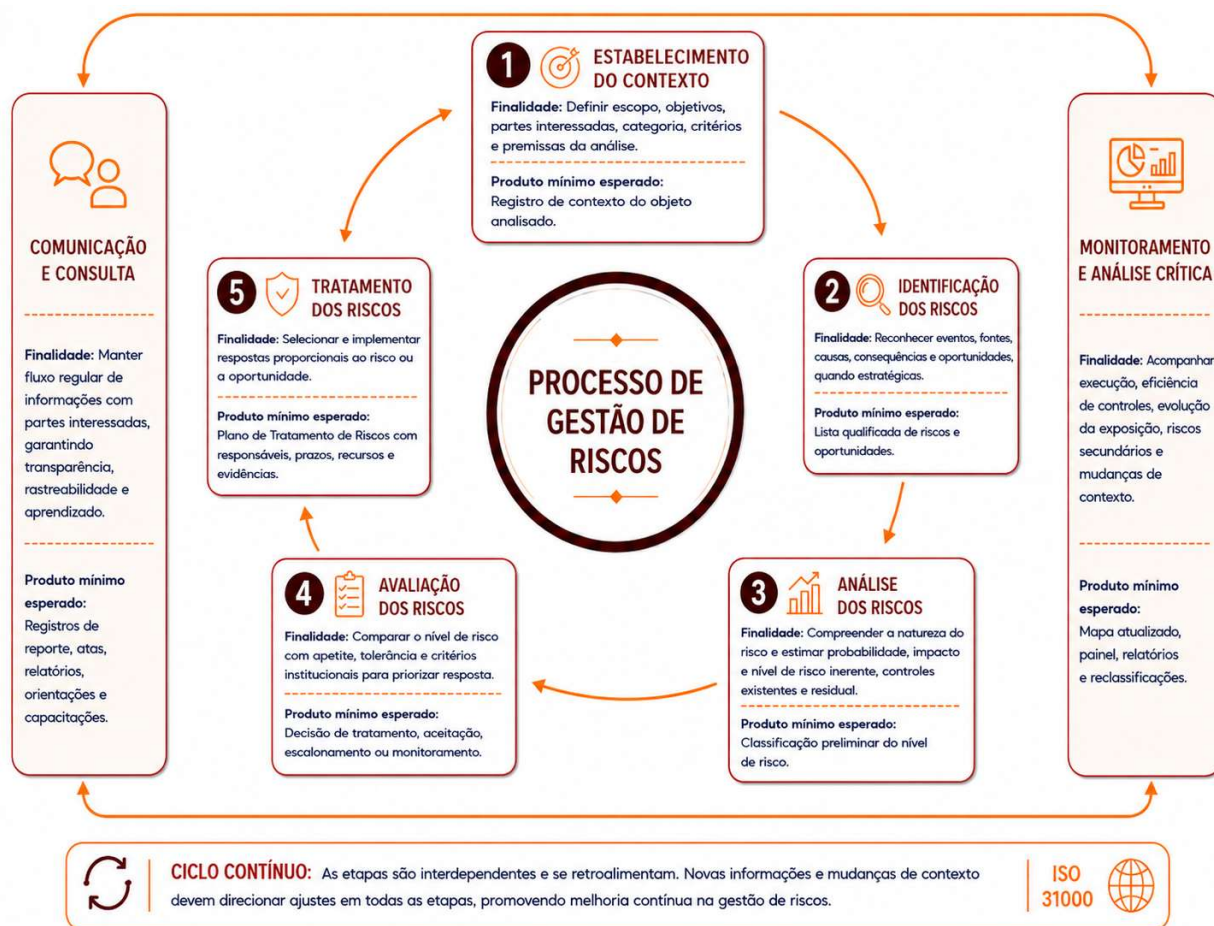
5. METODOLOGIA E PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos estabelece o fluxo metodológico para gerir riscos. O processo é estabelecido em sete etapas interdependentes, contínuas e retroalimentadas: estabelecimento do contexto; identificação; análise; avaliação; tratamento; monitoramento e análise crítica; e comunicação e consulta (a comunicação e a consulta devem ocorrer em todas as etapas, e não apenas ao final do ciclo).

Conforme a Política de Gestão de Riscos do CNMP e a ISO 31000, esse processo de gestão de riscos deve ser contínuo, estruturado, proporcional ao contexto analisado e integrado à tomada de decisão, permitindo que os riscos sejam compreendidos, priorizados e mantidos em níveis compatíveis com o apetite institucional. Dessa forma, a gestão de riscos deixa de ser uma atividade isolada e passa a compor a rotina de planejamento, execução, controle e melhoria contínua da organização.

O infográfico a seguir representa as sete etapas em formato visual e cíclico, evidenciando que o processo de gestão de riscos é contínuo, integrado e iterativo.

Figura 3: Etapas do Processo de Gestão de Riscos



O processo de gestão de riscos pode ser compreendido como o conjunto de atividades contínuas, realizado em todos os níveis da organização, destinado a identificar riscos que possam afetar o alcance dos objetivos institucionais e a apoiar decisões e ações necessárias para manter esses riscos em níveis compatíveis com os limites de exposição previamente estabelecido.

5.1 Mapa de Riscos

A Política de Gestão de Riscos do CNMP define o Mapa de Riscos como o documento que consolida os riscos identificados, analisados, avaliados e tratados no âmbito de cada unidade organizacional. O documento deve apresentar, no mínimo, os níveis de exposição, causas, consequências, controles existentes, responsáveis e medidas de tratamento, servindo como base para o monitoramento contínuo e para a integração dos riscos da unidade ao Painel Institucional de Riscos.

O Mapa de Riscos constitui o principal instrumento de registro, acompanhamento e rastreabilidade da gestão de riscos no âmbito das unidades do CNMP. Nele devem ser documentadas as informações essenciais sobre cada risco, desde sua identificação até a definição das respostas adotadas, permitindo que o proprietário do risco, os facilitadores, a SGE, a AUDIN e as instâncias de governança acompanhem a evolução da exposição ao longo do ciclo de gestão.

Recomenda-se o registro do Mapa de Riscos em processo SEI específico, pelo respectivo proprietário do risco, a quem compete assegurar a atualização das informações, a guarda das evidências, o registro das decisões adotadas e o reporte às instâncias competentes, quando necessário. Esse registro deve permitir a rastreabilidade das análises realizadas e das medidas de tratamento definidas.

O modelo do Mapa de Riscos é elaborado, padronizado e atualizado pela SGE, de modo a assegurar uniformidade metodológica, comparabilidade entre unidades, consolidação institucional das informações e integração com o Painel Institucional de Riscos. A SGE poderá promover ajustes no modelo sempre que houver necessidade de aprimoramento metodológico, alteração normativa, mudança relevante no contexto institucional ou revisão do Plano de Gestão de Riscos.

Além do modelo padronizado do Mapa de Riscos, a SGE poderá orientar a aplicação de métodos estruturados em ferramentas institucionais, de modo a apoiar as unidades na organização inicial das informações, na identificação preliminar de riscos, causas, consequências e possíveis medidas de tratamento.

A atualização do Mapa é de responsabilidade do proprietário do risco, com apoio do facilitador de riscos, quando designado, devendo ocorrer sempre que houver alteração relevante no contexto, mudança no nível de exposição, conclusão ou revisão de medidas, identificação de riscos secundários ou necessidade de reporte às instâncias competentes de governança.

5.1.1 Uso de ferramentas institucionais e de inteligência artificial

O uso de ferramentas institucionais, inclusive de inteligência artificial (IA), poderá ser adotado como apoio às etapas de identificação, análise e tratamento de riscos, com caráter exclusivamente auxiliar, não substituindo o julgamento técnico e a decisão do proprietário do risco, especialmente quanto à validação dos controles existentes, da probabilidade, do impacto, do nível de risco, do risco residual e das medidas de tratamento a serem registradas no Mapa de Riscos.

As informações geradas por IA deverão ser ajustadas e validadas antes de seu registro no Mapa de Riscos, permanecendo a responsabilidade integral pelas análises e decisões com o proprietário do risco.

É vedada a utilização de ferramentas de IA não homologadas institucionalmente para tratamento de informações sensíveis, sigilosas ou pessoais, devendo ser observadas as normas de segurança da informação e proteção de dados.

Compete à SGE orientar o uso dessas ferramentas, podendo disponibilizar diretrizes, boas práticas e instrumentos de apoio.

