MINISTÉRIO DA TRANSPARÊNCIA E

CONTROLADORIA-GERAL DA UNIÃO

BOLETIM INTERNO - EXTRA

Brasília-DF, 04 de abril de 2018

- Para conhecimento e devida execução, publica-se o seguinte:

ASSUNTOS GERAIS E ADMINISTRATIVOS

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO

1) GABINETE DO MINISTRO

ATO DO MINISTRO-SUBSTITUTO

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO

PORTARIA Nº 910, DE 03 DE ABRIL DE 2018

Aprova a Metodologia de Gestão de Riscos da Controladoria-Geral da União.

O MINISTRO DE ESTADO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO, Substituto, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição Federal, e tendo em vista o disposto no §1º do art. 14 da Portaria nº 915, de 12 de abril de 2017,

RESOLVE:

Art. 1º Aprovar, na forma do Anexo a esta Portaria, a Metodologia de Gestão de Riscos da CGU, que estabelece as etapas do processo de gerenciamento de riscos.

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

Documento assinado eletronicamente por **WAGNER DE CAMPOS ROSARIO**, **Ministro de Estado da Transparência e Controladoria-Geral da União, Substituto**, em 03/04/2018, às 19:20, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cgu.gov.br/conferir informando o código verificador 0675050 e o código CRC E35EC337

METODOLOGIA DE GESTÃO DE RISCOS

Ministério da Transparência e Controladoria-Geral da União - CGU

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO

SAS, Quadra 01, Bloco A, Edifício Darcy Ribeiro
70070-905 – Brasília-DF
cgu@cgu.gov.br

Wagner de Campos Rosário
Ministro Substituto da Transparência e Controladoria-Geral da União

José Marcelo Castro de Carvalho
Secretário-Executivo Substituto

Antônio Carlos Bezerra Leonel
Secretário Federal de Controle Interno

Gilberto Waller Junior
Ouvidor-Geral da União

Antônio Carlos Vasconcellos Nóbrega
Corregedor-Geral da União

Cláudia Taya
Secretária de Transparência e Prevenção da Corrupção

Walter Luis Araújo da Cunha
Diretor de Planejamento e Desenvolvimento Institucional

Priscila Escórcio de França
Coordenadora-Geral de Desenvolvimento Institucional

Equipe Técnica

Fabiano Gusmão Mello
Janice de Almeida Menezes dos Santos
Liliane de Paiva Nascimento

Brasília, abril de 2018.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS 5

1. INTRODUÇÃO 6

2. FUNDAMENTOS DA GESTÃO DE RISCOS DA CGU 7

2.1. PARÂMETROS LEGAIS E FRAMEWORKS 7

2.2. CONCEITOS 8

3. ESTRUTURA DE GESTÃO DE RISCOS DA CGU 10

3.1. COMPETÊNCIAS 10

3.1.1. Comitê de Gestão Estratégica (Art. 7º da PGR/CGU) 12

3.1.2. Comitê Gerencial (Art. 8º da PGR) 12

3.1.3. Núcleo de Gestão de Riscos (Art. 9º da PGR) 13

3.1.4. Responsáveis pelo gerenciamento de riscos dos processos organizacionais (Art. 10 da PGR) 13

3.1.5. Servidores da CGU (Art. 11 da PGR) 14

3.2. INTEGRAÇÃO NOS PROCESSOS ORGANIZACIONAIS 14

3.3. RECURSOS 14

3.4. COMUNICAÇÃO 14

3.5. CAPACITAÇÃO 15

4. METODOLOGIA DE GESTÃO DE RISCOS 15

4.1. DEFINIÇÃO DO PLANO DE GESTÃO DE RISCOS 17

4.2. SELEÇÃO DO PROCESSO ORGANIZACIONAL 17

4.3. ENTENDIMENTO DO CONTEXTO 18

4.4. IDENTIFICAÇÃO E ANÁLISE DOS RISCOS 19

4.5. AVALIAÇÃO DOS RISCOS 20

4.6. PRIORIZAÇÃO DOS RISCOS 22

4.7. DEFINIÇÃO DE RESPOSTAS AOS RISCOS 24

4.8. VALIDAÇÃO DOS RESULTADOS DAS ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS 25

4.9. IMPLEMENTAÇÃO DO PLANO DE TRATAMENTO 25

4.10. COMUNICAÇÃO E MONITORAMENTO 26

4.11. AVALIAÇÃO ESTRATÉGICA 28

5. REFERÊNCIAS BIBLIOGRÁFICAS 30

APÊNDICE I – MODELO DE PLANILHA DE APOIO AO PROCESSO DE GERENCIAMENTO DE RISCOS 31

APÊNDICE II – MODELO DE PLANO DE TRATAMENTO 32

APÊNDICE III – FORMATO E PROCESSO DE ELABORAÇÃO DOS CRITÉRIOS DE AVALIAÇÃO ESTRATÉGICA 33

LISTA DE ABREVIATURAS E SIGLAS

SIGLA	DESCRIÇÃO
ABNT	Associação Brasileira de Normas Técnicas
CGU	Ministério da Transparência e Controladoria-Geral da União
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ISO	International Organization for Standardization
NBR	Norma Brasileira
PGR	Política de Gestão de Riscos

1. INTRODUÇÃO

Este documento apresenta os fundamentos, a estrutura e a Metodologia de Gestão de Riscos do Ministério da Transparência e Controladoria-Geral da União (CGU) com o objetivo de orientar as unidades a implementá-la em conformidade com a sua Política de Gestão de Riscos (PGR/CGU), instituída por meio da Portaria CGU nº 915, de 12 de abril de 2017.

Segundo a PGR/CGU, a Gestão de Riscos é:

> *Arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente.*

A Gestão de Riscos da CGU objetiva, entre outros, o cumprimento do objetivo estratégico que consta no Planejamento Estratégico da CGU 2016-2019, definido por meio da Portaria nº 50.223, de 04 de dezembro de 2015:

> *Gestão Estratégica – Internalizar a gestão estratégica de forma sistêmica e aprimorar a comunicação interna e os instrumentos de gerenciamento de riscos e de planejamento, monitoramento e avaliação dos resultados.*

A construção deste documento iniciou-se em março de 2017, a partir dos estudos para elaboração da PGR/CGU. Com a publicação da Política, definiu-se uma metodologia que seria testada posteriormente em três processos organizacionais da CGU.

Essa aplicação-piloto da metodologia objetivou avaliar a sua aplicabilidade nos processos organizacionais da CGU. Os resultados dos pilotos permitiram identificar lacunas e oportunidades de melhorias para a 1ª versão da Metodologia de Gestão de Riscos da CGU, apresentada neste documento.

Portanto, este documento apresenta:

- Fundamentos da Gestão de Riscos da CGU. Nesse capítulo, são apresentados os conceitos básicos, os referenciais legais e teóricos, bem como os princípios e objetivos que norteiam a Gestão de Riscos da CGU;
- Estrutura da Gestão de Riscos da CGU, que apresenta as competências das instâncias da CGU, a forma de integração dos processos organizacionais, os recursos necessários e os mecanismos de comunicação para a Gestão de Riscos;
- Metodologia de Gestão de Riscos da CGU, com detalhes das etapas do processo de gerenciamento de riscos.

