CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

PORTARIA CNMP-PRESI Nº 214, DE 2 DE DEZEMBRO DE 2019.

Altera o anexo I da Portaria CNMP-PRESI nº 167, de 4 de dezembro de 2018, que institui o Plano de Gestão de Riscos e o Plano de Segurança Institucional do Conselho Nacional do Ministério Público.

O **PRESIDENTE DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO,** no uso das atribuições que lhe são conferidas pelos arts. 130-A, I, da Constituição Federal e 12, XIII e XVII, do Regimento Interno do Conselho Nacional do Ministério Público (Resolução n° 92, de 13 de março de 2013),

Considerando o resultado do projeto piloto de gestão de riscos, instituído pela Portaria CNMP-SG nº 33, de 7 de fevereiro de 2019, e o consignado na ata da 14ª Reunião do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI), inserida no Processo SEI nº 19.00.5000.0006202/2017-75, e da ata da 20ª Reunião do Comitê de Governança Corporativa e da Estratégia (CGCE), constante do Processo SEI nº 19.00.5000.0006202/2017-75, RESOLVE:

Art. 1º Alterar o anexo I da Portaria CNMP-PRESI nº 167, de 4 de dezembro de 2018, considerando as alterações aprovadas pelo SERSI e pelo CGCE, que passa a vigorar conforme o Anexo I desta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Brasília-DF, 2 de dezembro de 2019.

ANTÔNIO AUGUSTO BRANDÃO DE ARAS

Anexo I

Plano de Gestão de Riscos do CNMP

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

Plano de Gestão de Riscos do CNMP

Brasília, 2019

Presidente
Antônio Augusto Brandão de Aras

Corregedor Nacional
Rinaldo Reis Lima

Conselheiros
Valter Shuenquener de Araújo
Luciano Nunes Maia Freire
Luiz Fernando Bandeira de Mello Filho
Otavio Luiz Rodrigues Jr.
Sebastião Vieira Caixeta
Silvio Roberto Oliveira de Amorim Junior
Oswaldo D'Albuquerque Lima Neto
Fernanda Marinela de Sousa Santos
Sandra Krieger Gonçalves

Secretária-Geral
Mauricio Andreiuolo Rodrigues

Equipe de Elaboração
SERSI – Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional

SUMÁRIO

1. INTRODUÇÃO 5

2. TERMOS E DEFINIÇÕES 6

3. ESTRUTURA DE GESTÃO DE RICOS DO CNMP 7

3.1. DAS COMPETÊNCIAS 9

3.1.1. Do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional 9

3.1.2. Da Reunião de Acompanhamento Tático (RAT) 10

3.1.3. Do gestor de riscos 10

3.1.4. Da Secretaria-Geral e da Secretaria de Gestão Estratégica 11

4. PROCESSO DE GESTÃO DE RISCOS 12

4.1. ESTABELECIMENTO DO CONTEXTO 13

4.2. IDENTIFICAÇÃO E ANÁLISE DE RISCOS 14

4.2.1. Taxonomia de eventos de riscos e de causa 15

4.3. AVALIAÇÃO DE RISCOS 20

4.4. TRATAMENTO DE RISCOS 26

4.5. MONITORAMENTO E ANÁLISE CRÍTICA 28

4.6. COMUNICAÇÃO E CONSULTA 29

5. REFERÊNCIAS 30

1. INTRODUÇÃO

No dia 1º de março de 2016, o Comitê de Governança Corporativa e da Estratégia (CGCE), em reunião ordinária, aprovou a criação de Grupo de Trabalho para estudar e propor a Cadeia de Valor e as políticas de gestão de riscos e de segurança institucional do CNMP (GT-Riscos), em atendimento ao Acordão nº 1273/2015–TCU–Plenário e ao disposto no art. 27 da Portaria CNMP-PRESI nº 36, de abril de 2016, revogada pela Portaria CNMP-PRESI nº 25, de fevereiro de 2018. Ao final de dezesseis encontros com profícuos debates sobre o tema, o Grupo concluiu três produtos: a Cadeia de Valor do CNMP (Portaria CNMP-PRESI nº 37, de 18 de abril de 2017); a Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45, de 27 de abril de 2017); e a Política de Segurança Institucional (Portaria CNMP-PRESI nº 153, de 7 de dezembro de 2017).

A Cadeia de Valor do CNMP consiste na representação gráfica dos principais macroprocessos que agregam valor à instituição, alinhada à possibilidade de análise das relações entre eles e como cada um deles contribui para o cumprimento das atribuições do órgão. Já as Políticas de Gestão de Riscos e de Segurança Institucional estabelecem objetivos, princípios, diretrizes, recursos, responsabilidades e procedimentos em conformidade com as melhores práticas adotadas pelo setor público, alinhados com o Planejamento Estratégico e a Cadeia de Valor do CNMP.

Essas iniciativas têm por objetivo minimizar os riscos das principais atividades aqui desenvolvidas e aumentar a segurança da instituição em sua atuação, tendo por consequência maior eficiência na prestação de serviços para a sociedade.

Este documento detalhará a Política de Gestão de Riscos do CNMP, servindo de referência para todas as unidades do CNMP, sem prejuízo da utilização de outras normas complementares específicas relativas à Instituição ou suas unidades. Este plano tem como escopo de aplicação os processos de trabalho do terceiro nível da Cadeia de Valor do CNMP.

Para a elaboração deste documento, foram utilizados planos e manuais de referência, quais sejam, *Enterprise Risk Management – Integrated Framework* (COSO II) e a norma ABNT NBR ISO 31000. Além disso, foi feito *benchmarking* nas seguintes instituições: Tribunal de Contas da União, Ministério do Planejamento, Desenvolvimento e Gestão; Ministério da Transparência e Corregedoria-Geral da União, Tribunal Superior do Trabalho, Tribunal Regional do Trabalho da 18ª Região e Tribunal Regional Eleitoral do Rio Grande do Sul.

2. TERMOS E DEFINIÇÕES

Para fins deste documento, consideram-se os seguintes conceitos:

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

- Objeto de avaliação de riscos: processos de trabalho do terceiro nível da Cadeia de Valor do CNMP.

- Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade.

- Gestor de riscos: pessoa ou entidade com responsabilidade e autoridade para gerenciar um risco.

- Controle interno: conjunto de atividades, planos, métodos, indicadores e procedimentos interligados, estabelecidos com vistas a assegurar que os diversos objetivos das unidades do CNMP sejam alcançados, evidenciando eventuais desvios.

- Contexto externo: ambiente externo no qual a organização busca atingir seus objetivos.