5.2 Etapa I: Estabelecimento do contexto

O estabelecimento do contexto é a etapa inicial obrigatória. Deve delimitar o objeto de análise, explicitar seus objetivos, indicar a razão da priorização, identificar partes interessadas, definir categoria e critérios, e registrar as premissas que orientarão a mensuração do risco.

Tabela 4: Estabelecimento do contexto

CAMPO	PERGUNTA ORIENTADORA	ORIENTAÇÃO DE PREENCHIMENTO
Tipo de objeto	O que será analisado?	Objetivo estratégico ou prioritário, objetivo tático, projeto, processo, ativo, iniciativa, ação, serviço ou outro elemento crítico.
Objeto analisado	Qual é o escopo específico?	Descrever de forma objetiva o processo, projeto, objetivo, ativo ou decisão analisada.
Objetivos associados	Que resultado deve ser alcançado?	Relacionar objetivo estratégico, objetivo tático, KR, entrega, meta, requisito normativo ou valor público afetado.
Unidade responsável	Quem é o proprietário do risco?	Informar autoridade ou unidade com responsabilidade final pela gestão do risco.
Partes interessadas	Quem influência ou é impactado?	Listar pessoas, unidades, órgãos, grupos ou entidades internas e externas relevantes.
Categoria de risco	Que tipo de risco predomina?	Assinalar categoria principal e, se necessário, categorias secundárias.
Contexto interno e externo	Quais fatores condicionam o risco?	Registrar fatores políticos, legais, tecnológicos, orçamentários, reputacionais, culturais, de pessoas, processos, sistemas e dados.
Crítérios de risco	Como o risco será avaliado?	Utilizar sempre probabilidade e impacto institucionais, apetite, tolerância e regra de escalonamento aplicáveis.

5.3 Etapa II: Identificação dos riscos

A identificação consiste na busca, reconhecimento e descrição dos riscos, mediante registro de evento, fonte, causa, consequência, controles existentes e, quando aplicável, oportunidades. A descrição do risco deve permitir compreensão clara do que pode acontecer, porque pode acontecer e qual objetivo pode ser afetado.

Tabela 5: Identificação dos riscos

ELEMENTO	DESCRIÇÃO
Evento de risco	Ocorrência incerta que pode afetar o objetivo. Deve ser redigida como evento, e não como simples ausência de controle.
Fonte de risco	Elemento que pode dar origem ao risco, isoladamente ou em combinação com outros.
Causa	Condição, vulnerabilidade ou fator que viabiliza a ocorrência do evento.
Consequência	Efeito potencial sobre objetivo, entrega, conformidade, integridade, imagem, continuidade ou valor público.

ELEMENTO	DESCRIÇÃO
Oportunidade	Evento favorável aplicável ao nível estratégico que possa potencializar o alcance de objetivo institucional.

Para a identificação e a descrição adequada dos riscos, recomenda-se que sua formulação evidencie a relação entre causa, evento, consequência e objetivo afetado. Assim, sempre que possível, o risco deve ser descrito a partir da seguinte lógica:

*“Devido a [causa/fonte], pode ocorrer [evento de risco],
ocasionando [consequência] sobre [objeto da gestão de riscos]”.*

Essa estrutura contribui para evitar registros genéricos, facilita a análise posterior e melhora a definição das medidas de tratamento.

5.4 Etapa III: Análise dos riscos

A análise dos riscos consiste na etapa destinada a determinar o nível de exposição associado a cada risco identificado, a partir da combinação entre a probabilidade de ocorrência do evento e o impacto potencial sobre os objetivos, entregas e resultados institucionais. Essa avaliação deve ser realizada com base em critérios previamente definidos, de forma padronizada, proporcional e coerente com o contexto do objeto analisado, permitindo comparar riscos, estabelecer prioridades e subsidiar a definição das respostas mais adequadas. A avaliação observará escalas institucionais de probabilidade e impacto, cujo resultado orientará a classificação do nível de risco e o grau de tratamento, monitoramento e reporte necessário.

5.4.1 Escala de probabilidade

A escala de probabilidade tem por finalidade orientar a estimativa da chance de ocorrência de determinado evento de risco durante o ciclo de gestão. Essa avaliação deve considerar o histórico de ocorrências, a existência de vulnerabilidades, o grau de exposição do objeto analisado e a efetividade dos controles existentes, servindo como um dos critérios para posterior definição do nível de risco.

Tabela 6: Escala de probabilidade

ESCALA DE PROBABILIDADE	DESCRIÇÃO	CRITÉRIO ORIENTATIVO
Baixa – 1	O evento é excepcional, pouco plausível ou não esperado no ciclo de gestão.	Não há histórico recente, há poucos indícios de ocorrência ou os controles existentes tendem a prevenir adequadamente o evento.
Média – 2	O evento pode ocorrer em circunstâncias normais.	Há vulnerabilidades conhecidas, histórico eventual ou condições que tornam a ocorrência possível durante o ciclo de gestão.
Alta – 3	O evento tende a ocorrer ou é esperado/recorrente no ciclo de gestão.	Há histórico relevante, exposição frequente, fragilidade significativa ou controles insuficientes para prevenir a ocorrência.

5.4.2 Escala de impacto

A escala de impacto tem por finalidade orientar a avaliação dos efeitos que a materialização de um evento de risco pode produzir sobre os objetivos, entregas, prazos, custos, qualidade, conformidade, integridade, imagem, continuidade ou reputação institucional. Essa avaliação deve considerar a relevância do objeto analisado e a extensão dos possíveis prejuízos ou consequências, compondo, juntamente com a probabilidade, a base para a definição do nível de risco.

Tabela 7: Escala de impacto

ESCALA DE IMPACTO	DESCRIÇÃO	CRITÉRIO ORIENTATIVO
Baixo – 1	Efeito residual ou limitado, absorvível pela rotina da unidade ou corrigível com medidas simples.	Não compromete de forma relevante o objetivo, o prazo, o custo, a qualidade, a conformidade, a integridade ou a imagem institucional. Pode gerar ajustes pontuais, retrabalho simples ou atraso de baixa materialidade.
Médio – 2	Efeito relevante, que exige coordenação gerencial e adoção de medidas corretivas ou preventivas estruturadas.	Afeta entrega, prazo, custo, qualidade, conformidade ou percepção institucional de forma controlável, podendo comprometer parcialmente o alcance do objetivo ou exigir atuação coordenada da unidade responsável.
Alto – 3	Efeito significativo ou severo, com potencial de comprometer objetivo relevante, unidade, imagem institucional, continuidade, integridade, legalidade ou confiança social.	Compromete resultado importante ou objetivo estratégico, exige intervenção tática ou estratégica, resposta coordenada e priorização pela governança, especialmente quando envolver alta sensibilidade institucional, reputacional, legal ou de integridade.

5.4.3 Nível de risco

A classificação do nível de risco tem por finalidade orientar a priorização das respostas institucionais, considerando a exposição resultante da combinação entre probabilidade e impacto. Os níveis apresentados a seguir indicam o grau de atenção, monitoramento e tratamento esperado para cada risco, de acordo com sua relevância para os objetivos, entregas e responsabilidades institucionais.

Tabela 8: Escala de Nível de risco

NÍVEL DE RISCO	DESCRIÇÃO	CRITÉRIO ORIENTATIVO
Baixo	Exposição reduzida, com baixo potencial de comprometer o objetivo analisado.	O risco pode ser monitorado pela própria unidade responsável, sem necessidade de tratamento adicional imediato, salvo decisão do proprietário do risco.
Médio	Exposição moderada, com possibilidade de afetar parcialmente o alcance do objetivo.	Requer acompanhamento gerencial e, quando necessário, definição de medidas de tratamento proporcionais ao risco.
Alto	Exposição relevante, com potencial de comprometer resultado, entrega, conformidade, integridade, imagem ou objetivo institucional.	Requer priorização, plano de tratamento, definição de responsáveis, prazos e monitoramento periódico.
Crítico	Exposição severa, com potencial de comprometer objetivo estratégico, continuidade, legalidade, integridade, reputação institucional ou confiança social.	Requer tratamento prioritário, acompanhamento pelas instâncias competentes de governança e reporte estruturado à alta administração.

A matriz de riscos representa a combinação entre a escala de probabilidade e a escala de impacto, classificando o nível de risco de forma padronizada. A pontuação apresentada tem caráter orientativo e apoia à análise, à comparação entre riscos e à definição das prioridades de tratamento, sem substituir a avaliação técnica do proprietário do risco e das instâncias competentes.