Demais informações operacionais sobre a Gestão de Riscos da CGU serão apresentadas em manual operacional, a ser publicado pelo Núcleo de Gestão de Riscos e divulgado aos servidores da CGU.

2. FUNDAMENTOS DA GESTÃO DE RISCOS DA CGU

2.1. PARÂMETROS LEGAIS E FRAMEWORKS

Em 1992, a gestão de riscos corporativos ganhou destaque com a publicação do guia Internal Control – Integrated Framework – pelo *Committee of Sponsoring Organizations of the Treadway Commission – COSO –*, pelo qual organizações passaram a ser orientadas quanto ao aprimoramento dos seus sistemas de controle interno. Segundo o COSO, esses sistemas são formados por componentes integrados, que incluem a avaliação de riscos. Com enfoque nesse componente, em 2004, o COSO lançou o Enterprise Risk Management - Integrated Framework – COSO-ERM –, que traz componentes, princípios e conceitos para a gestão de riscos corporativos.

Nessa mesma direção, em 2009, foi lançada a norma ABNT NBR ISO 31000:2009 Gestão de Riscos – Princípios e Diretrizes, com o objetivo de disseminar princípios e diretrizes para gestão de riscos, aplicáveis a organizações de qualquer setor.

No âmbito do Poder Executivo Federal, o marco regulatório que orienta os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança é a Instrução Normativa MP/CGU nº 01, de 10 de maio de 2016, em que são apresentados conceitos, princípios, objetivos e responsabilidades relacionados aos temas.

Com vistas ao cumprimento dessa Instrução Normativa e utilizando como parâmetros os frameworks citados acima, a CGU publicou a sua Política de Gestão de Riscos (PGR/CGU), por meio da Portaria CGU nº 915, de 12 de abril de 2017. A PGR/CGU aborda conceitos básicos, princípios, objetivos, operacionalização e competências no âmbito da Gestão de Riscos da CGU.

De acordo com a PGR/CGU, a Gestão de Riscos consiste na arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente. Trata-se de um sistema institucional de natureza permanente, estruturado e monitorado principalmente pelo Comitê de Gestão Estratégica e pela alta administração e direcionado às atividades de identificar, analisar e avaliar riscos, decidir sobre estratégias de resposta e ações para tratamento desses riscos, além de monitorar e comunicar sobre o processo de gerenciamento desses riscos, com vistas a apoiar a tomada de decisão, em todos os níveis, e ao efetivo alcance dos objetivos da CGU.

Recentemente, foi publicado o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Quanto a esse Decreto, destaca-se o art. 17 que dá atribuições à alta administração do Poder Executivo Federal sobre a gestão de riscos, conforme abaixo:

> *Art. 17 A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização*

no cumprimento da sua missão institucional, observados os seguintes princípios:

I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

II - integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e

IV - utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

Dessa forma, a evolução da Gestão de Riscos da CGU busca o alinhamento com os principais frameworks do mercado e com a legislação afeta ao tema.

2.2. CONCEITOS

Para fins deste documento, consideram-se os seguintes conceitos (extraídos do art. 2º da PGR/CGU):

- Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;
- 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;
- Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;
- Meta: alvo ou propósito com que se define um objetivo a ser alcançado;
- Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização;
- Risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;
- Gestão de riscos: arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente;
- Gerenciamento de risco: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais;
- Controle interno da gestão: processo que engloba o conjunto de regras, procedimentos, dire-

trizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

- 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; e
- Apetite a risco: nível de risco que uma organização está disposta a aceitar.

Os princípios e objetivos da Gestão de Riscos da CGU são apresentados nos quadros 1 e 2, respectivamente:

Quadro 1: Princípios da Gestão de Riscos da CGU

Agregar valor e proteger o ambiente interno da CGU
Ser parte integrante dos processos organizacionais
Subsidiar a tomada de decisões
Abordar explicitamente a incerteza
Ser sistemática, estruturada e oportuna
Ser baseada nas melhores informações disponíveis
Considerar fatores humanos e culturais
Ser transparente e inclusiva
Ser dinâmica, iterativa e capaz de reagir a mudanças
Apoiar a melhoria contínua da CGU
Estar integrada às oportunidades e à inovação

Fonte: art. 3º da PGR/CGU

Quadro 2: Objetivos da Gestão de Riscos da CGU

Aumentar a probabilidade de atingimento dos objetivos da CGU
Fomentar uma gestão proativa
Atentar para a necessidade de se identificar e tratar riscos em toda a CGU
Facilitar a identificação de oportunidades e ameaças
Prezar pelas conformidades legal e normativa dos processos organizacionais
Melhorar a prestação de contas à sociedade
Melhorar a governança
Estabelecer uma base confiável para a tomada de decisão e o planejamento
Melhorar o controle interno da gestão
Alocar e utilizar eficazmente os recursos para a mitigação de riscos
Melhorar a eficácia e a eficiência operacional
Melhorar a prevenção de perdas e a gestão de incidentes
Minimizar perdas
Melhorar a aprendizagem organizacional
Aumentar a capacidade da organização de se adaptar a mudanças

Fonte: art. 4º da PGR/CGU

3. ESTRUTURA DE GESTÃO DE RISCOS DA CGU

Segundo a norma ISO 31000:2009, a estrutura de Gestão de Riscos de uma organização 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.*

A ISO trata dos 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.

Na CGU, o componente Mandato e Comprometimento é demonstrado pelas ações do Comitê de Gestão Estratégica e da alta administração em promover a Gestão de Riscos da CGU; primeiro, pela aprovação da PGR/CGU; segundo, por definir suas competências e responsabilidades na Política (Capítulo V – Das competências). Essas competências também se encontram na seção 3.1 deste capítulo.

Na Concepção da estrutura para gerenciar riscos, além da publicação da sua Política de Gestão de Riscos em abril de 2017, a CGU definiu a responsabilização das suas unidades e agentes (seção 3.1), a forma de integração dos processos organizacionais (seção 3.2), os recursos necessários (seção 3.3) e as formas de comunicação (seção 3.4) no âmbito de sua Gestão de Riscos.

O Monitoramento e a Análise Crítica da estrutura de Gestão de Riscos são constantes, por meio da comparação da Gestão de Riscos da CGU com bases normativas, frameworks, contextos de Governo e da CGU, percepção de servidores, entre outros.

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar na estrutura e na metodologia de Gestão de Riscos da CGU, é prevista uma revisão anual desses componentes (Melhoria Contínua da Estrutura). Porém, mudanças no contexto desse Órgão podem provocar a necessidade de implantação de melhorias de forma antecipada.

3.1. COMPETÊNCIAS

A Gestão de Riscos da CGU é gerida de forma integrada. A PGR/CGU define competências específicas sobre gestão de riscos para a estrutura de governança da CGU (instituída pela Portaria nº 1308, de 22 de maio de 2015), que é composta pelo Comitê de Gestão Estratégica e pelo Comitê Gerencial. A PGR/CGU delega à Diplad – até que sejam designados servidores e estrutura própria – a competência de Núcleo de Gestão de Riscos, define o papel de responsável pelo gerenciamento de riscos do processo organizacional e traz responsabilidades a todos os servidores da CGU.