- Contexto interno: ambiente interno no qual a organização busca atingir seus objetivos.

- Eventos de risco: incidente ou uma ocorrência que afeta a realização dos diversos objetivos do CNMP.

- Consequências: resultado de um evento que afeta os diversos objetivos do CNMP.

- Causas: condições que viabilizam a concretização de um evento que afetam os objetivos. São resultantes da junção das fontes de risco com as vulnerabilidades.

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

- Vulnerabilidades: Ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.

- Nível de risco: magnitude de um risco, expressa em termos da combinação das probabilidades e do impacto.

- Risco: possibilidade que um evento, iminente ou futuro, ocorra e afete negativamente a realização dos objetivos do CNMP.

    - Risco inerente: risco ao qual os processos de trabalho do CNMP estão sujeitos, desconsiderados os controles existentes.

    - Risco residual: risco remanescente após a incidência dos controles aplicados.

- Risco emergente: risco decorrente da adoção das medidas de controle para um risco inerente ou residual.

- Critérios de risco: padrão de referência para a avaliação dos riscos.
- Apetite a risco: nível de risco que o CNMP se dispõe a aceitar na busca por agregar valor aos serviços prestados.
- Análise de riscos: processo de compreender a natureza do risco e determinar o nível de risco.
- Avaliação de riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.
- Tratamento de riscos: abordagem do CNMP após avaliar o risco e, a partir daí, adotar medidas para evitá-lo, transferi-lo/compartilhá-lo, mitigá-lo e, eventualmente, aceitá-lo.
- Medida de controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.
- Matriz RACI: corresponde à sigla para *Responsible*, *Accountable*, *Consulted* e *Informed* (em português, pode-se traduzir livremente para Responsável, Aprovador, Consultado e Informado). Assim, a matriz RACI é uma ferramenta por meio da qual cada colaborador toma consciência de suas atribuições durante o processo de gestão de riscos. É uma matriz de distribuição de responsabilidades.

3. ESTRUTURA DE GESTÃO DE RISCOS DO CNMP

Segundo a norma ISO 31000[1], a gestão de riscos em uma organização possui três pilares: os princípios, a estrutura e o processo.

No âmbito do CNMP, nos termos dos art. 3º e 4º da Portaria CNMP-PRESI nº 45, de 27 de abril de 2017, os princípios foram desdobrados em diretrizes e objetivos, respectivamente, conforme quadro abaixo:

Quadro 1 – Diretrizes da Gestão de Riscos do CNMP

Princípios da Gestão de Riscos no CNMP	Diretrizes	• Conformidade dos processos à legislação aplicável • Alinhamento ao Planejamento Estratégico e à Cadeia de Valor • Promoção dos valores institucionais • Disseminação da cultura de gestão de riscos • Adequação do apetite ao risco às estratégias adotadas • Comprometimento das partes envolvidas nos processos organizacionais de tomada de decisões

[1] A ISO 31000 é uma norma da família de gestão de risco criada pela International Organization for Standardization. Seu objetivo é estabelecer princípios e orientações genéricas sobre gestão de riscos nas organizações.

		• Dinamismo, iteratividade e capacidade de reagir a mudanças • Fomento à melhoria contínua da gestão
	Objetivos	• Identificar potenciais eventos que afetem o alcance da missão institucional • Fornecer informações íntegras para o processo de tomada de decisão • Aprimorar os processos de controle interno

Em relação à estrutura de gestão de riscos, a referida ISO conceitua que é o "*conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização".* Ainda dentro da estrutura, a norma mencionada trata dos seguintes componentes: Mandato e Comprometimento, Concepção da Estrutura para Gerenciar Riscos, Implementação da Gestão de Riscos, Monitoramento e Análise Crítica da Estrutura e Melhoria Contínua da Estrutura.

No CNMP, o componente Mandato e Comprometimento é demonstrado pelas ações do Comitê do Governança Corporativa e da Estratégia (CGCE), do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI) e da alta administração em promover a Gestão de Riscos do CNMP.

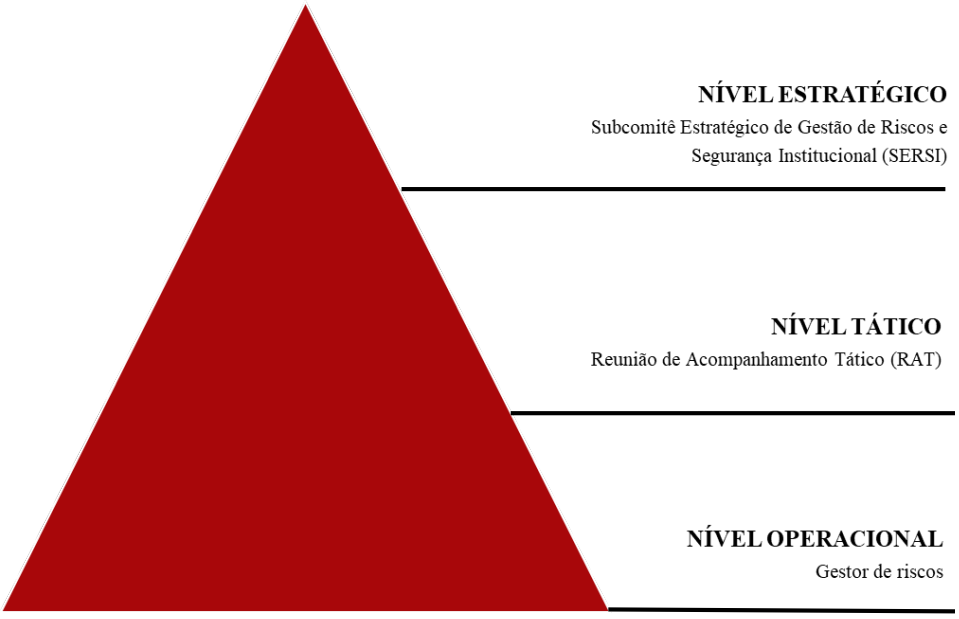
Na concepção da Estrutura para Gerenciar Riscos, além do CGCE, foi definida a Política de Gestão de Riscos por meio da Portaria CNMP-PRESI nº 45/2017 e foi instituído o SERSI pela Portaria CNMP-PRESI nº 50, de 24 de abril de 2018, normativos que definem o processo de gestão de riscos e as competências e responsabilidades.