Figura 4: Matriz de Riscos 3x3

Nível de Risco		PROBABILIDADE		
		Baixa 1	Média 2	Alta 3
IMPACTO	Alto 3	3 Médio	6 Alto	9 Crítico
	Médio 2	2 Baixo	4	6 Médio
	Baixo 1	1 Baixo	2 Baixo	3 Médio

A pontuação obtida pela multiplicação da “probabilidade” e do “impacto”, de acordo com a matriz acima, configura o nível de risco inerente do objeto analisado.

5.4.4 Nível de risco residual

Após avaliar o risco inerente, a unidade deve identificar controles existentes e avaliar sua efetividade. A análise do risco residual deve considerar se os controles reduzem de forma suficiente a probabilidade, o impacto ou ambos.

Tabela 9: Eficácia dos controles

EFICÁCIA DO CONTROLE	FATOR MULTIPLICADOR	DESCRIÇÃO
Inexistente	1,0	Não há controle identificado, formalizado ou evidenciável para reduzir a probabilidade ou o impacto do risco.
Fraca	0,75	Há controle existente, mas informal, pouco conhecido, não testado, sem responsável definido ou com baixa capacidade de reduzir a exposição ao risco.
Mediana	0,5	Há controle definido e aplicado, mas com limitações de execução, cobertura, evidência, monitoramento ou efetividade.
Forte	0,25	O controle é formal, executado, evidenciado, proporcional ao risco, monitorado e possui evidências confiáveis de funcionamento.

O risco residual será estimado a partir da aplicação do fator de eficácia dos controles sobre a pontuação do risco inerente. Essa pontuação deve apoiar a avaliação técnica do proprietário do risco, considerando a qualidade das evidências, a efetividade dos controles e o contexto do objeto analisado. A redução do risco somente deverá ser reconhecida quando houver controle formalizado, executado, monitorado e devidamente evidenciado.

Tabela 10: Risco Inerente x Controle

RISCO INERENTE	EFICÁCIA DO CONTROLE “INEXISTENTE”	EFICÁCIA DO CONTROLE “FRACO”	EFICÁCIA DO CONTROLE “MEDIANO”	EFICÁCIA DO CONTROLE “FORTE”
1	1,00 — Baixo	0,75 — Baixo	0,50 — Baixo	0,25 — Baixo
2	2,00 — Baixo	1,50 — Baixo	1,00 — Baixo	0,50 — Baixo
3	3,00 — Médio	2,25 — Baixo	1,50 — Baixo	0,75 — Baixo
4	4,00 — Médio	3,00 — Médio	2,00 — Baixo	1,00 — Baixo
6	6,00 — Alto	4,50 — Médio	3,00 — Médio	1,50 — Baixo
9	9,00 — Crítico	6,75 — Alto	4,50 — Médio	2,25 — Baixo

A tabela apresenta todas as possibilidades de risco residual, de acordo com o risco inerente e os respectivos controles e seus níveis de eficácia. O risco residual será classificado de acordo com as faixas da figura abaixo:

Figura 5: Nível de Risco Residual

Faixa da pontuação residual	Nível de risco residual
até 2,9	Baixo
de 3,0 a 4,9	Médio
de 5,0 a 8,9	Alto
9,0	Crítico

5.5 Etapa IV: Avaliação de riscos

A avaliação de riscos consiste na etapa destinada a comparar o nível de risco residual, obtido na etapa de análise, com os critérios institucionais de risco e com o apetite a risco definido pelo CNMP. Seu objetivo é verificar se o risco residual se encontra em nível aceitável, tolerável ou acima do limite admitido, subsidiando a decisão quanto à necessidade de tratamento, monitoramento, escalonamento ou aceitação formal do risco.

Dessa forma, a avaliação de riscos não se confunde com a análise. Enquanto a análise estima a exposição residual do risco, considerando probabilidade, impacto e eficácia dos controles existentes, a avaliação interpreta esse resultado à luz do apetite institucional, da relevância do objetivo afetado, da categoria do risco, do contexto vigente e da capacidade de resposta da organização.

5.5.1 Finalidade da avaliação de riscos

A avaliação de riscos tem por finalidade orientar a tomada de decisão sobre o tratamento dos riscos, assegurando que os esforços institucionais sejam proporcionais ao nível de exposição identificado e coerentes com o apetite a risco. A avaliação deve permitir responder, no mínimo, às seguintes questões:

Tabela 11: Finalidade avaliação de riscos

QUESTÃO ORIENTADORA	FINALIDADE
O risco residual está dentro do apetite a risco definido?	Verificar se o risco pode ser aceito ou se exige resposta adicional.
O risco residual é compatível com a relevância do objetivo afetado?	Avaliar se a exposição é aceitável diante da importância estratégica, tática ou operacional do objeto analisado.
O risco residual exige tratamento adicional?	Definir se serão necessárias novas medidas de controle, prevenção, mitigação ou resposta.
O risco residual deve ser escalado?	Verificar se o risco deve ser submetido a instâncias superiores de governança.
O risco residual deve compor o Painel Institucional de Riscos?	Verificar a necessidade de integração ao painel, especialmente nos casos de riscos altos e críticos.
A aceitação do risco deve ser formalizada?	Assegurar rastreabilidade e responsabilização pela decisão.

5.5.2 Comparação do risco residual com o apetite a risco

A avaliação deverá considerar o nível de risco residual resultante da etapa de análise (ver item 5.4) e compará-lo com o apetite a risco aplicável ao objeto analisado.

O apetite a risco representa o nível de exposição que o CNMP está disposto a aceitar, considerando seus objetivos, valores, obrigações legais, capacidade operacional, integridade, reputação e compromisso com a geração de valor público.

A Política de Gestão de Riscos prevê que o apetite a riscos será revisado e deliberado pelas instâncias de Governança, sendo aprovado pela Presidência e informado, periodicamente, aos Proprietários de Riscos.

Para fins metodológicos, a comparação entre risco residual e apetite a risco poderá observar a seguinte orientação:

Tabela 12: Orientação de avaliação de risco residual

SITUAÇÃO DO RISCO RESIDUAL	INTERPRETAÇÃO	DECISÃO ORIENTATIVA
Risco residual dentro do apetite	A exposição é considerada aceitável para o contexto analisado.	Aceitar o risco e, possivelmente, manter monitoramento.
Risco residual próximo ao limite do apetite	A exposição é tolerável, mas exige atenção gerencial.	Monitorar e, se necessário, adotar tratamento proporcional.
Risco residual acima do apetite	A exposição supera o nível admitido pelo CNMP.	Definir tratamento adicional, responsáveis, prazos e evidências.
Risco residual muito acima do apetite ou de alta sensibilidade institucional	A exposição pode comprometer objetivos relevantes, integridade, conformidade, reputação ou confiança social.	Priorizar tratamento e submeter às instâncias competentes de governança.

5.5.3 Avaliação por categoria de risco

A avaliação de riscos deverá considerar que determinadas categorias podem exigir menor tolerância institucional, ainda que a pontuação residual não seja a mais elevada. Riscos de integridade, conformidade e reputacionais, por exemplo, podem demandar tratamento ou escalonamento em razão de sua sensibilidade institucional, legal ou ética.

Tabela 13: Avaliação de risco residual por categoria

CATEGORIA DE RISCO	ASPECTO A OBSERVAR NA AVALIAÇÃO
Estratégico	Potencial de comprometer objetivos estratégicos, a missão, a visão, a Mandala Estratégica ou prioridades definidas pela Presidência.
Tático	Potencial de comprometer objetivos táticos, painéis de contribuição ou entregas intermediárias necessárias ao alcance da estratégia.
Operacional	Potencial de comprometer processos, atividades, pessoas, sistemas, infraestrutura ou continuidade de serviços.
Conformidade	Potencial de descumprimento de normas legais, constitucionais, regulamentares ou contratuais.
Integridade	Potencial de ocorrência de fraude, corrupção, irregularidade, desvio ético ou conduta incompatível com os valores institucionais.
Reputacional	Potencial de comprometer a imagem, a credibilidade ou a confiança da sociedade no CNMP.

Nos riscos estratégicos, a avaliação deve considerar também oportunidades capazes de potencializar resultados e agregar valor institucional. Essa abordagem é aplicável exclusivamente aos riscos estratégicos, conforme previsto na Política de Gestão de Riscos do CNMP.