Para coordenar os papéis dos atores envolvidos na Gestão de Riscos, a IN CGU/MP nº 01/2016 apresenta a estrutura de três linhas de defesa, conforme proposto pelo *The Institute of Internal Auditors* (IIA) da seguinte forma:

- 1ª linha de defesa: controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo Federal;

- 2ª linha de defesa: supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance;
- 3ª linha de defesa: constituída pelas auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa) e da supervisão dos controles internos (segunda linha ou camada de defesa).

Na CGU, a 1ª linha de defesa da Gestão de Riscos é composta pelos servidores e pelos responsáveis pelo gerenciamento de riscos dos processos organizacionais. Na 2ª linha, atuam o Núcleo de Gestão de Riscos e o Comitê Gerencial, formado por representantes das unidades diretamente subordinadas à alta administração, das diretorias do Gabinete do Ministro, das diretorias do Gabinete da Secretaria-Executiva e das Controladorias-Gerais da União nos Estados.

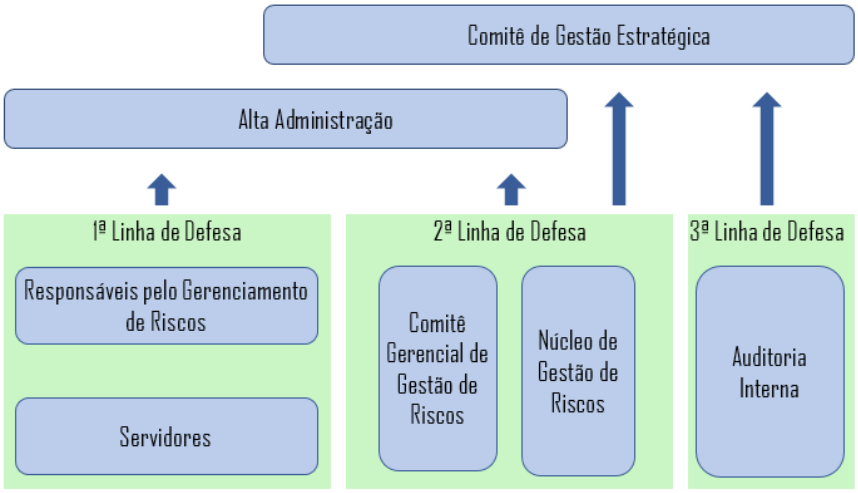
Em relação a 3ª linha de defesa, há a singularidade da CGU de exercer as funções de auditoria interna dos órgãos e entidades do Poder Executivo Federal, o que demanda solução não-convencional para o exercício da função de auditoria interna em sua própria estrutura. Por isso, está em andamento estudo para definição dessa função na CGU e consequente alteração da Lei nº 13.502, de 1º de novembro de 2017. Os cenários apresentados por esse estudo foram apresentados à estrutura de governança da CGU, e o prazo final para decisão é maio de 2018.

A alta administração da CGU, em consonância ao que define o Decreto nº 9203/2017, é formada pelos dirigentes máximos das quatro unidades finalísticas do Órgão – Secretaria Federal de Controle Interno, Secretaria de Transparência e Prevenção da Corrupção, Corregedoria-Geral da União e Ouvidoria-Geral da União –, pelo Secretário-Executivo e pelo Ministro.

O Comitê de Gestão Estratégica é o órgão colegiado de decisão máxima na estrutura de governança da CGU formado pelos membros da alta administração e presidido pelo Ministro da CGU, conforme Portaria nº 1308/2015.

A figura 1 mostra as linhas de defesa na Gestão de Riscos na CGU:

Figura 1: Linhas de defesa na Gestão de Riscos da CGU.



Fonte: Declaração de Posicionamento do IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles (IIA, 2013, adaptado)

A PGR/CGU define as seguintes competências:

3.1.1. COMITÊ DE GESTÃO ESTRATÉGICA (ART. 7º DA PGR/CGU)

- Definir e atualizar as estratégias de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- Definir os níveis de apetite a risco dos processos organizacionais;
- Definir os responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- Definir a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- Aprovar as respostas e as respectivas medidas de controle a serem implementadas nos processos organizacionais;
- Aprovar a Metodologia de Gestão de Riscos e suas revisões;
- Aprovar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- Monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
- Avaliar o desempenho da arquitetura de Gestão de Riscos e fortalecer a aderência dos processos à conformidade normativa;
- Definir indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da CGU;
- Garantir o apoio institucional para promover a Gestão de Riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores;
- Garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade da CGU; e
- Supervisionar a atuação das demais instâncias da Gestão de Riscos.

3.1.2. COMITÊ GERENCIAL (ART. 8º DA PGR)

- Auxiliar o Comitê de Gestão Estratégica na definição e nas atualizações da estratégia de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- Auxiliar na definição dos níveis de apetite a risco dos processos organizacionais;
- Auxiliar na definição dos responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- Auxiliar na definição da periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- Auxiliar na aprovação das respostas e das respectivas medidas de controle a serem implementadas nos processos organizacionais;
- Avaliar a proposta de Metodologia de Gestão de Riscos e suas revisões;

- Avaliar 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;
- Auxiliar na avaliação do desempenho e da conformidade legal e normativa da Gestão de Riscos; e
- Auxiliar na definição dos indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da CGU.

3.1.3. NÚCLEO DE GESTÃO DE RISCOS (ART. 9º DA PGR)

- Propor a Metodologia de Gestão de Riscos e suas revisões;
- 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 a identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;
- Consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê Gerencial e ao Comitê de Gestão Estratégica;
- Oferecer capacitação continuada em Gestão de Riscos para os servidores da CGU;
- Elaborar Plano de Comunicação de Gestão de Riscos;
- Medir o desempenho da Gestão de Riscos objetivando a sua melhoria contínua;
- Construir e propor ao Comitê Gerencial e ao Comitê de Gestão Estratégica os indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da CGU; 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.

3.1.4. RESPONSÁVEIS PELO GERENCIAMENTO DE RISCOS DOS PROCESSOS ORGANIZACIONAIS (ART. 10 DA PGR)

- Identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao que define a PGR;
- Propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade;
- Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;
- Informar o Núcleo de Gestão de Riscos sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;
- Responder às requisições do Núcleo de Gestão de Riscos; e

- Disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade a todos os níveis da CGU e demais partes interessadas.

3.1.5. SERVIDORES DA CGU (ART. 11 DA PGR)

- Monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

3.2. INTEGRAÇÃO NOS PROCESSOS ORGANIZACIONAIS

Dois dos princípios da Gestão de Riscos da CGU são apoiar a melhoria de seus processos organizacionais e subsidiar a tomada de decisão.

Para isso, cada unidade da CGU deve elaborar Plano de Gestão de Riscos (vide seção 4.1), que será integrado ao seu Plano Operacional Anual, com a identificação dos processos organizacionais sob sua responsabilidade que serão objeto da Gestão de Riscos.