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar na estrutura e na metodologia de Gestão de Riscos do CNMP, é prevista revisão da Política de Gestão de Riscos e deste Plano em período não superior a dois anos (Melhoria Contínua da Estrutura). Porém, mudanças no contexto do CNMP podem provocar a necessidade de implantação de melhorias de forma antecipada, desde que propostas pelo SERSI e aprovadas pela Secretaria-Geral do CNMP, conforme inciso III do art. 10-E da Portaria CNMP-PRESI nº 50, de 24 de abril de 2018, que altera a Portaria CNMP-PRESI nº 160/2014, instituindo o SERSI no âmbito do CGCE.

3.1. DAS COMPETÊNCIAS

As competências quanto à gestão de riscos do CNMP foram definidas na Política de Gestão de Riscos, na Portaria que institui o SERSI, bem como neste documento. Desse modo, a governança de gestão de riscos configura-se conforme a Figura 1:

Figura 1 – Dimensões da estrutura de governança de gestão de riscos



Ressalta-se, ainda, que os níveis de riscos serão tratados em suas respectivas instâncias de governança conforme a Seção 4.4, que define as diretrizes para resposta perante o nível do risco identificado.

3.1.1. Do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional

A principal instância de governança sobre gestão de riscos do CNMP é o SERSI, instituído por meio da Portaria CNMP-PRESI nº 50, de 24 de abril de 2018. Vinculado ao CGCE, o Subcomitê Estratégico é composto por representantes das seguintes unidades: Presidência; Corregedoria Nacional; Secretaria-Geral; Comissões; Secretaria de Gestão Estratégica; Secretaria de Administração; Secretaria Processual; Secretaria de Tecnologia da Informação; Assessoria de Comunicação Social; Auditoria Interna; Coordenadoria Gestão de Pessoas e Coordenadoria de Segurança e Transporte.

As competências do SERSI estão definidas no art. 10-E da Portaria CNMP-PRESI nº 160/2014, quais sejam:

- analisar e deliberar sobre riscos ou ameaças que possam comprometer a prestação de serviços, a imagem junto à sociedade, a autonomia e a efetividade dos resultados no alcance da estratégia;
- monitorar, avaliar e propor a revisão das Políticas de Gestão de Riscos e de Segurança Institucional, periodicamente, submetendo-as à apreciação da Presidência do CNMP;
- elaborar, monitorar, avaliar e propor a revisão do Plano de Gestão de Riscos e do Plano de Segurança Institucional, submetendo-os à deliberação da Secretaria-Geral;
- definir, anualmente, o apetite a riscos do CNMP, conforme previsto na Política de Gestão de Riscos do CNMP; e
- avaliar a eficácia e a efetividade do processo de gerenciamento de riscos e da segurança institucional.

3.1.2. Da Reunião de Acompanhamento Tático (RAT)

A Reunião de Acompanhamento Tático (RAT) é definida na Portaria CNMP-PRESI nº 25/2018 e é realizada entre o secretário-geral, a chefia de gabinete da Presidência e os titulares de secretarias e da Auditoria Interna para riscos afetos à atividade-meio; e entre o secretário-geral, a chefia de gabinete da Presidência e os integrantes da cada Comissão, da Corregedoria Nacional, da Ouvidoria Nacional, da Unidade Nacional de Capacitação do Ministério Público e dos Gabinetes dos conselheiros para riscos afetos à atividade finalística.

3.1.3. Do gestor de riscos

A Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45/2017) define as seguintes competências aos gestores de riscos, relativamente aos objetos de avaliação de riscos sob sua responsabilidade:

- escolher, justificadamente, dentre os objetos (objetivos estratégicos e de contribuição, ações, projetos, iniciativas, ativos e processos de trabalho) sob sua responsabilidade, quais terão os riscos gerenciados, à vista da dimensão dos prejuízos que possam causar;
- assegurar que o risco seja gerenciado de acordo com os critérios do processo de gestão de riscos estabelecidos neste Plano; e

- gerar e reportar informações adequadas sobre a gestão de riscos às instâncias de governança.

Ainda, de acordo com o art. 15 da Portaria CNMP-PRESI nº 45/2017, são considerados **gestores de riscos**, dentre outros, o Presidente, o Corregedor Nacional, o Ouvidor Nacional, os Conselheiros, os presidentes e membros auxiliares das comissões permanentes e temporárias, o Secretário-Geral, os secretários e titulares de unidades administrativas.

3.1.4. Da Secretaria-Geral e da Secretaria de Gestão Estratégica

Compete à Secretaria-Geral presidir o SERSI, realizar estudos e adotar as medidas necessárias para a edição, pela Presidência, de atos normativos dispondo sobre a gestão do conhecimento e a implementação da gestão de riscos e segurança institucional, nos termos do art. 27 da Portaria CNMP-PRESI nº 25/2018.

Para assessorar a SG, segundo o §5º do art. 10-E da Portaria CNMP-PRESI nº 160/2014, a coordenação do processo de gestão riscos do CNMP compete à Secretaria de Gestão Estratégica (SGE). Desse modo, especificam-se as seguintes competências:

- auxiliar o SERSI na definição e nas atualizações da estratégia de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
- dar suporte à identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;
- consolidar os resultados das diversas unidades em relatórios gerenciais e encaminhá-los às instâncias de governança e monitoramento;
- oferecer capacitação continuada em Gestão de Riscos para os servidores do CNMP;
- promover a disseminação da cultura de gestão de riscos; e
- requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

4. PROCESSO DE GESTÃO DE RISCOS

A gestão de riscos no CNMP explicitada neste documento dar-se-á sobre os processos de trabalho constantes do 3º nível da Cadeia de Valor. Cabe aos gestores de risco, conforme as responsabilidades definidas na Política de Gestão de Riscos, escolher os processos que terão os riscos gerenciados e tratados com prioridade em cada unidade do CNMP, em face da dimensão dos prejuízos que a não gestão dos riscos possa causar. Ainda podem ser levados em consideração critérios de escolha, tais como: o alinhamento do processo com os objetivos estratégicos do CNMP e o impacto em caso de incidentes ou o custo do processo.

Definido o processo de trabalho, convém ao gestor de riscos elaborar uma matriz RACI, que estabelece as responsabilidades específicas para cada atividade da gestão de riscos em cada unidade. Assim, o responsável (R) é quem efetivamente irá executar a atividade; o aprovador (A) é o responsável pelo aceite formal da atividade ou produto entregue, podendo delegar a função para outros profissionais, mas não a responsabilidade; o consultado (C) é a pessoa que possa fornecer informação sobre a referida atividade; e o informado (I) é a pessoa ou os grupos de pessoas que precisam ser notificados de resultados ou ações tomadas, mas não precisam estar envolvidos no processo de tomada de decisão. O Quadro 2 apresenta um modelo de matriz de responsabilidades (RACI).