5.5.4 Decisão quanto à resposta ao risco

Ao final da avaliação, o proprietário do risco deverá indicar a decisão preliminar quanto à resposta ao risco residual, observando os critérios institucionais, o apetite a risco e a necessidade de eventual deliberação superior.

Tabela 14: Decisões sobre risco residual

DECISÃO	QUANDO UTILIZAR (SUGESTIVO)	RESULTADO ESPERADO
Aceitar	Quando o risco residual estiver dentro do apetite a risco ou quando o custo do tratamento for desproporcional, desde que a aceitação seja justificada.	Registro da aceitação e manutenção do monitoramento.
Monitorar	Quando o risco residual for tolerável, mas exigir acompanhamento periódico em razão de possível mudança de contexto.	Definição de periodicidade, responsável e forma de acompanhamento.
Tratar	Quando o risco residual estiver acima do apetite ou puder comprometer objetivo, entrega, conformidade, integridade, reputação ou continuidade.	Elaboração de plano de tratamento, com medidas, responsáveis, prazos e evidências.
Escalar	Quando o risco residual exigir decisão de instância superior, envolver alta sensibilidade institucional ou ultrapassar a competência da unidade responsável.	Submissão às instâncias competentes de governança para orientação ou deliberação.

Nos casos em que a decisão seja ‘tratar’, deverão ser adotadas as estratégias previstas na Etapa V (item 5.6), tais como evitar, mitigar, transferir ou remover a fonte do risco, devendo o proprietário selecionar a alternativa mais adequada ao contexto e ao apetite a risco.

5.5.5 Produto e registro da avaliação de riscos

A avaliação de riscos deverá ser registrada no Mapa de Riscos da unidade, de modo a garantir rastreabilidade da decisão e subsidiar o monitoramento posterior. O produto da avaliação de riscos será a decisão fundamentada sobre a aceitabilidade do risco residual. Essa decisão deverá indicar se o risco será aceito, monitorado, tratado ou escalado, bem como se deverá compor o Painel Institucional de Riscos.

A avaliação deverá assegurar que os riscos acima do apetite institucional recebam tratamento adequado e proporcional, enquanto os riscos dentro do apetite permaneçam sob monitoramento, de modo a preservar a aderência à estratégia, à integridade, à conformidade, à transparência e à geração de valor público pelo CNMP.

5.6 Etapa V: Tratamento dos riscos

O tratamento dos riscos consiste na definição e implementação das respostas necessárias para modificar o nível de exposição identificado, de modo a manter os riscos em patamar compatível com o apetite institucional e com os objetivos do CNMP. Essa etapa deve considerar o nível de risco residual, a relevância do objetivo afetado, a natureza do risco, a viabilidade das medidas propostas, os custos envolvidos, os benefícios esperados e os eventuais riscos secundários decorrentes da resposta adotada. As ações de tratamento devem ser proporcionais, justificadas, registradas e monitoráveis, assegurando clareza quanto aos responsáveis, prazos, evidências e critérios de acompanhamento.

5.6.1 Tratamento de ameaças

O tratamento consiste na seleção e implementação de uma ou mais ações para modificar o nível de risco. As respostas devem ser proporcionais, economicamente justificáveis, rastreáveis e compatíveis com o apetite institucional.

Tabela 15: Resposta aos riscos

ESTRATÉGIA	QUANDO UTILIZAR	EXEMPLOS
Evitar	Quando a exposição for incompatível com o apetite ou a atividade puder ser descontinuada/reformulada.	Suspender iniciativa, alterar escopo, substituir procedimento.
Remover fonte de risco	Quando for possível eliminar a causa ou fonte que dá origem ao risco, sem necessariamente suspender a atividade ou alterar integralmente o objetivo.	Eliminar etapa desnecessária do fluxo, substituir sistema vulnerável, corrigir causa estrutural recorrente, retirar acesso indevido, extinguir dependência operacional crítica.
Mitigar	Quando for possível reduzir probabilidade ou impacto com controles proporcionais.	Revisar fluxo, automatizar validação, capacitar equipe, implantar dupla checagem.
Transferir/compartilhar	Quando parte do risco puder ser alocada a terceiro, parceiro, contrato, seguro ou arranjo de cooperação, sem afastar responsabilidade institucional.	Cláusulas contratuais, acordos de nível de serviço, cooperação técnica.
Aceitar	Quando o risco residual estiver dentro do apetite ou quando o custo do tratamento superar o benefício esperado.	Aceite formal documentado pelo proprietário de risco e monitoramento periódico.
Escalar	Quando o risco exceder alçada, envolver múltiplas unidades ou exigir decisão estratégica/tática.	Reporte à SGE, comitê temático, Instância Superior de Governança ou Presidência.

5.6.2 Registro das medidas de tratamento no Mapa de Riscos

As medidas de tratamento deverão ser registradas no Mapa de Riscos da unidade, especialmente quando o risco residual for classificado como alto ou crítico, ou quando riscos médios exigirem acompanhamento específico em razão de tendência de agravamento, impacto relevante, exigência normativa ou sensibilidade institucional. O registro deve permitir a compreensão da resposta definida, sua justificativa, os responsáveis pela execução, os prazos, as evidências esperadas e a forma de acompanhamento, assegurando rastreabilidade e transparência às decisões adotadas pelo proprietário do risco.

O registro no Mapa de Riscos transforma a análise em memória institucional, a decisão em evidência e a gestão de riscos em processo rastreável.

O Mapa de Riscos deve consolidar as medidas de tratamento relacionadas a cada risco, compondo a base para o monitoramento contínuo pela unidade e para eventual integração ao Painel Institucional de Riscos.

5.7 Etapa VI: Monitoramento e análise crítica

O monitoramento consiste na verificação contínua da situação dos riscos, da execução dos tratamentos, da efetividade dos controles, da ocorrência de incidentes, da evolução de exposição e das mudanças de contexto. A análise crítica deve subsidiar a revisão de critérios, controles, tratamento, apetite e metodologia.

Tabela 16: Monitoramento e análise crítica

ATIVIDADE	PERIODICIDADE MÍNIMA	RESPONSÁVEL PRIMÁRIO	SUPERVISÃO/APOIO
Atualização do Mapa de Riscos da Unidade	Trimestral, ou antes se houver mudança relevante	Proprietário de Risco	SGE
Monitoramento das ações de tratamento	Contínuo	Proprietário de Risco	SGE / Comitê Temático, conforme nível
Reclassificação de risco	Sempre que houver alteração de probabilidade, impacto, contexto ou controles	Proprietário de Risco	SGE
Atualização do Painel Institucional de Riscos	Contínuo	SGE	Comitês Temáticos / Governança
Relatório Anual de Acompanhamento da Gestão de Riscos	Anual	SGE	Alta Administração
Revisão do Plano e da metodologia	Até dois anos ou extraordinariamente	SGE / Comitê Temático	Instância Superior de Governança / Presidência

5.7.1 Painel Institucional de Riscos

O Painel Institucional de Riscos é a solução de inteligência de negócios — BI — destinada a consolidar, representar visualmente e acompanhar, de forma dinâmica, as informações constantes dos Mapas de Riscos das unidades do CNMP.

A ferramenta tem por finalidade apoiar a análise integrada da exposição institucional a riscos, permitindo a visualização dos riscos estratégicos e dos riscos relevantes identificados pelas unidades, bem como de suas causas, consequências, níveis de exposição, controles, medidas de tratamento, responsáveis, prazos, indicadores e situação de execução.

O Painel Institucional de Riscos será alimentado pelos dados constantes dos Mapas de Riscos das unidades e dos riscos estratégicos identificados no âmbito institucional, devendo estar alinhado ao PE-CNMP e contemplar, entre outras informações, riscos estratégicos, riscos de nível alto e crítico, oportunidades estratégicas relevantes, níveis de exposição, unidades responsáveis, medidas de tratamento, prazos, indicadores, situação de execução e demais elementos necessários à identificação de tendências, à priorização de ações, ao acompanhamento das medidas de tratamento, ao apoio à tomada de decisão pela Alta Administração e à comunicação estruturada dos riscos institucionais. Considerando que o Painel Institucional de Riscos consolida informações sensíveis relativas à exposição institucional, às vulnerabilidades, aos

controles existentes e às medidas de tratamento dos riscos, seu acesso deverá ter caráter restrito, observadas as diretrizes de segurança da informação, a necessidade de conhecimento dos usuários autorizados e as regras aplicáveis à proteção de informações institucionais.