Como critério de seleção desses processos, ressalta-se o que define o art. 5º da PGR/CGU, que orienta a priorização de processos organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos no Planejamento Estratégico da CGU.

3.3. RECURSOS

A unidade responsável pelo processo organizacional deve designar equipe para participar das etapas do processo de gerenciamento de riscos. Essa equipe deve ser composta por servidores que conheçam o processo, seus objetivos, contextos, atores envolvidos, resultados e controles já existentes.

Além disso, é importante a participação de servidores com conhecimento acerca da Metodologia de Gestão de Riscos da CGU. Essas pessoas podem ser servidores que participaram da Formação de Multiplicadores em Gestão de Riscos ou que compõem o Núcleo de Gestão de Riscos.

Os recursos operacionais e tecnológicos necessários para apoiar a condução das atividades de Gestão de Riscos da CGU serão definidos em manual operacional, a ser publicado pelo Núcleo de Gestão de Riscos.

3.4. COMUNICAÇÃO

A comunicação sobre os processos de gerenciamento de riscos e seus resultados deve ser conduzida de maneira formal, utilizando o sistema definido pela CGU.

De forma geral, as informações produzidas durante as etapas do processo de gerenciamento de riscos têm caráter restrito. Esse nível de restrição deve ser observado pelos servidores da CGU e demais partes.

Demais comunicações sobre a Gestão de Riscos da CGU serão feitas por meio da elaboração de banners e materiais, publicações na IntraCGU e na página da CGU na internet, por exemplo.

3.5. CAPACITAÇÃO

O Núcleo de Gestão de Riscos, com o apoio de outras unidades de capacitação da CGU, oferecerá, no mínimo, uma capacitação semestral com o objetivo de formar multiplicadores de Gestão de Riscos na CGU.

Outros treinamentos sobre a aplicação da Metodologia de Gestão de Riscos podem ser solicitados pelas unidades. Os treinamentos devem ocorrer, preferencialmente, antes do início do processo de gerenciamento de riscos nos processos organizacionais da CGU.

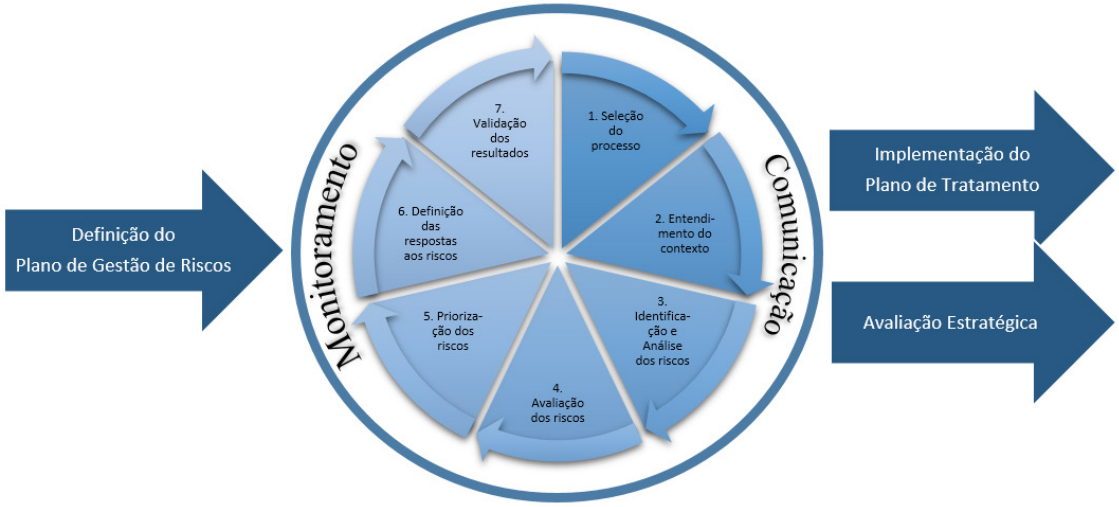
4. METODOLOGIA DE GESTÃO DE RISCOS

A Metodologia de Gestão de Riscos da CGU objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos na CGU, por meio da definição de um processo de gerenciamento de riscos. Segundo o art. 6º da PGR/CGU, são necessárias, no mínimo, as seguintes etapas:

> *I – entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;*
>
> *II – identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;*
>
> *III – análise de riscos: etapa em que são identificadas as possíveis causas e consequências do risco;*
>
> *IV – avaliação de riscos: etapa em que são estimados os níveis dos riscos identificados;*
>
> *V – priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;*
>
> *VI – definição de respostas aos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas; e*
>
> *VII – comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas a sua melhoria.*

A figura 2 apresenta as etapas do processo de gerenciamento de riscos da CGU:

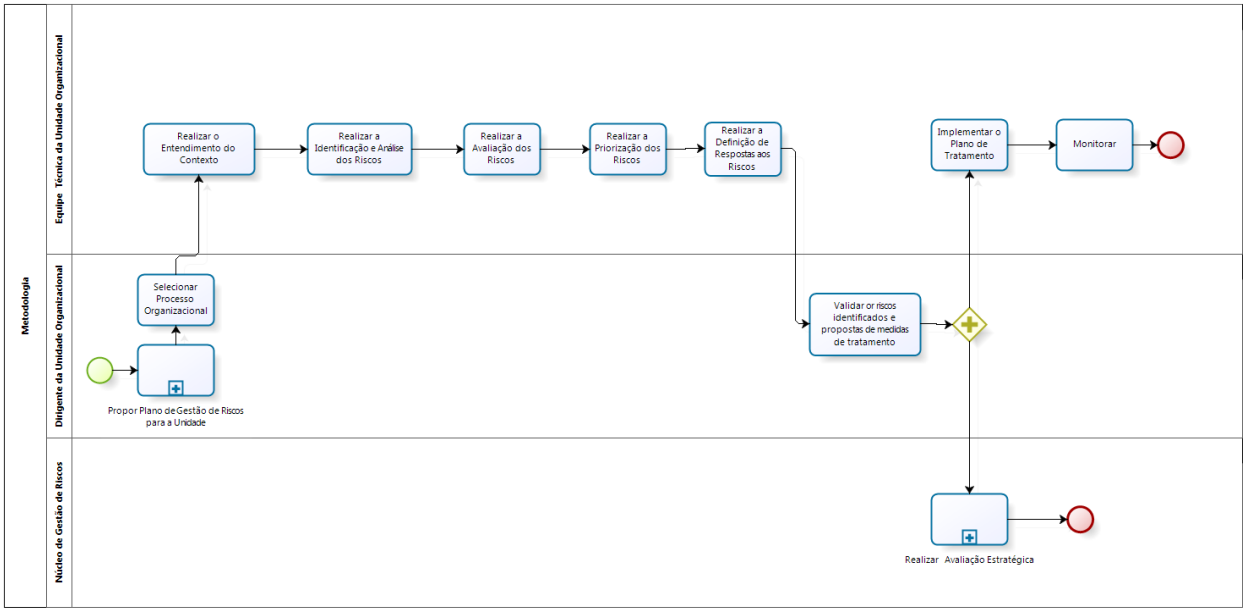
Figura 2: Etapas da Metodologia de Gestão de Riscos da CGU



Fonte: Diretoria de Planejamento e Desenvolvimento Institucional (Diplad)/CGU.