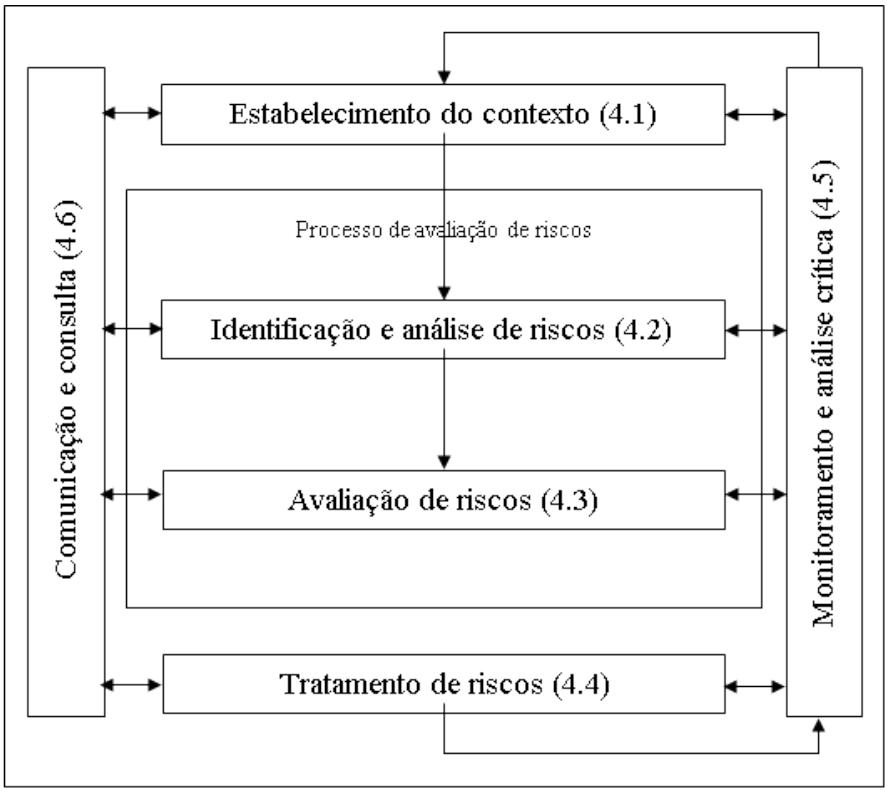
Quadro 2 – Matriz RACI para o processo de gerenciamento de riscos

Atividade	SG	SERSI	SGE	Gestor de Riscos	Servidor
Estabelecer o contexto					
Identificar os riscos					
Analisar os riscos					
Avaliar os riscos					
Tratar os riscos					
Elaborar o Plano de Tratamento de Riscos					
Monitoramento e análise crítica					
Comunicar e consultar					
Capacitar envolvidos					

R *– Responsável;* ***A*** *– Aprovador;* ***C*** *– Consultado;* ***I*** *– Informado*

Uma vez definida a priorização, dar-se-á início ao processo de gestão de riscos, conforme modelo da Norma ABNT NBR 31000:2009, adaptada à realidade do CNMP (Figura 2).

Figura 2 – Processo de gestão de riscos



Fonte: ABNT NBR 31000:2009 (adaptada)

Assim, o processo é composto por 6 (seis) atividades que interagem de forma cíclica. Abaixo, encontra-se a definição de cada atividade e os principais artefatos e atores envolvidos.

4.1. ESTABELECIMENTO DO CONTEXTO

Nesta etapa, devem ser identificados, pelo menos:

- Descrição resumida do processo de trabalho que terá os riscos gerenciados;
- Objetivos a serem alcançados pelo processo de trabalho; e
- Justificativa para a aplicação do processo de gerenciamento de riscos no processo de trabalho.

Também é necessária a definição dos critérios de risco a serem levados em consideração ao gerenciar riscos no CNMP. Essa atividade é de fundamental importância, pois é a partir dela que todas as demais atividades serão desenvolvidas. A fim de deixar o plano mais didático, os critérios de riscos serão definidos ao longo das demais atividades, à medida que forem sendo utilizados.

4.2. IDENTIFICAÇÃO E ANÁLISE DE RISCOS

A identificação dos riscos consiste na busca, no reconhecimento e na descrição de riscos, mediante a identificação das fontes de risco, eventos e suas causas. A finalidade dessa etapa é gerar uma lista abrangente de eventos que possam evitar, prejudicar, impedir ou atrasar o cumprimento dos objetivos do processo de trabalho. A identificação abrangente é fundamental, pois um risco que não é identificado nesta fase não será incluído em análises posteriores.

Nessa fase, o gestor deverá utilizar, como referência, as taxonomias de eventos de riscos e de causas definidas no item 4.2.1. Para a identificação dos riscos, o gestor pode utilizar técnicas como *brainstorming*[2], entrevista com especialistas, entre outras. Uma vez identificado o risco, o gestor deverá categorizá-lo como estratégico, operacional, de conformidade ou de integridade. Vale ressaltar que um risco pode ser classificado em mais de uma categoria. Destaca-se que essas categorias de riscos estão definidas nos incisos V a VIII do art. 2º da Portaria CNMP-PRESI nº 45/2017.

Identificados e categorizados os riscos, convém analisá-los de forma criteriosa, pois essa análise fornece subsídios para a avaliação de riscos, bem como para as estratégias, métodos e decisões de tratamento dos riscos. A análise envolve a apreciação das causas e das fontes de riscos, suas consequências negativas e a probabilidade de que esses eventos venham a ocorrer.

Nessa etapa, é importante apontar os fatores que afetam as consequências e a probabilidade de ocorrência dos riscos, ou a combinação de ambos, confrontados com os controles existentes, a fim de testar a eficácia e a eficiência desses controles. A combinação das consequências, as quais podem ser expressas em termos de impactos tangíveis e intangíveis, com a probabilidade, serve para determinar o nível do risco inerente.

O Quadro 3 apresenta o Formulário de Identificação e Análise de Riscos:

---

[2] O *brainstorming*, em português, significa tempestade de ideias. É uma técnica de dinâmica de grupo utilizada no levantamento do maior número de ideias e soluções possíveis para um problema particular e necessariamente real.