5.8 Etapa VII: Comunicação e consulta

A comunicação e a consulta constituem atividades contínuas e transversais ao processo de gestão de riscos, devendo ocorrer em todas as suas etapas, desde o estabelecimento do contexto até o monitoramento e a análise crítica. Sua finalidade é assegurar fluxo regular, tempestivo e qualificado de informações entre as partes envolvidas no processo de gestão de riscos.

A comunicação busca promover entendimento comum sobre os riscos, seus níveis de exposição, controles existentes, medidas de tratamento e decisões adotadas. A consulta, por sua vez, permite incorporar percepções, evidências, conhecimentos técnicos e informações relevantes para qualificar a identificação, a análise, a avaliação, o tratamento e o monitoramento dos riscos.

A comunicação e a consulta devem observar os princípios de transparência, rastreabilidade, integridade, confiabilidade, confidencialidade, proteção de dados e publicidade ativa. Informações sensíveis, especialmente aquelas relacionadas a riscos de integridade, conformidade, segurança institucional, tecnologia, dados pessoais ou exposição reputacional, deverão ser tratadas por canais adequados e com observância das restrições legais e institucionais aplicáveis.

Os instrumentos de comunicação e consulta devem apoiar a tomada de decisão, o acompanhamento dos riscos, a prestação de contas, o aprendizado institucional e a melhoria contínua da metodologia. Para tanto, serão utilizados, entre outros, os seguintes instrumentos:

Tabela 17: Instrumentos de comunicação e consulta

INSTRUMENTO	FINALIDADE
Mapa de Riscos da Unidade	Registrar e atualizar riscos, controles, tratamentos e evidências no âmbito da unidade.
Painel Institucional de Riscos	Consolidar riscos estratégicos, altos e críticos, oportunidades e tratamentos para tomada de decisão.
Relatórios periódicos e anual	Subsidiar reuniões de análise do PE-CNMP, prestação de contas e aprimoramento da metodologia.
Reuniões de análise e acompanhamento	Deliberar sobre priorização, tratamento, reclassificação e escalonamento.
Capacitações e orientações técnicas	Fortalecer cultura de riscos e uniformizar aplicação da metodologia.
Comunicação institucional	Dar transparência a resultados consolidados, preservadas informações sensíveis e restrições legais.

6. ABORDAGEM ESPECÍFICA PARA RISCOS ESTRATÉGICOS

Os riscos estratégicos são aqueles que podem afetar a definição ou o alcance dos **objetivos estratégicos**, da **missão** e da **visão** do CNMP, podendo se manifestar como ameaças ou oportunidades. Em razão de sua relevância institucional, sua gestão deve estar diretamente integrada ao PE-CNMP, à **Mandala Estratégica**, aos objetivos estratégicos prioritários definidos pela Presidência e às instâncias de governança responsáveis pelo direcionamento, monitoramento e tomada de decisão.

Mandala Estratégica: Instrumento visual de comunicação que organiza e apresenta a estratégia do órgão de forma simplificada, integrando missão, visão, valores e objetivos estratégicos em linguagem clara e acessível, facilitando a compreensão e o engajamento.

A abordagem dos riscos estratégicos deve considerar fatores internos e externos que possam influenciar a capacidade do CNMP de alcançar seus resultados institucionais, tais como mudanças normativas, institucionais, orçamentárias, tecnológicas, sociais, reputacionais, de articulação interinstitucional ou de governança. Também deve considerar oportunidades capazes de potencializar resultados, fortalecer a atuação institucional e ampliar a geração de valor público.

Para os fins deste Referencial, compete à Presidência do CNMP exercer a supervisão institucional dos riscos estratégicos, bem como atuar como proprietária daqueles cuja natureza, relevância ou transversalidade justifique tal atribuição, sem prejuízo da designação dessa responsabilidade a outras unidades administrativas. A SGE caberá atuar como facilitadora do processo de gestão de riscos estratégicos, prestando apoio metodológico, técnico e operacional às unidades responsáveis pela identificação, avaliação, tratamento, monitoramento e comunicação dos riscos.

6.1 Objeto da gestão de riscos estratégicos

A gestão de riscos estratégicos terá como objeto principal os objetivos estratégicos do CNMP, especialmente aqueles priorizados anualmente pela Presidência. Também poderão ser considerados outros temas, iniciativas ou decisões de alta relevância institucional, desde que tenham potencial de afetar a missão, a visão, a Mandala Estratégica, a continuidade de políticas institucionais, a reputação do Conselho ou sua capacidade de gerar valor público.

A análise deverá partir sempre do objetivo estratégico, evitando a formulação de riscos genéricos ou desvinculados da estratégia.

6.2 Papéis e responsabilidades na gestão de riscos estratégicos

A gestão dos riscos estratégicos observará a seguinte distribuição de papéis:

Tabela 18: Responsabilidades na gestão de riscos estratégicos

ATOR	PAPEL NA GESTÃO DOS RISCOS ESTRATÉGICOS
Presidência	Atuar como proprietária dos riscos estratégicos, elaborar e validar o Mapa de Riscos Estratégicos, definir as respostas institucionais aplicáveis e assegurar o alinhamento dos riscos à estratégia e ao apetite institucional. Definir e priorizar as medidas de tratamento.
SGE	Atuar como facilitadora do processo, prestando apoio metodológico e técnico no processo de gestão de riscos.
Comitês Temáticos de Governança	Contribuir, quando aplicável, com informações técnicas, avaliação de impactos, análise de medidas de tratamento e acompanhamento de riscos relacionados às suas áreas temáticas.
Unidades envolvidas	Fornecer informações, evidências, dados, percepções e subsídios necessários à compreensão dos riscos estratégicos e à definição das medidas de tratamento. Adotar as ações previstas nas medidas de tratamento.
AUDIN	Atuar como instância de avaliação independente, quando cabível, avaliando a governança, os controles e a efetividade do processo de gestão de riscos.

A SGE auxiliará a Presidência na condução do processo de gestão dos riscos estratégicos, desde o levantamento do contexto até a elaboração do respectivo Mapa de Riscos. Após a consolidação técnica, o Mapa de Riscos Estratégicos será submetido à validação da Presidência e, uma vez validado, comunicado aos atores e às instâncias interessadas, observadas a natureza das informações.

6.3 Abordagem para riscos positivos (oportunidades)

Os riscos positivos, tratados neste Referencial como oportunidades, correspondem a eventos incertos que podem contribuir para o alcance ou para a potencialização dos objetivos estratégicos do CNMP. Em consonância com os princípios da gestão de riscos, a consideração de oportunidades amplia a capacidade institucional de gerar valor público, apoiar a tomada de decisão e fortalecer o alcance dos resultados estratégicos.

A análise de oportunidades aplica-se exclusivamente aos riscos estratégicos e deverá estar vinculada aos objetivos estratégicos, à missão, à visão institucional, à Mandala Estratégica ou às prioridades institucionais. Não constitui finalidade desta abordagem identificar oportunidades desvinculadas da estratégia ou associadas exclusivamente à execução rotineira das atividades administrativas.

As oportunidades poderão decorrer de fatores internos ou externos capazes de favorecer o desempenho institucional, tais como avanços tecnológicos, mudanças normativas, parcerias estratégicas, disponibilidade de recursos, evolução de práticas de governança, transformações sociais ou outras condições que permitam ampliar resultados, gerar ganhos de eficiência, fortalecer a imagem institucional ou melhorar a prestação de serviços à sociedade.

A gestão das oportunidades observará as mesmas etapas gerais do processo de gestão de riscos previstas neste Referencial, com as adaptações metodológicas descritas a seguir.

6.3.1 Estabelecimento do contexto de riscos positivos

A análise deverá partir de objeto previamente definido, identificando-se os fatores internos e externos que possam favorecer sua consecução ou potencialização. Nessa etapa deverão ser avaliados os benefícios esperados, as partes interessadas envolvidas, as condições necessárias para aproveitamento da oportunidade e as restrições existentes.

6.3.2 Identificação de risco positivo

A oportunidade deverá ser descrita como evento incerto capaz de produzir efeitos favoráveis sobre os objetivos estratégicos. Nesta etapa busca-se identificar o que pode dar certo além do esperado e ser perseguido pela Instituição. Recomenda-se a seguinte estrutura de formulação:

*"Em razão de [fator impulsionador], pode ocorrer [evento favorável],
proporcionando [benefício esperado] para [objeto]."*

A identificação deve registrar, sempre que possível: fator impulsionador ou fonte da oportunidade; evento favorável; benefícios esperados; objetivo estratégico beneficiado; e mecanismos já existentes que favoreçam sua materialização.