A figura 3 mostra, a partir das competências definidas na PGR/CGU, como os atores se relacionam durante as etapas da Metodologia:

Figura 3: Fluxo do processo de gerenciamento de riscos da CGU



Fonte: Diretoria de Planejamento e Desenvolvimento Institucional (Diplad)/CGU.

A Metodologia de Gestão de Riscos da CGU é orientada a processo organizacional e obedece a um modelo de aplicação descentralizado. Ou seja, as unidades organizacionais podem executar os processos de gerenciamento de riscos em processos sob sua responsabilidade, desde que obedecidas as diretrizes e orientações apresentadas neste documento. Os resultados desses processos devem ser informados ao Núcleo de Gestão de Riscos, que os reportará ao Comitê Gerencial e ao Comitê de Gestão Estratégica da CGU. Além disso, o Núcleo deve selecionar os riscos classificados como "Extremo" para a Avaliação Estratégica (seção 4.11 deste documento).

Se já possuir metodologia própria, a unidade organizacional deve, em até 12 meses, alinhá-la à Metodologia apresentada neste documento, conforme prevê o art. 14 da PGR/CGU:

"Art. 14. As iniciativas relacionadas à Gestão de Riscos existentes na CGU anteriormente à publicação desta Portaria deverão ser gradualmente alinhadas à Metodologia de Gestão de Riscos aprovada pelo Comitê de Gestão Estratégica

(...)

§2º O alinhamento de que trata o caput deste artigo deve ser feito no prazo máximo de 12 (doze) meses após a aprovação da Metodologia de Gestão de Riscos. (grifo nosso)"

4.1. DEFINIÇÃO DO PLANO DE GESTÃO DE RISCOS

Conforme previsto na seção 3.2 deste documento, o dirigente máximo da unidade organizacional deve identificar e priorizar os processos organizacionais que comporão o Plano de Gestão de Riscos da sua unidade, observando o critério estabelecido no art. 5º da PGR/CGU:

O gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas da CGU, sendo priorizados os processos organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos no Planejamento Estratégico da CGU.

Esse Plano de Gestão de Riscos também deve contemplar os Planos de Tratamento nos processos de gerenciamento de riscos e, após aprovação, ser integrado ao Plano Operacional Anual da unidade, conforme diretrizes previstas na Portaria nº 1.243, de 31 de maio de 2017[1]. Segundo essa Portaria, a avaliação do Planejamento da CGU compete à Diretoria de Planejamento e Desenvolvimento Institucional (Diplad), que encaminha os resultados ao Comitê de Gestão Estratégica.

4.2. SELEÇÃO DO PROCESSO ORGANIZACIONAL

Esta etapa objetiva apontar qual processo organizacional previsto no Plano de Gestão de Riscos será objeto do processo de gerenciamento de riscos. Para esse processo, deve-se identificar, pelo menos:

- O responsável pelo gerenciamento de risco (conforme previsto no art. 7º, III, da PGR). Esse servidor deve ter alçada suficiente para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos (art. 10º, parágrafo único, da PGR);
- A equipe técnica que participará do processo de gerenciamento de riscos.

1 A Portaria nº 1.243/2017 estabelece as normas para a avaliação e o monitoramento trimestral da execução das ações do Plano Operacional Anual e do Planejamento Estratégico.

4.3. ENTENDIMENTO DO CONTEXTO

Nesta etapa, o processo organizacional e seus objetivos são analisados à luz de seus ambientes interno e externo.

Nesta etapa, devem ser identificados, pelo menos:

- Descrição resumida do processo. A descrição é um breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- Fluxo (mapa) do processo organizacional;
- Objetivos do processo organizacional. É importante apontar quais objetivos são alcançados pelo processo organizacional. Sendo possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas como estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras. Para identificação dos objetivos, pode-se buscar responder à questão "O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?";
- Relação de Objetivos Estratégicos da CGU alcançados pelo processo;
- Periodicidade máxima do ciclo do processo de gerenciamento de riscos (conforme art. 7º, IV, da PGR/CGU). A unidade deve propor qual o prazo necessário para a um novo gerenciamento de riscos do processo organizacional;

> O ciclo de revisão dos processos de gerenciamento de riscos de processos organizacionais da CGU deve ocorrer entre 1 e 2 anos.

- Unidade demandante do processo de gerenciamento de riscos no processo organizacional (a própria unidade ou o Comitê de Gestão Estratégica, por exemplo);
- Justificativa para o processo de gerenciamento de riscos no processo. Apresentar os motivos que levaram a implementar a gestão de riscos no processo organizacional.
- Unidade responsável pelo processo organizacional;
- Leis e regulamentos relacionados ao processo organizacional;
- Ciclo médio do processo organizacional (em dias);
- Sistemas tecnológicos que apoiam o processo organizacional;
- Partes interessadas no processo, podendo ser internas ou externas;
- Informações sobre o contexto externo do processo, considerando cenário atual ou futuro, oportunidades e ameaças relacionadas, percepções das partes interessadas externas e outros fatos relevantes;
- Informações sobre o contexto interno do processo, considerando políticas, objetivos, diretrizes e estratégias que o impactam, forças e fraquezas relacionadas, percepções das partes interessadas internas, principais ocorrências de problemas e outros fatos relevantes;
- Apetite a risco da unidade para o processo organizacional, caso seja diferente do definido neste documento (seção 4.6 deste documento).

4.4. IDENTIFICAÇÃO E ANÁLISE DOS RISCOS

Considerando o resultado da etapa de Entendimento do Contexto, o fluxo do processo organizacional e a partir da experiência da equipe técnica designada deve-se construir uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas.

Os riscos podem ser identificados a partir de perguntas, como:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

Os eventos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa, e, para tanto, podem ser utilizadas as seguintes questões:

- O evento é um risco que pode comprometer claramente um objetivo do processo?
- O evento é um risco ou uma falha no desenho do processo organizacional?
- À luz dos objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?
- O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo?

Para eventos identificados e analisados como riscos do processo, deve-se indicar:

- Objetivo do processo organizacional/etapa impactado pelo risco;
- Categoria do risco, dentre as definidas para a CGU:
    - Operacional: eventos que podem comprometer as atividades da CGU, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;
    - Legal: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da CGU;
    - Financeiro/orçamentário: eventos que podem comprometer a capacidade da CGU de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;
    - Integridade: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela CGU e a realização de seus objetivos.
- Causas: motivos que podem promover a ocorrência do risco;
- Consequências: resultados do risco que afetam os objetivos;
- Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com

o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos / checklist definidos para o processo e capacitação dos servidores envolvidos no processo;

- Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.

O Apêndice I deste documento traz o modelo de planilha para o registro de informações produzidas nas etapas de Identificação e Análise de Riscos (colunas 1 a 8).

4.5. AVALIAÇÃO DOS RISCOS

Nesta etapa, são calculados os níveis dos riscos identificados pela equipe técnica designada, a partir de critérios de probabilidade e impacto.

> A unidade pode, se preferir, utilizar os critérios de probabilidade e impacto aprovados para Avaliação Estratégica (seção 4.11) nesta etapa de Avaliação.