Quadro 3 – Formulário de Identificação e Análise de Riscos

Processo de trabalho objeto de Avaliação de Riscos:					**Copilado por: Data:**
Objetivo do processo de trabalho:					**Analisado por: Data:**
Justificativa para o gerenciamento dos riscos:					
Riscos Identificados					
ID	**Eventos de Risco**	**Detalhamento do risco**	**Causa**	**Observações sobre a causa**	**Categoria do risco**
1					
2					
3					

4.2.1. Taxonomia de eventos de riscos e de causa

A taxonomia de eventos de riscos está dividida em quinze categorias distintas, compondo o nível 1. Esse nível pode ser subdividido em até dois subníveis de categoria (nível 2 e 3), mutuamente excludentes.

No caso de dúvidas sobre qual das subcategorias adotar na classificação de um evento de risco, considera-se aquele que representa melhor esse evento de risco. Se um evento de risco não tiver condições de ser enquadrado em nenhuma das taxonomias, a equipe do levantamento de riscos pode criar uma nova subcategoria, a qual, posteriormente, será submetida ao SERSI para deliberação.

Quadro 4 – Taxonomia de eventos de riscos

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
1. Fraude Interna	**1.1. Atividade não autorizada**		Perda decorrente de ações não autorizadas, não comunicadas ou realizadas de forma enganosa por membro, servidor, estagiário ou terceirizado, para obter benefício pessoal ou terceiros, violando normas, controles internos e leis, de forma intencional.	Exemplos: vazamento de informações, alteração de dados, conluio, entre outros.
	1.2. Furto		Perda derivada de ato interno intencional com o objetivo de apropriar indevidamente valores financeiros, bens físicos ou informações. Pode incluir apropriação indébita, roubo, furto de	Ações de vandalismo devem ser classificadas

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
			informações eletrônicas, entre outros.	como "Terrorismo e vandalismo".
2. Fraude Externa	**2.1. Furto e Fraude**		Perda derivada de ato de terceiros com o objetivo de apropriar valores financeiros, bens físicos ou informações do CNMP ou de terceiros, como por exemplo, enviar documentação incorreta ou enganosa.	Exceção: ações de vandalismo e furto de dados via meio eletrônico (classificar em "invasão de sistemas").
	2.2. Invasão de Sistemas		Perda derivada de acesso não autorizado que visa burlar o sistema, explorar suas vulnerabilidades ou furtar dados da instituição ou de seus usuários.	Exemplo: *acking*, ataque de vírus, entre outros.
3. Uso indevido de autoridade	**3.1. Contra o exercício profissional**		Atentar contra os direitos e garantias legais assegurados ao exercício profissional com abuso ou desvio do poder hierárquico ou sem competência legal para atender interesse próprio ou de terceiros. Proceder a qualquer tentativa de obrigar o servidor a executar o que evidentemente não está no âmbito das suas atribuições ou a deixar de executar o que está previsto.	
	3.2. Contra a honra e o patrimônio		Atentar contra a honra ou o patrimônio de pessoa natural (no caso, servidor público) ou jurídica com abuso ou desvio de poder ou sem competência legal para atender interesse próprio ou de terceiros.	
4. Nepotismo			Nomear, designar, contratar ou alocar familiar de Conselheiro ou de ocupante de cargo em comissão ou função de confiança para exercício de cargo em comissão, função de confiança ou para a prestação de serviços no CNMP.	
5. Conflito de interesses			Exercício de atividades incompatíveis com as atribuições do cargo; Intermediação indevida de interesses privados; Concessão de favores e privilégios ilegais a pessoa jurídica; Recebimento de presentes/vantagens.	
6. Ameaças à imparcialidade e à autonomia técnica			Ser influenciado a agir de maneira parcial por pressões internas ou externas indevidas, normalmente ocorridas entre pares, por abuso de poder, por tráfico de influência ou constrangimento ilegal.	
7. Conduta profissional inadequada			Deixar de realizar as atribuições conferidas com profissionalismo, honestidade, imparcialidade, responsabilidade, seriedade, eficiência, qualidade e/ou urbanidade.	
8. Uso indevido ou manipulação de dados/ informações			Divulgação ou uso indevido de dados ou informações; alteração indevida de dados/informações; restrição de publicidade ou de acesso a dados ou informações	
9. Desvio de pessoal ou de			Desviar ou utilizar, em obra ou serviço particular, veículos, máquinas, equipamentos ou material de qualquer natureza, de	

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
recursos materiais			propriedade ou à disposição de entidades públicas, bem como o trabalho de servidores públicos, empregados ou terceiros contratados por essas entidades para fins particulares ou para desempenho de atribuição que seja de sua responsabilidade ou de seu subordinado.	
10. Dano a bens físicos	**10.1. Desastres e outros eventos**	10.1.1 Desastres	Perdas decorrentes de tempestades, erosão, quedas de raios, vendaval, incêndio, explosão, queda de equipamentos, danos de obras, etc.	
		10.1.2 Terrorismo e Vandalismo	Perda decorrente de ações de terrorismo ou vandalismo.	
11. Interrupção de atividade e falha de sistema	**11.1. Sistemas**	11.1.1 *Software*/ *Hardware*/ Rede	Inclui indisponibilidade ou falha da rede de processamento, transmissão e de comunicação ou dimensionamento incorreto de hardware.	É válido para sistemas ou equipamentos dos quais a unidade é fornecedor e não usuário. Se usuário, tratar como causa TIC
		11.1.2 Telecomunicações	Inclui indisponibilidade ou falha da rede de processamento, transmissão e de comunicação.	
		11.1.3 Serviços de infraestrutura e fornecimentos essenciais	Inclui indisponibilidade de serviços públicos como, por exemplo, fornecimento de eletricidade, água e esgoto, correios, entre outros.	
12. Execução e Gerenciamento de Processos e de Informação	**12.1. Execução e Gerenciamento de Processos**	12.1.1 Erro de informação	Perda ou falha derivada de informações inexatas, incorretas, desatualizadas ou incompletas que são produtos do processo	
		12.1.2. Falha na execução de processos/ práticas de *compliance*	Perda derivada de processamento inadequado ou incorreto de rotinas, procedimentos, sistemas de controle e modelos, de forma não intencional. Também inclui a operacionalização inadequada de sistemas tecnológicos.	Não engloba falha interna no sistema tecnológico decorrente de manutenção ou desenvolvimento. O evento deve ser classificado em como "interrupção de atividades e falha de sistemas".
		12.1.3 Perda de prazo/ atraso atendimento de demandas	Perda ou falha derivada de atividades realizadas fora do horário determinado ou de forma não tempestiva.	
		12.1.4 Erro	Perda derivada de registro contábil não confiável (inexato, incorreto ou incompleto).	