6.3.3 Análise de risco positivo

A análise consiste na avaliação da probabilidade de ocorrência do evento favorável e da magnitude dos benefícios que poderão ser obtidos. A probabilidade deverá indicar a chance de concretização da oportunidade, enquanto o impacto deverá representar o potencial de geração de valor institucional. Consideram-se, entre outros aspectos: contribuição para os objetivos estratégicos; melhoria da eficiência institucional; fortalecimento da imagem e da confiança social; geração de economia ou racionalização de recursos; e ampliação da capacidade institucional de entrega de resultados.

Tal como nas ameaças, a combinação entre probabilidade e impacto permitirá identificar o grau de relevância da oportunidade para fins de priorização.

Tabela 19: Escala de probabilidade para riscos positivos (oportunidades)

Escala	Descrição
Baixa – 1	A oportunidade possui reduzida probabilidade de concretização no ciclo de gestão, dependendo de fatores pouco controláveis ou de baixa previsibilidade.
Média – 2	A oportunidade apresenta condições razoáveis para ocorrer, existindo fatores favoráveis que podem permitir sua concretização.
Alta – 3	A oportunidade possui elevada probabilidade de concretização, amparada por fatores favoráveis consistentes, tendências consolidadas ou condições já existentes.

Tabela 20: Escala de impacto para riscos positivos (oportunidades)

Escala	Descrição
Baixo – 1	Benefícios pontuais ou incrementais, com impacto restrito a determinada iniciativa, processo ou unidade organizacional.
Médio – 2	Benefícios relevantes, capazes de melhorar resultados, processos ou serviços institucionais, com reflexos perceptíveis para mais de uma unidade ou objetivo estratégico.
Alto – 3	Benefícios significativos ou transformacionais, com potencial de impulsionar objetivos estratégicos, gerar valor público relevante, fortalecer a atuação institucional ou produzir ganhos expressivos de desempenho, eficiência ou reputação institucional.

A classificação da oportunidade observará a mesma Matriz de Riscos 3x3 utilizada para os riscos de natureza negativa, permitindo identificar os eventos favoráveis que demandam priorização, monitoramento ou adoção de medidas específicas de aproveitamento pela Administração.

Tabela 21. Escala de nível de risco positivo (oportunidade)

NÍVEL DE RISCO	INTERPRETAÇÃO
Baixo	Exposição reduzida, com baixo potencial de geração de benefícios para o objetivo analisado.
Médio	Exposição moderada, com possibilidade de favorecer parcialmente o alcance do objetivo.
Alto	Exposição relevante, com potencial de ampliar resultados, agregar valor ou favorecer o alcance do objetivo institucional.
Crítico	Exposição muito relevante, com elevado potencial de geração de benefícios estratégicos, fortalecimento institucional ou impulso significativo ao alcance dos objetivos.

Após a determinação do nível inerente da oportunidade, deverão ser identificados os mecanismos existentes capazes de favorecer sua concretização ou potencializar os benefícios esperados. Esses mecanismos podem compreender iniciativas em andamento, competências institucionais, recursos disponíveis, soluções tecnológicas, instrumentos normativos, parcerias estratégicas ou quaisquer outras condições favoráveis ao aproveitamento da oportunidade.

A análise da efetividade desses mecanismos permitirá estimar o nível residual do risco positivo (oportunidade), considerando a capacidade institucional já existente para viabilizar sua concretização e maximizar os benefícios associados.

Tabela 22. Efetividade dos mecanismos de aproveitamento da oportunidade

EFETIVIDADE DO MECANISMO	FATOR	DESCRIÇÃO
Inexistente	0,25	Não há mecanismos identificados capazes de favorecer a concretização da oportunidade ou ampliar seus benefícios.
Fraca	0,50	Existem mecanismos isolados ou informais, com baixa capacidade de favorecer a concretização da oportunidade ou de ampliar seus resultados.
Mediana	0,75	Existem mecanismos definidos e em funcionamento, porém com limitações de alcance, monitoramento ou efetividade.
Forte	1,0	Existem mecanismos estruturados, monitorados e efetivos, capazes de favorecer significativamente a concretização da oportunidade e a obtenção dos benefícios esperados.

O nível residual da oportunidade deverá ser calculado mediante a aplicação do fator de efetividade dos mecanismos existentes sobre a pontuação do nível inerente. O resultado obtido representa o nível residual da

oportunidade após a consideração dos mecanismos existentes, servindo de subsídio para a avaliação de sua conveniência, prioridade e aproveitamento institucional.

O nível residual da oportunidade deverá ser considerado na etapa de avaliação, juntamente com sua relevância estratégica, viabilidade técnica e operacional, disponibilidade de recursos e potencial de geração de valor público, subsidiando a decisão quanto ao seu aproveitamento, monitoramento ou não priorização.

6.3.4 Avaliação de risco positivo

A avaliação deverá verificar se a oportunidade possui relevância estratégica suficiente para justificar a mobilização de esforços institucionais e a adoção de medidas destinadas ao seu aproveitamento.

Além da classificação obtida na análise, deverão ser considerados o alinhamento com os objetivos estratégicos, a aderência às prioridades institucionais, a viabilidade técnica e operacional, a disponibilidade de recursos, os custos de implementação, os benefícios esperados e os eventuais riscos secundários decorrentes de sua implementação.

A avaliação tem por finalidade subsidiar a tomada de decisão quanto à conveniência e à oportunidade de adoção de medidas voltadas à captura, potencialização ou monitoramento dos benefícios identificados, observando os interesses institucionais e a geração de valor público.

A oportunidade residual deverá ser comparada ao apetite a risco positivo definido pelo CNMP, de forma a verificar se o potencial benefício identificado justifica a adoção de ações institucionais voltadas ao seu aproveitamento.

Tabela 23. Orientação de avaliação de risco positivo residual (de oportunidade)

SITUAÇÃO	INTERPRETAÇÃO	ORIENTAÇÃO
Oportunidade residual acima do apetite	A oportunidade apresenta elevado potencial de geração de valor e é compatível com a estratégia institucional.	Priorizar o aproveitamento da oportunidade, definindo ações, responsáveis, prazos e mecanismos de acompanhamento.
Oportunidade residual próxima ao apetite	A oportunidade possui potencial relevante, porém demanda análise complementar quanto à viabilidade, aos custos e à alocação de recursos.	Monitorar a oportunidade e avaliar medidas proporcionais para seu aproveitamento.
Oportunidade residual abaixo do apetite	Os benefícios esperados são limitados ou insuficientes para justificar esforços institucionais adicionais.	Registrar a avaliação e não priorizar sua implementação no contexto analisado.

Ao final da avaliação, a oportunidade poderá ser classificada como priorizada para aproveitamento, monitorada para avaliação futura ou não priorizada, devendo a decisão ser devidamente registrada e fundamentada, de modo a assegurar rastreabilidade, transparência e suporte ao processo de tomada de decisão institucional.

6.3.5 Tratamento do risco positivo

O aproveitamento da oportunidade constitui a etapa destinada à implementação das ações definidas na avaliação do risco positivo. Aplica-se às oportunidades classificadas como prioritárias ou àquelas cujas relevâncias, após comparação com o apetite a risco institucional, justifique a adoção de medidas voltadas à captura ou potencialização dos benefícios esperados.

Enquanto os riscos negativos demandam ações de tratamento para redução da exposição, os riscos positivos demandam ações de aproveitamento destinadas a aumentar sua probabilidade de ocorrência, ampliar seus benefícios ou acelerar sua materialização.

As ações de aproveitamento devem ser proporcionais à relevância da oportunidade identificada e observar critérios de viabilidade técnica, disponibilidade de recursos, economicidade, alinhamento estratégico e geração de valor público.

Tabela 24. Resposta aos riscos positivos (oportunidades)

ESTRATÉGIA	QUANDO UTILIZAR
Potencializar	Quando a oportunidade já existe e ações adicionais podem ampliar seus benefícios ou aumentar sua probabilidade de ocorrência.
Viabilizar	Quando a oportunidade depende da criação de condições para sua implementação.
Compartilhar	Quando a realização da oportunidade puder ser ampliada mediante cooperação institucional.
Monitorar	Quando a oportunidade ainda não justificar atuação imediata ou depender de fatores futuros.
Não priorizar	Quando a análise demonstrar que os custos, riscos secundários, esforços necessários ou limitações de contexto não justificam a adoção de medidas voltadas ao aproveitamento da oportunidade.