Os quadros 3 e 4 trazem as escalas de probabilidade e impacto, respectivamente:

Quadro 3: Escala de Probabilidade

Probabilidade	Descrição da probabilidade, desconsiderando os controles	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

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

Quadro 4: Escala de Impacto

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/ divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito Alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

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

A multiplicação entre os valores de probabilidade e impacto 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.

RI = NP x NI

em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

A partir do resultado do cálculo, o risco pode ser classificado dentro das seguintes faixas:

Quadro 5: Classificação do Risco

Classificação	Faixa
Risco Baixo - RB	0 – 9,99
Risco Médio - RM	10 – 39,99
Risco Alto - RA	40 – 79,99
Risco Extremo - RE	80 – 100

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

Revisão do processo em novo ciclo do processo de gerenciamento de riscos

De forma geral, nos ciclos seguintes do processo de gerenciamento de risco do processo organizacional, a unidade deve considerar o nível de risco inerente calculado no 1º ciclo e reavaliar os controles para o cálculo do risco residual. A comparação entre os níveis de riscos residuais de diferentes ciclos objetiva identificar se os controles definidos nos Planos de Tratamento estão sendo eficazes para tratar o risco.

A seguinte matriz representa os possíveis resultados da combinação das escalas de probabilidade e impacto.

Quadro 6: Matriz de Riscos

IMPACTO						
	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

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

Em seguida, a equipe técnica designada deve avaliar a eficácia dos controles internos existentes em relação aos objetivos do processo organizacional. Ou seja, é necessário verificar se os controles apontados durante a etapa de Identificação e Análise do risco têm auxiliado no tratamento adequado desse risco. O quadro 7 mostra os níveis de avaliação da eficácia dos controles existentes:

Quadro 7: Níveis de Avaliação dos Controles Internos Existentes

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

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

O valor final da multiplicação entre o valor do risco inerente e o fator de avaliação dos controles corresponde ao nível de risco residual.

RR = RI x FC

em que:

RR = nível do risco residual

RI = nível do risco inerente

FC = fator de avaliação dos controles existentes

O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente da faixa definida para o risco inerente.

O Apêndice I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Avaliação de Riscos (colunas 9 a 13).

4.6. PRIORIZAÇÃO DOS RISCOS

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para identificar quais riscos serão priorizados para tratamento.

A faixa de classificação do risco residual deve ser considerada para a definição da atitude da unidade em relação à priorização para tratamento. O quadro 8 mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Quadro 8: Atitude perante o risco para cada classificação

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	Nível de risco dentro 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.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de Avaliação Estratégica (seção 4.11), comunicado ao Comitê de Gestão Estratégica e ao dirigente máximo da unidade e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Gestão Estratégica.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo Comitê de Gestão Estratégica.

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

Sobre o Apetite a Risco do Processo Organizacional

A unidade organizacional pode definir, em conformidade com o contexto do processo organizacional em avaliação, faixas de classificação distintas das apontadas neste documento para refletir o nível de apetite a risco desse processo. Segundo a PGR/CGU, apetite a risco é o "nível de risco que a unidade está disposta a aceitar". Além disso, esse apetite deve ser aprovado pelo Comitê de Gestão Estratégica (art. 8º, II, PGR/CGU).

É importante que o apetite a risco do processo organizacional seja estabelecido no início do processo de gerenciamento de riscos. Uma vez definido, a unidade declara que:

- todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;

- todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

Sobre o Risco Extremo

Além dos riscos classificados como "Extremo", riscos com as outras classificações (baixo, médio ou alto) podem ser objeto da Avaliação Estratégica (seção 4.11), desde que indicados pelo dirigente máximo da unidade.

O Apêndice I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Priorização de Riscos (colunas 14 a 16).

4.7. DEFINIÇÃO DE RESPOSTAS AOS RISCOS

Esta etapa objetiva definir as opções e as medidas de tratamento (controles) para os riscos priorizados na etapa anterior.

Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco, contexto da CGU ou custo do controle, conforme apresenta o quadro 9.

Quadro 9: Opções de tratamento do risco

Opção de Tratamento	Descrição
Mitigar	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Na CGU, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. Na CGU, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a CGU. Na CGU, evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Gestão Estratégica.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: Diretoria de Planejamento e Desenvolvimento Institucional (Diplad)/CGU

Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco "Baixo" ou "Médio").

O Plano de Tratamento gerado pelo processo de gerenciamento de riscos do processo organizacional é um plano de ação para a implementação das medidas de tratamento dos riscos desse processo organizacional. Por isso, deve conter, pelo menos:

- Iniciativa, com a proposta de projeto ou ação que implementará um conjunto de medidas de tratamento;
- Medida(s) de tratamento contemplada(s) na iniciativa e o risco relacionado que deseja tratar;
- Objetivos/benefícios esperados por medida de tratamento;
- Unidade organizacional responsável pela implementação da iniciativa;
- Unidades organizacionais corresponsáveis pela implementação da iniciativa, ou seja, unidades envolvidas na implementação da medida de tratamento;
- Servidor ou cargo responsável pela implementação;
- Breve descrição sobre a implementação;
- Custo estimado para a implementação;
- Data prevista para início da implementação;

- Data prevista para o término da implementação;
- Situação da iniciativa.

É importante que, em uma primeira abordagem da elaboração do Plano de Tratamento, avalie-se a necessidade de melhorar ou extinguir controles já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

Se as iniciativas definidas no Plano de Tratamento envolverem mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de Plano para que essas unidades validem as iniciativas de que participarem.

O Apêndice II deste documento traz um modelo de Plano de Tratamento.

4.8. VALIDAÇÃO DOS RESULTADOS DAS ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS

Os resultados das etapas anteriores do processo de gerenciamento de riscos (entendimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos e definição de respostas aos riscos) devem ser avaliados e aprovados pelo dirigente máximo da unidade organizacional.

Após a aprovação desses resultados, o responsável pelo processo de gerenciamento de riscos ou o dirigente da unidade deve:

- Encaminhar esses resultados ao Núcleo de Gestão de Riscos;
- Incluir as iniciativas previstas no Plano de Tratamento no Plano de Gestão de Riscos da sua unidade;
- Encaminhar o Plano de Tratamento aprovado às unidades corresponsáveis pelas iniciativas para que essas também incluam as ações em seu Plano Operacional corrente.

4.9. IMPLEMENTAÇÃO DO PLANO DE TRATAMENTO

A implementação do Plano de Tratamento envolve a participação da unidade organizacional responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas.

A responsabilidade primária pelo Plano de Tratamento permanece com a unidade organizacional responsável pelo processo organizacional. No Plano de Tratamento, deve ser definido o principal responsável pela implementação da iniciativa (servidor ou cargo), que também deverá monitorar e reportar a evolução das iniciativas.

4.10. COMUNICAÇÃO E MONITORAMENTO

Segundo a ISO 31000:2009, durante todas as etapas do processo de gerenciamento de riscos, é importante comunicar as partes interessadas.