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
		contábil		
	12.2. Gerenciamento da informação	12.2.1. Erro/ não de divulgação de informação interna	Perda derivada de informações não divulgadas em documentos internos ou de forma não confiável (inexatas, incorretas, incompletas).	Exemplos: comunicados, relatórios, ordens de serviço, Intranet, entre outros.
		12.2.2. Erro/ não de divulgação de informação externa	Perda derivada de informações não divulgadas em documentos externos de forma não confiável (inexatas, incorretas, incompletas).	
	12.3. Fornecedor	12.3.1. Produto/ serviço não conforme	Perda derivada de execução ou entrega defeituosa de produtos e serviços (prazo, qualidade, quantidade, custos).	
		12.3.2. Disputas legais	Perda relacionada às discordâncias das obrigações contratuais ou legais.	
		12.3.3. Falência	Perdas decorrentes da falência do fornecedor.	
13. Prática Trabalhista e Segurança do Trabalho	**13.1. Recursos Humanos e Cultura**		Perda relacionada com a gestão de pessoal ao longo de todo o ciclo produtivo, desde o recrutamento até o término do vínculo trabalhista, que podem levar à queda de produtividade, dificuldade de retenção, *turnover*, litígio ou processos judiciais.	Pode incluir questões relacionadas com discriminação, assédio, greve, remuneração, reposição de mão de obra, entre outros.
	13.2. Segurança do Trabalho		Perda relacionada com condições e práticas trabalhistas insalubres ou inapropriadas, violência pessoal, perigos relacionados com deslocamento ou viagens a serviço, que afetam a saúde e segurança do servidor, independente da gravidade.	
14. Práticas de Negócio e legal	**14.1. Partes interessadas**	14.1.1. Obrigação legal	Perda derivada de falhas no relacionamento com a população e órgãos públicos decorrente de não cumprimento de leis, regras ou regulamentações.	Inclui mau uso de Informações confidenciais, deixar de cumprir obrigações legais, entre outros.
		14.1.2. Práticas de mercado	Perdas decorrentes do não envio ou do envio de propostas superestimadas ou subestimadas e do fato de o contrato já não ser mais vantajoso para a administração.	
15. Restrições orçamentárias			Perdas derivadas de restrições e contingenciamento orçamentários.	

Para cada risco identificado são também investigadas suas possíveis causas. Podem ocorrer situações em que sejam detectadas mais de uma causa, independente da origem.

Cada causa deve ser classificada com base na taxonomia de causas, que está dividida em causas internas (Quadro 5) e externas (Quadro 6), cada qual com várias subcategorias.

As causas internas são aquelas que surgem dentro da organização e as externas são aquelas que surgem fora da organização.

Quadro 5 – Taxonomia de causas internas

Nível 1	Nível 2	Descrição
1. Recursos Humanos	**1.1. Turnover**	
	1.2. Número de servidores	
	1.3. Gestão do conhecimento institucional	Eventos relacionados a ausência de compilação e valorização dos precedentes (Base de Conhecimento, manuais e enunciados).
	1.4. Gestão de competências	Eventos relacionados a deficiências no desenvolvimento de competências e habilidades do servidor e/ou do superior hierárquicos; trabalhos que demandam competências específicas; interpretação equivocada dos normativos, entre outro; ausência de mecanismos de aferição do desempenho dos servidores da organização
	1.5. Greve	
	1.6. Carga de trabalho	Eventos relacionados à incapacidade de gerir o tempo; capacidade operacional insuficiente em relação às demandas, entre outros
	1.7. Clima organizacional	Eventos relacionados à desmotivação, qualidade de vida, saúde do servidor, entre outros.
	1.8. Cultura organizacional	Falta de comprometimento do servidor com os objetivos institucionais e com o serviço prestado; interferência nos trabalhos da equipe por agentes externos (ex: políticos e gestores institucionais).
	1.9. Outros RH	Má-fé do servidor e/ou do superior hierárquico (perseguição, amizade, preferência etc.); o normativo favorece a discricionariedade para a prática do ato; solicitações indevidas indiretas ou diretas por autoridades; pressão familiar; falta de comunicação do servidor quanto à sua suspeição; falta de atenção (não intencional).
2. Tecnologia da		Eventos relacionados à disponibilidade de recursos de TI, como *hardware*, *software*, sistemas obsoletos ou ausentes,

Nível 1	Nível 2	Descrição
Informação		demandas internas por recursos de TI e outros.
3. Gerenciamento	**3.1. Planejamento**	Eventos relacionados à formulação das orientações estratégicas e seus desdobramentos (indicadores de desempenho, estabelecimento de metas para as ações, etc.); não aderência às diretrizes e procedimentos da organização, entre outros.
	3.2. Controle	Eventos relacionados ao monitoramento e implementação de controles.
	3.3. Organização	Eventos relacionados à forma de coordenar e adequar os recursos organizacionais.
	3.4. Liderança	Eventos relacionados às competências do líder/gestor em comunicar diretrizes, objetivos, metas; estimular a prática de valores organizacionais; promover a integração das equipes e com outros componentes do CNMP; tomar decisões; articular interesses; priorizar ações; inovar; delegar; resolver conflitos, entre outros.
	3.5. Outros Gerenciamento	Deficiências nos fluxos dos processos de trabalho e de informações entre as unidades da organização; fragilidade no processo de comunicação de informações produzidas ou custodiadas pelo CNMP
4. Recursos Financeiros		Eventos relacionados com indisponibilidade de recursos financeiros.
5. Recursos Materiais		Eventos relacionados com qualidade inadequada, carência de recursos materiais ou obsolescência.
6. Segurança Institucional		Eventos relacionados à segurança orgânica (segurança de pessoas, de materiais, das áreas e instalações e de informação) e segurança ativa, tais como sabotagem, propaganda adversa e espionagem.
7. Regulação		Eventos relacionados com mudanças no ambiente legal e regulatório.

Quadro 6 – Taxonomia de Causas Externas

Nível 1	Descrição
1. Econômica	Eventos relacionados com mudança do ambiente econômico.
2. Política	Eventos relacionados com fatores do ambiente político que podem comprometer os resultados do macroprocesso, projeto ou iniciativa.
3. Regulação	Eventos relacionados com mudanças no ambiente legal e regulatório.
4. Energia elétrica	Eventos relacionados à disponibilidade de fornecimento de energia elétrica.
5. Telecomunicações	Eventos relacionados à disponibilidade de fornecimento de telecomunicações.
6. Terceiros	Eventos decorrentes da relação com terceiros.
7. Fornecedores	Eventos decorrentes da relação com fornecedores (relação contratual).