As medidas definidas deverão possuir responsáveis, prazos, indicadores e evidências de acompanhamento, de modo a permitir a verificação dos benefícios esperados e dos resultados efetivamente alcançados.

6.3.6 Monitoramento e análise crítica de risco positivo

O monitoramento das oportunidades deverá verificar a evolução dos fatores que favorecem sua ocorrência, a execução das ações definidas, a efetividade das medidas de aproveitamento, os benefícios efetivamente alcançados, a permanência da relevância estratégica da oportunidade, a aderência da oportunidade ao apetite a risco institucional.

O monitoramento deverá verificar, ainda, se a oportunidade permanece compatível com o apetite a risco definido pelo CNMP e se os benefícios esperados continuam justificando a manutenção das ações de aproveitamento inicialmente estabelecidas.

Alterações relevantes no contexto institucional poderão ensejar a reavaliação da oportunidade, a revisão das ações planejadas, a redefinição de prioridades ou o encerramento das medidas de aproveitamento.

A análise crítica deverá considerar os resultados obtidos, os benefícios efetivamente capturados, a adequação dos mecanismos adotados e a permanência dos pressupostos que justificaram a priorização da oportunidade, servindo de subsídio à melhoria contínua da gestão de riscos estratégicos.

6.3.7 Comunicação e consulta de risco positivo

As oportunidades estratégicas classificadas como prioritárias, bem como aquelas consideradas relevantes pelas instâncias de governança, deverão ser registradas no respectivo Mapa de Riscos e comunicadas às partes interessadas competentes, observadas a natureza da informação e as competências institucionais.

As oportunidades registradas nos Mapas de Riscos poderão subsidiar a composição do Painel Institucional de Riscos, especialmente quando apresentarem elevada relevância estratégica, potencial significativo de geração de valor público ou demandarem acompanhamento pelas instâncias de governança.

A comunicação deverá permitir que a Alta Administração acompanhe oportunidades priorizadas; benefícios esperados; ações de aproveitamento em andamento; resultados alcançados; aderência ao apetite a risco institucional e eventuais riscos associados à sua implementação.

A consulta deverá ocorrer de forma contínua ao longo do processo de gestão das oportunidades, permitindo a incorporação de informações, percepções, evidências e conhecimentos especializados que contribuam para a adequada avaliação e aproveitamento dos eventos favoráveis identificados.

A gestão de oportunidades não substitui a gestão das ameaças nem implica a implementação de todas as oportunidades identificadas. Sua finalidade é assegurar que eventos incertos com potencial de produzir efeitos positivos sobre os objetivos estratégicos sejam identificados, analisados, avaliados, monitorados e, quando conveniente, aproveitados pela Administração, contribuindo para a ampliação da geração de valor público, para o fortalecimento da atuação institucional e para o alcance da estratégia do CNMP.



7. ABORDAGEM PARA AS DEMAIS CATEGORIAS DE RISCOS

Além da abordagem específica para riscos estratégicos, a gestão de riscos do CNMP contemplará os riscos táticos, operacionais, de conformidade, de integridade e reputacionais. Essas categorias não devem ser analisadas de forma isolada ou desconectada pelas unidades administrativas, mas sempre à luz de sua relação com os objetivos estratégicos e seus respectivos riscos.

A análise dessas categorias deve considerar que um mesmo evento de risco pode afetar mais de uma dimensão institucional, desde que haja relação com eventos de riscos estratégicos previamente mapeados. Assim, um risco operacional pode gerar reflexos reputacionais ou de conformidade; um risco de integridade pode comprometer a confiança social e a imagem institucional; e um risco tático pode revelar fragilidades operacionais, normativas ou de governança, sempre que tais efeitos estejam vinculados a riscos estratégicos identificados. Por isso, a classificação deverá indicar a categoria predominante, sem prejuízo do registro de categorias associadas ou riscos secundários, quando aplicável.

A abordagem integrada busca assegurar que a gestão de riscos seja orientada pela estratégia institucional, evitando levantamentos fragmentados, excessivamente setoriais ou desvinculados dos resultados esperados pelo CNMP. Dessa forma, os eventuais riscos identificados pelas unidades podem contribuir para o aprimoramento do planejamento, o fortalecimento dos controles, a priorização de processos críticos, a continuidade dos serviços, a integridade, a conformidade, a reputação institucional e o alcance dos objetivos estratégicos.

7.1 Objetos de análise

A identificação dos riscos táticos, operacionais, de conformidade, de integridade e reputacionais poderá partir de diferentes objetos institucionais, conforme a natureza da análise realizada. Em todas as situações, a unidade poderá realizar gestão de riscos se houver relação entre o risco identificado e os objetivos, entregas, processos ou responsabilidades que obrigatoriamente tenham vinculação com a estratégia institucional.

Quanto aos riscos táticos, estes terão como referência os objetivos táticos definidos nos Painéis de Contribuição das unidades, considerando os fatores que possam comprometer sua consecução e, por consequência, afetar a entrega de resultados intermediários necessários ao alcance dos objetivos estratégicos do CNMP.

Painel de Contribuição: instrumento de monitoramento que relaciona os objetivos táticos das unidades com as respectivas ações setoriais, visando diagnosticar, planejar e gerir recursos e processos táticos de maneira alinhada aos objetivos estratégicos.

Já os riscos operacionais, de conformidade, de integridade e reputacionais serão identificados, em regra, a partir da análise dos macroprocessos da Cadeia de Valor do CNMP, especialmente dos processos críticos, sempre mantendo a vinculação com os objetivos estratégicos e eventuais riscos mapeados.

Processo crítico: aquele cuja interrupção, falha, indisponibilidade ou execução inadequada possa comprometer entregas relevantes, serviços essenciais, obrigações legais, continuidade institucional, imagem do CNMP ou geração de valor público.

A priorização dos processos críticos poderá utilizar, quando disponível, subsídios da Política e do Plano de Continuidade de Negócios, de análises de impacto nos negócios — *Business Impact Analysis* (BIA) —, de critérios de criticidade, matriz de priorização, relevância estratégica, materialidade, histórico de incidentes ou outros instrumentos que auxiliem a identificação dos processos que demandam tratamento prioritário no âmbito da gestão de riscos.

Os riscos identificados, especialmente aqueles que demandem medidas de tratamento, deverão subsidiar o planejamento da unidade e apoiar a definição de ações concretas para redução da exposição ao risco. Quando pertinente, essas medidas poderão servir como insumo para a formulação de potenciais resultados-chave (KRs) em ciclos futuros, fortalecendo a integração entre gestão de riscos, desdobramento da estratégia e acompanhamento dos resultados institucionais.

Para fins de análise, devem ser observadas as seguintes orientações:

Tabela 25: Categorias de riscos e orientações de análise

CATEGORIA	ORIENTAÇÃO DE ANÁLISE
Risco tático	Avaliar eventos que possam comprometer, atrasar, prejudicar ou limitar o alcance dos objetivos táticos definidos nos Painéis de Contribuição das unidades e que, por consequência, afetem o alcance da estratégia ou contribuam para o aumento de exposição de riscos estratégicos.
Risco operacional	Avaliar eventos que possam gerar falhas, atrasos, retrabalho, indisponibilidade, ineficiência, perda de qualidade, interrupção de serviços ou comprometimento de processos críticos, que afetem o alcance da estratégia ou contribuam para o aumento de exposição de riscos estratégicos.
Risco de conformidade	Avaliar eventos que possam ocasionar descumprimento normativo, responsabilização institucional, sanções, nulidades ou falhas de aderência a obrigações legais, que porventura possam afetar o alcance da estratégia ou contribuam para o aumento de exposição de riscos estratégicos.
Risco de integridade	Avaliar eventos que possam comprometer valores institucionais, confiança, imparcialidade, probidade, ética pública ou mecanismos de prevenção e detecção.
Risco reputacional	Avaliar eventos que possam afetar a legitimidade, a comunicação institucional, a confiança da sociedade ou a percepção de valor do CNMP.

7.2 Papéis e responsabilidades

A gestão dos riscos táticos, operacionais, de conformidade, de integridade e reputacionais será conduzida pelas unidades responsáveis pelos respectivos objetivos táticos, macroprocessos, processos críticos, projetos, atividades, serviços ou ativos institucionais, observadas as competências institucionais e os fluxos de reporte definidos neste Referencial.