A PGR/CGU prevê em seu art. 12:

> *O Comitê de Gestão Estratégica, o Comitê Gerencial, o Núcleo de Gestão de Riscos e os responsáveis pelo gerenciamento de riscos dos processos organizacionais deverão manter fluxo regular e constante de informações entre si.*

Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI apresentada no quadro 10.

A Matriz de Responsabilidade RACI define Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de riscos na CGU. Segundo SOUZA e BRASIL (2017), são elementos da Matriz RACI:

- Responsável: quem executa a atividade;
- Autoridade: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;
- Consultado: quem pode agregar valor ou é essencial para a implementação;
- Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Durante as etapas do processo de gerenciamento de riscos da CGU, é importante que a comunicação observe os agentes ou unidades apontadas como consultados ou informados na Matriz RACI do quadro 10.

Quadro 10: Matriz RACI para o processo de gerenciamento de riscos na CGU

	Comitê de Gestão Estratégica	Comitê Gerencial	Núcleo de Gestão de Riscos	Dirigente da Unidade	Responsável pelo gerenciamento de riscos	Equipe Técnica Designada	Responsável pela implementação	Servidores da CGU
Definir Plano de Gestão de Riscos da Unidade	A	C	I	R	C	I	I	I
Selecionar Processo Organizacional	A	I	C	R	C	I		
Realizar o Entendimento do Contexto	I	I	C	A	R	R		
Realizar a Identificação e Análise dos Riscos	I	I	C	A	R	R		
Realizar a Avaliação dos Riscos	I	I	C	A	R	R		
Realizar a Priorização dos Riscos	I	I	C	A	R	R		

Realizar a Definição de Respostas aos Riscos	I	I	C	A	R	R		
Validar os Riscos Levantados	I	I	C	R	C	C		
Implementar o Plano de Tratamento	I	I	C	A	I	C	R	
Monitorar	I/R	I	C	A	R	I	C	R
Realizar Avaliação Estratégica	A	C	R	C	C	R		

Fonte: Diretoria de Planejamento e Desenvolvimento Institucional (Diplad)/CGU.

O monitoramento, no âmbito do processo de gerenciamento de riscos, deve ser realizado principalmente pela unidade responsável pelo processo organizacional, de forma a:

- Garantir que os controles sejam eficazes e eficientes;
- Analisar as ocorrências dos riscos;
- Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;
- Identificar os riscos emergentes.

Porém, a PGR/CGU, em seu art. 11, também delega a todos os servidores da CGU a responsabilidade de monitorar os níveis dos riscos e suas medidas de tratamento:

> *Art. 11. Compete a todos os servidores da CGU o monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento. Parágrafo único. No monitoramento de que trata o caput deste artigo, caso sejam identificadas mudanças ou fragilidades nos processos organizacionais, o servidor deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos do processo em questão.*

Mudanças identificadas durante o monitoramento devem ser encaminhadas ao Núcleo de Gestão de Riscos, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais da CGU.

Trimestralmente, o Núcleo de Gestão de Riscos produzirá um boletim com o resultado do acompanhamento das ações relacionadas ao Plano de Gestão de Riscos de cada unidade, que será enviado ao Comitê Gerencial e ao Comitê de Gestão Estratégica.

Além disso, o Núcleo elaborará o Relatório de Monitoramento da Gestão de Riscos da CGU com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao Comitê Gerencial e ao Comitê de Gestão Estratégica.

4.11. AVALIAÇÃO ESTRATÉGICA

Riscos residuais classificados como "Extremo" na etapa de Avaliação de Riscos (seção 4.6 deste documento) serão avaliados novamente pelo Núcleo e pela equipe técnica designada por meio de critérios de mensuração específicos para as dimensões de probabilidade e impacto. O Apêndice III apresenta o processo de elaboração e o formato desses critérios, denominados critérios de Avaliação Estratégica.

A definição desses critérios observa o previsto no parágrafo único do art. 6º da PGR/CGU:

> *A Metodologia de Gestão de Riscos deverá contemplar critérios predefinidos de avaliação, de forma a permitir a comparabilidade entre os riscos.*

Essa comparabilidade auxilia a decisão, pelo Comitê de Gestão Estratégica da CGU, para a priorização para tratamento de riscos de diferentes processos.

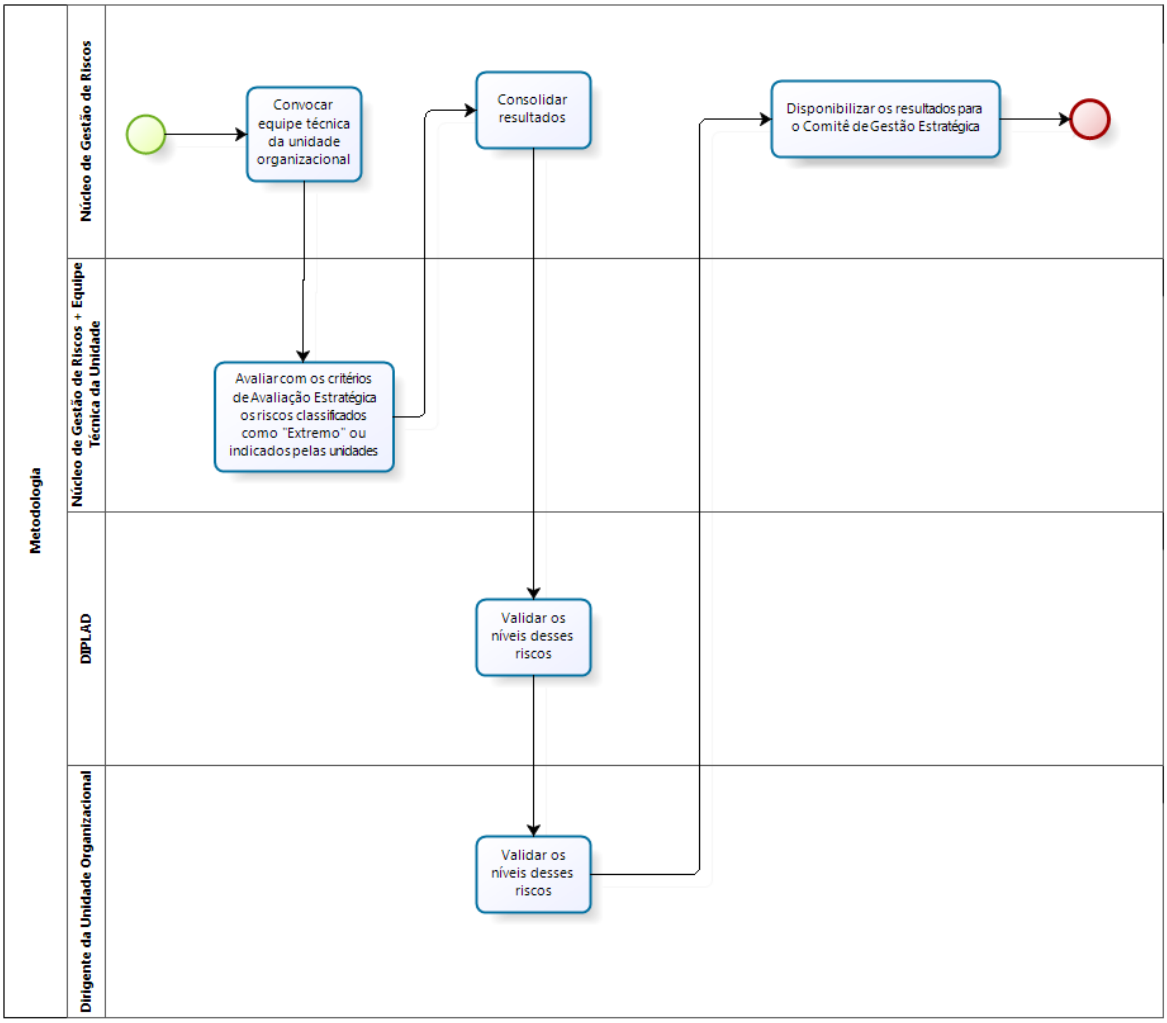
Durante a Avaliação Estratégica, a equipe técnica designada pela unidade responsável pelo processo organizacional e o Núcleo de Gestão de Riscos devem discutir e determinar os níveis dos riscos selecionados dentro de cada critério que compõe a probabilidade e o impacto. O resultado será, então, a média ponderada dos valores desses níveis, considerando os pesos desses critérios[2]. Esse resultado será apresentado ao Comitê de Gestão Estratégica por meio do dashboard específico de Gestão de Riscos.