4.3. AVALIAÇÃO DE RISCOS

A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados das etapas anteriores, sobre quais riscos necessitam de tratamento e a prioridade para a implementação das ações de tratamento do risco.

A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios do processo de gestão do CNMP, quais sejam: probabilidade, impacto, apetite a riscos, matriz de classificação de riscos, diretrizes para priorização e tratamento, e matriz da eficácia dos controles.

A probabilidade diz respeito às chances de um evento ocorrer. Dessa forma, o Quadro 7 define os graus de probabilidade e os respectivos níveis.

Quadro 7 – Escala de probabilidade

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

Fonte: Adaptado de Plano de Gestão de Riscos (TST, 2015)

O impacto, por sua vez, está relacionado às consequências do evento nos objetos, caso ele ocorra. Visando a diminuir a subjetividade do método, optou-se por definir o nível desse impacto considerando as dimensões financeira, reputacional e de negócios no objetivo do processo de trabalho analisado.

Para cada cruzamento de risco é feita a avaliação dos impactos dos eventos identificados nas três dimensões:

1. **Impacto na dimensão financeira:** O impacto na dimensão financeira avalia a perda financeira gerada pelo evento de risco como, por exemplo, pagamento de multas, litígios, compensações, custas legais, negociações mal concluídas, ressarcimento de danos de bens, etc.

2. **Impacto na dimensão reputacional:** Do ponto de vista da dimensão reputacional, avalia-se como um evento de risco pode prejudicar a reputação e credibilidade do

CNMP. O efeito reputacional adverso deve estar vinculado à imagem externa do CNMP, ou seja, sua imagem perante o Ministério Público, fornecedores, órgão de governo, parceiros e a sociedade em geral.

3. **Impacto na dimensão de negócios:** Na dimensão de negócios, busca-se avaliar se a ocorrência de um evento compromete o negócio a ponto de afetar a entrega de um produto ou serviço, inclusive aqueles intimamente relacionados ao planejamento estratégico ou até o cumprimento da missão. Para avaliar o impacto na dimensão negócio, devem ser consideradas as definições de missão, visão e planejamento estratégico.

Desse modo, primeiramente o gestor deve analisar o impacto nessas dimensões, conforme quadro abaixo:

Quadro 8 – Escala de impacto

Financeiro	Reputacional	Negócios	Nível
Impacto foi insignificante.	Impacto insignificante.	Impacto insignificante.	1
Perda ou estimativa até R$20.000 (x <= R$20.000).	Eventos que se limitam às partes envolvidas, tenham caráter pontual e/ou não tenham sido divulgados em qualquer mídia.	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance das metas do processo.	2
Perda ou estimativa entre R$20.000 e R$176.000 (R$ 20.000 < x <= R$ 176.000).	Eventos que envolvam membros ou gestores do CNMP, tenham impactos de curto prazo e/ou tenham alcançado mídias institucionais do Ministério Público.	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance dos objetivos do CNMP.	3
Perda ou estimativa de perda entre R$176.000 a R$1.430.000 (R$176.000 < x <= R$ 1.430.000).	Eventos que envolvam a Presidência, os Conselheiros, a Corregedoria e/ou a Secretaria-Geral, tenham impacto de médio prazo e/ou alcançado a mídia nacional.	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance da visão do CNMP.	4
Perda ou estimativa de perda maior que R$1.430.000 (x > R$ 1.430.000).	Eventos que envolvam a Presidência, os Conselheiros, a Corregedoria e/ou a Secretaria-Geral, tenham impacto de longo prazo e/ou tenham alcançado a mídia internacional	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance da missão do CNMP.	5

Fonte: Adaptado do BCB

Em relação ao Quadro 8, pode ocorrer de os níveis serem diferentes para cada dimensão. Nesse caso, o gestor de riscos deve considerar o nível mais alto. Por exemplo, caso na dimensão Financeira o gestor considere que o impacto é insignificante (nível 1) e na dimensão Negócios considere que o evento de risco impacta na entrega do produto ou serviço de tal forma que

prejudica o alcance das metas do processo (nível 2), o nível de impacto a ser considerado será o 2.

Tendo em mãos os níveis de probabilidade e impacto, o gestor de riscos deve fazer a multiplicação desses níveis, que define o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

O risco pode ser classificado dentro das seguintes faixas:

Quadro 9 – Classificação do risco

Classificação	Faixa
Risco Baixo	0 – 4,99
Risco Médio	5,00 – 9,99
Risco Alto	10,00 – 14,99
Risco Extremo	15,00 – 25,00

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

Quadro 10 – Matriz de riscos

Nível de Risco **Extremo** **Alto** **Médio** Baixo		**PROBABILIDADE**				
		Muito baixa 1	**Baixa 2**	**Média 3**	**Alta 4**	**Muito alta 5**
IMPACTO	**Muito alto 5**	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito baixo 1	1	2	3	4	5

Para finalizar os critérios de riscos, o CNMP definiu a Tabela da Eficácia dos Controles Existentes (Quadro 11), a qual estabelece critérios objetivos para análise dos controles implementados e para cálculo do risco residual. Esse quadro deve ser aplicado logo após a definição dos níveis de riscos, caso já existam controles implementados, e após a adoção das medidas de tratamento dos riscos.

Quadro 11 – Eficácia dos controles existentes

Eficácia do Controle	Situação do controle	Multiplicador do Risco Inerente
Inexistente	Ausência completa de controle.	1,0
Fraco	Controle parcialmente implantado e com deficiências. Geralmente depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	0,8
Mediano	Controle parcialmente implantado. Entretanto, pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	0,6
Satisfatório	Controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade.	0,4
Forte	Controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.	0,2

Fonte: Plano de Gestão de Riscos (TST, 2015)

Ressalta-se, também, que o apetite a risco do CNMP levará em consideração o risco no nível baixo, ou seja, para riscos nesse nível, não há a necessidade de ações e medidas de tratamento. Assim, basta apenas o seu monitoramento constante para assegurar que eles ainda se encontram nesses patamares.