Compete ao titular da unidade, ou ao gestor responsável pelo objeto analisado, atuar como proprietário do risco, assegurando a identificação, análise, avaliação, tratamento, monitoramento e reporte dos riscos sob sua responsabilidade. A SGE atuará como unidade de apoio metodológico, cabendo-lhe orientar as unidades quanto à aplicação da metodologia institucional, disponibilizar instrumentos padronizados, apoiar

capacitações, consolidar informações, promovendo o alinhamento entre a gestão de riscos, os Painéis de Contribuição, a Cadeia de Valor e o Planejamento Estratégico do CNMP.

Quando designado, o facilitador de riscos da unidade apoiará tecnicamente o proprietário do risco na aplicação da metodologia, no preenchimento dos instrumentos, na organização das evidências, no acompanhamento das medidas de tratamento e na atualização do Mapa de Riscos da Unidade, sem prejuízo da responsabilidade final do proprietário do risco.

Os eventuais mapas de riscos elaborados nas Unidades Administrativas do CNMP devem ser de conhecimento da SGE e, quando cabível, também será dado conhecimento aos comitês temáticos ou às instâncias superiores de governança. Essa abordagem busca assegurar que os riscos identificados pelas unidades sejam analisados de forma integrada, proporcional e orientada à estratégia, evitando levantamentos isolados e fortalecendo a conexão entre objetivos institucionais, processos críticos, controles, continuidade dos serviços, integridade, conformidade, reputação e geração de valor público.

Tabela 26: Papéis e responsabilidades na gestão das demais categorias

ATOR	PAPEL NA GESTÃO DOS DEMAIS TIPOS DE RISCOS
Titular da unidade ou gestor responsável pelo objeto analisado	Atuar como proprietário do risco, assegurando a identificação, análise, avaliação, tratamento, monitoramento e reporte dos riscos relacionados a processos, projetos, atividades, serviços ou ativos sob sua responsabilidade.
Facilitador de riscos da unidade	Apoiar tecnicamente a aplicação da metodologia, o preenchimento dos instrumentos, a organização das evidências, o acompanhamento das medidas de tratamento e a atualização do Mapa de Riscos da Unidade.
SGE	Orientar metodologicamente as unidades, disponibilizar instrumentos padronizados, apoiar capacitações, consolidar informações e integrar riscos relevantes ao Painel Institucional de Riscos, quando aplicável.
Unidade Setorial de Integridade	Apoiar e orientar, quando aplicável, a análise e o tratamento de riscos de integridade, especialmente aqueles relacionados a fraude, corrupção, irregularidades, desvios éticos ou de conduta.
Comitês Temáticos de Governança	Acompanhar riscos de maior exposição, riscos que envolvam múltiplas unidades ou riscos que demandem deliberação, priorização ou alinhamento institucional.
AUDIN	Atuar como instância de avaliação independente, avaliando, quando cabível, a governança, os controles internos, a integridade, a conformidade e a efetividade do processo de gestão de riscos.

8. INTEGRAÇÃO ENTRE A GESTÃO DE RISCOS E O PLANEJAMENTO INSTITUCIONAL

A gestão de riscos do CNMP deve ser compreendida de forma integrada, conectando os níveis estratégico, tático e operacional aos objetos institucionais que podem ser afetados por incertezas. Essa integração permite que os riscos sejam identificados no nível adequado, sem perda de visão sistêmica, e que os riscos secundários ou associados sejam reconhecidos e tratados de forma proporcional.

Os riscos estratégicos partem dos objetivos estratégicos, da missão, da visão e das prioridades institucionais. Os riscos táticos partem, especialmente, dos objetivos táticos definidos nos Painéis de Contribuição das unidades.

Os riscos operacionais, de conformidade, de integridade e reputacionais podem ser identificados principalmente a partir da análise dos macroprocessos que compõem a Cadeia de Valor, uma vez que estes sustentam a execução da estratégia institucional. Esses riscos também podem ser identificados no nível estratégico, quando representarem fatores capazes de comprometer o alcance dos objetivos do órgão. Nessa perspectiva, a gestão de riscos somente se justifica quando houver vínculo claro entre os eventos de risco e os objetivos institucionais, de modo que sua identificação, avaliação e tratamento contribuam para a preservação ou a geração de valor público.

Registra-se, para fins metodológicos, que todos os eventos de riscos que passem pelo processo de gestão de riscos devem obrigatoriamente estar relacionados a possíveis impactos aos objetivos estratégicos do CNMP.

A tabela a seguir sintetiza a conexão entre objetos de análise, categorias principais e potenciais riscos secundários.

Tabela 27: Integração riscos e planejamento

OBJETOS	INSTRUMENTO	CATEGORIA PRINCIPAL	POTENCIAIS RISCOS SECUNDÁRIOS	VINCULAÇÃO
Objetivos Estratégicos, Visão e Missão do CNMP	Mandala Estratégica	Riscos Estratégicos	Riscos de Conformidade Riscos de Integridade Risco Reputacional	-
Objetivos Táticos e Propósito das Unidades	Painel de Contribuição	Riscos Táticos	Riscos Operacionais Riscos de Conformidade Riscos de Integridade Risco Reputacional	Riscos Estratégicos
Macroprocessos e processos	Cadeia de Valor	Riscos Operacionais	Riscos de Conformidade Riscos de Integridade Risco Reputacional	Riscos Estratégicos

Essa integração assegura que a gestão de riscos não seja tratada como atividade isolada, mas como parte do próprio ciclo de planejamento, execução, monitoramento e aperfeiçoamento institucional. Ao conectar objetivos estratégicos, objetivos táticos e macroprocessos da Cadeia de Valor, o CNMP fortalece a coerência entre estratégia e operação, amplia a capacidade de antecipar eventos que possam comprometer seus resultados e direciona os esforços de tratamento para os pontos de maior relevância institucional. Dessa forma, os Mapas

de Riscos das Unidades e o Painel Institucional de Riscos passam a atuar como instrumentos complementares de governança, apoiando decisões mais qualificadas, transparentes e orientadas à geração de valor público.

8.1 Integração com outros instrumentos institucionais

Os conceitos, critérios, escalas e instrumentos previstos neste Referencial poderão subsidiar outros processos, planos e documentos institucionais que demandem análise de riscos, vulnerabilidades, impactos, controles ou medidas de tratamento. Essa integração permite maior uniformidade metodológica, evita duplicidade de esforços e fortalece a coerência entre gestão de riscos, planejamento, continuidade, segurança, integridade, proteção de dados e governança.

Entre os instrumentos que poderão utilizar este Referencial, destacam-se a Política e o Plano de Continuidade do Negócio, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), os planos de ação decorrentes de auditorias, os programas e planos de integridade, os planos de segurança da informação, os diagnósticos de maturidade, os projetos institucionais e outros instrumentos de gestão que envolvam identificação, avaliação ou tratamento de riscos.

No âmbito dos projetos, a metodologia aqui apresentada poderá apoiar a identificação de eventos que possam comprometer escopo, prazo, custo, qualidade, entregas, conformidade, integridade, reputação ou geração de valor público. Dessa forma, os Mapas de Riscos, as escalas de probabilidade e impacto, a avaliação de controles e o registro das medidas de tratamento poderão ser utilizados como insumos para qualificar o planejamento, a execução, o monitoramento e a tomada de decisão em diferentes frentes institucionais.



REFERÊNCIAS

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Portaria CNMP-PRESI nº 85, de 17 de março de 2026. Institui a Política de Gestão de Riscos do Conselho Nacional do Ministério Público.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Portaria CNMP-PRESI nº 271, de 5 de outubro de 2026. Altera a Portaria CNMP-PRESI nº 85, de 17 de março de 2026, que institui a Política de Gestão de Riscos do Conselho Nacional do Ministério Público.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Portaria CNMP-PRESI nº 272, de 5 de outubro de 2026. Institui o Plano Bienal de Gestão de Riscos do Conselho Nacional do Ministério Público para o período compreendido entre o terceiro trimestre de 2026 e o segundo trimestre de 2028 e estabelece o escopo prioritário e o apetite institucional a riscos.

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

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise risk management: integrating with strategy and performance. Durham, NC: COSO, 2017.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Referencial básico de gestão de riscos. Brasília: TCU, 2018.