O Quadro 12 representa o Formulário de Avaliação de Riscos:

Quadro 12 – Formulário de Avaliação de Riscos

Processo de trabalho objeto de Avaliação de Riscos:											**Compilado por:** **Data:**
Objetivo do processo de trabalho:											**Analisado por:** **Data:**
Riscos Identificados					**Probabilidade**	**Impacto**	**Risco Inerente**	**Controles Existentes**			**Risco Residual**
ID	**Eventos de Risco**	**Detalhamento do risco**	**Causa**	**Observações sobre a causa**				**Descrição**	**Eficácia**		
1											
2											

4.4. TRATAMENTO DE RISCOS

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para definir as diretrizes para respostas consoante quadro a seguir:

Quadro 13 – Diretrizes para resposta perante o nível do risco

Nível de Risco	Descrição	Diretriz para Resposta
Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de avaliação pelo Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI).	Qualquer risco encontrado nessa área deve ter uma resposta imediata. O gestor de risco deverá apresentar plano de ação de tratamento do risco no prazo máximo de 15 dias. O plano de ação deverá ser apreciado pelo Subcomitê, aprovado pelo Secretário-Geral e implementado em até 3 meses. O monitoramento será feito no Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI). Admite-se postergar o tratamento somente mediante parecer do gestor de riscos, apreciação do Subcomitê e aprovação do Secretário-Geral.
Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser objeto de avaliação da Reunião de Acompanhamento Tático (RAT).	Qualquer risco encontrado nessa área deve ter uma resposta em até 15 dias. O gestor de risco deverá apresentar plano de ação de tratamento do risco no prazo máximo de 30 dias. O plano de ação deverá ser apreciado na Reunião de Acompanhamento Tático (RAT), aprovado pelo Secretário-Geral e implementado em até 6 meses. O monitoramento será feito na Reunião de Acompanhamento Tático (RAT). Admite-se postergar o tratamento somente mediante parecer do gestor de riscos e aprovação do Secretário-Geral.
Médio	Nível de risco além do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	O gestor de riscos da unidade deve adotar medidas de tratamento no decorrer de um ano. O monitoramento será feito nas RAOs.
Baixo	Nível de risco dentro do apetite a risco, onde há possíveis oportunidades de maior retorno que podem ser exploradas.	Explorar as oportunidades se determinado pelo gestor de riscos.

As ações de tratamento de riscos são: evitar o risco, não iniciando ou descontinuando a atividade que dá origem ao risco; mitigar o risco, implantando controles que diminuam a probabilidade de ocorrência do risco ou suas consequências; aceitar o risco, assumindo o risco, por escolha consciente e justificada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício; e transferir o risco, compartilhando ou transferindo o risco com outra parte interessada.

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos. A implementação do tratamento pode gerar novos controles ou modificar os controles existentes. A fase inicial do tratamento de riscos é a elaboração do Plano de Tratamento de Riscos, que deve levar em consideração a eficácia das ações já existentes, as restrições organizacionais, técnicas e estruturais, os requisitos legais, a análise custo-benefício e as ações a serem realizadas. Além disso, no Plano de Tratamento de Riscos devem constar os responsáveis, as prioridades e os prazos de execução.

Quadro 14 – Plano de Tratamento de Riscos

Processo de trabalho objeto de Avaliação de Riscos:								**Compilado por:** **Data:**		
Objetivo do processo de trabalho:								**Analisado por:** **Data:**		
Riscos Prioritários				**Categoria do Risco**	**Tipo de Tratamento**	**Ações e Medidas de Tratamento**	**Relação Custo-Benefício**	**Responsável**	**Período de Execução**	**Monitoramento do Risco e seu Tratamento**
ID	**Eventos de Risco**	**Causas**	**Observações sobre a causa**							
1										
2										
3										

4.5. MONITORAMENTO E ANÁLISE CRÍTICA

A fase de monitoramento e análise crítica acontecerá nas reuniões do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional, nas Reuniões de Acompanhamento Tático, nas Reuniões Acompanhamento Operacional e por meio do gestor de riscos, periodicamente ou quando acontecer em resposta a um fato específico.

Entre as finalidades do monitoramento e análise crítica estão a garantia de que os controles sejam eficazes e eficientes, a obtenção de informações adicionais para melhorar a avaliação dos riscos e identificar os riscos residuais que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo.

O Quadro 15 representa o Formulário de Monitoramento e Análise.

Quadro 15 – Formulário de Monitoramento e Análise

Processo de trabalho objeto de Avaliação de Riscos:						**Compilado por:** **Data:**						
Objetivo do processo de trabalho:						**Analisado por:** **Data:**						
Risco				**Categoria do Risco**	**Controles existentes**	**Data**	**Ocorrência do Risco**	**Novos controles**	**Risco Residual**	**Melhoria**		
ID	**Eventos de Risco**	**Causas**	**Observações sobre a causa**							**Requerida**	**Responsável**	**Situação**
1												
2												
3												

4.6. COMUNICAÇÃO E CONSULTA

A comunicação e a consulta devem dar-se em processos contínuos e iterativos, capazes de fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas. Têm como objetivo facilitar a troca de informações, levando em consideração os aspectos de confidencialidade, integridade e confiabilidade.

A comunicação e a consulta às partes interessadas acontecem durante todas as fases do processo de gestão de riscos e são direcionadores para a tomada de decisão. É importante que a comunicação observe os agentes e unidades apontadas como consultados ou informados na Matriz RACI do Quadro 2.

Mudanças identificadas durante o monitoramento devem ser encaminhadas à Secretaria de Gestão Estratégica, a quem compete consolidar os resultados das diversas unidades em relatórios gerenciais e encaminhá-los às instâncias de governança e monitoramento.

A Secretaria de Gestão Estratégica elaborará o Relatório de Monitoramento da Gestão de Riscos do CNMP com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional. Após análise do Subcomitê, o Relatório deverá ser encaminhado ao Comitê de Governança Corporativa e da Estratégia para apreciação.

5. REFERÊNCIAS

ABNT NBR ISO 31000. **Gestão de riscos**: princípios e diretrizes. Rio de Janeiro/RJ, 2009. Disponível em: <https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf>. Acesso em: 10 maio 2016.

BRASIL. Tribunal Superior do Trabalho. **Política de Gestão de Riscos**, Brasília/DF, 2015. Disponível em: <https://goo.gl/inz6kf>. Acesso em: 10 maio 2016.

_____. _____. **Plano de Gestão de Riscos**, Brasília/DF, 2015. Disponível em: <https://goo.gl/mzAJTK>. Acesso em: 1º jun. 2016.

_____. Ministério do Planejamento Desenvolvimento e Gestão. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão**, Brasília/DF, 2017. Disponível em: <http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc/view>. Acesso em: 9 abr. 2018.

_____. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de Gestão de Riscos**, Brasília/DF, 2018. Disponível em: <https://goo.gl/tWgtnA>. Acesso em: 9 abr. 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission.* **Gerenciamento de Riscos Corporativos:** Estrutura Integrada Sumário Executivo. Nova Iorque/EUA, 2007. Disponível em: <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>. Acesso em: 10 maio 2015.