Os critérios de probabilidade e impacto da Avaliação Estratégica e seus respectivos pesos comporão documento específico.

A figura 4 apresenta as etapas da Avaliação Estratégica:

2 Os pesos de cada critério são definidos após a rodada da AHP – *Analitic Hyerarchy Process* –, conforme exposto no Apêndice III deste documento.

Figura 4: Etapas da Avaliação Estratégica



Fonte: Diretoria de Planejamento e Desenvolvimento Institucional (Diplad)/CGU.

Os resultados da Avaliação Estratégica subsidiarão a priorização quanto à alocação de recursos para o atingimento de objetivos institucionais, que poderá refletir na revisão dos Planos de Tratamento dos riscos propostos pelas unidades.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. **Gestão de Riscos – Princípio e diretrizes.** NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2009.

AHP. ***Analytic Hierarchy Process***, Excel MS Excel 2010 (extensão xlsx). O modelo AHP foi desenvolvido por Goepel, Klaus D., modelo BPMSG AHP Excel, cuja versão é de livre uso. Disponível em http://bpmsg.com

BRASIL. **Instrução Normativa Conjunta MP/CGU Nº 01**, de 10 de maio de 2016, que estabelece a adoção de uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Assessoria Especial de Controles Internos. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília. Brasília. V1.1.2 – 2017.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Gestão de Riscos e Controles Internos no Setor Público**. 55p. Abril de 2017.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 915**, de 12 de abril de 2017, que institui a Política de Gestão de Riscos – PGR – do Ministério da Transparência, Fiscalização e Controladoria-Geral da União – CGU.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 50.223**, de 04 de dezembro de 2015, que aprova o Planejamento Estratégico da CGU para o quadriênio 2016-2019.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos**. Disponível em http://portal.tcu.gov.br/gestao-e-governanca/gestao-de-riscos/. Acesso em Abril de 2017.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade**. Brasília. 164 p., 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e *Pricewaterhouse Coopers Governance, Risk and Compliance*, Estados Unidos da América, 2007.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. **Risk Assessment in Practice**. Disponível em https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf. Acesso em 27 de abril de 2017.

IIA. *The Institute of Internal Auditors*. **As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.** Disponível em http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf. Acesso em 18 de novembro de 2016.

SOUZA, Kleberson; BRASIL, Franklin. **Como gerenciar riscos na administração pública – Estudo prático em licitações**. Editora Negócios Públicos. Curitiba. 149 p. 2017.

APÊNDICE I – MODELO DE PLANILHA DE APOIO AO PROCESSO DE GERENCIAMENTO DE RISCOS

Identificação e Análise do Risco								Avaliação dos Riscos					Priorização dos Riscos				Respostas aos Riscos	
					Controles													
Processo/Etapa (1)	Objetivo (2)	Evento de Risco (3)	Categoria (4)	Causa (5)	Consequência (6)	Preventivo (7)	Atenuação e recuperação (8)	Probabilidade (9)	Impacto (10)	Risco Inerente (11)	Avaliação dos Controles (12)	Risco Residual (13)	Classificação (14)	Priorizado (15)	Justificativa (16)	Tipo de Tratamento (17)	Medidas de Tratamento (18)	

APÊNDICE II – MODELO DE PLANO DE TRATAMENTO

Iniciativa	Evento de Risco/Medida de tratamento	Unidade Responsável	Unidades Correspondentes	Responsável pela Implementação	Como será Implementado	Custo Previsto	Data Prevista Início da Implementação	Data Prevista para o Término da Implementação	Situação

APÊNDICE III – FORMATO E PROCESSO DE ELABORAÇÃO DOS CRITÉRIOS DE AVALIAÇÃO ESTRATÉGICA

A etapa de Avaliação Estratégica utiliza critérios de avaliação específicos para as dimensões de probabilidade e impacto para os riscos residuais classificados como "Extremo" ou indicados pelos dirigentes máximos das unidades da CGU. Esses critérios devem ser estáveis o suficiente para que seja possível a comparabilidade entre riscos de diferentes processos organizacionais da CGU que utilizaram a metodologia proposta neste documento.

O quadro 11 apresenta o modelo utilizado para os critérios de Avaliação Estratégica da CGU. Cada critério possui alternativas, com valores entre 0% e 100%. Além disso, é estabelecido um peso para cada critério, resultado da aplicação do método de Análise Hierárquica de Processos – AHP [3]– entre membros do Comitê Gerencial, aprovado pelo Comitê de Gestão Estratégica da CGU.

Quadro 11: Critérios de Avaliação Estratégica

Probabilidade			Impacto		
Critério 1 (Peso P.A)	Critério 2 (Peso P.B)	Critério 3 (Peso P.C)	Critério 4 (Peso I.A)	Critério 5 (Peso I.B)	Critério 6 (Peso I.C)
Alternativa 1.1	Alternativa 2.1	Alternativa 3.1	Alternativa 4.1	Alternativa 5.1	Alternativa 6.1
Alternativa 1.2	Alternativa 2.2	Alternativa 3.2	Alternativa 4.2	Alternativa 5.2	Alternativa 6.2
Alternativa 1.3	Alternativa 2.3	Alternativa 3.3	Alternativa 4.3	Alternativa 5.3	Alternativa 6.3
Alternativa 1.4	Alternativa 2.4	Alternativa 3.4	Alternativa 4.4	Alternativa 5.4	Alternativa 6.4
Alternativa 1.5	Alternativa 2.5	Alternativa 3.5	Alternativa 4.5	Alternativa 5.5	Alternativa 6.5
Alternativa 1.6	Alternativa 2.6	Alternativa 3.6	Alternativa 4.6	Alternativa 5.6	Alternativa 6.6

Fonte: Diretoria de Planejamento e Desenvolvimento Institucional (Diplad)/CGU.

A definição dos critérios de Avaliação Estratégica da CGU considera as seguintes etapas:

a) Proposição dos critérios

O Núcleo de Gestão de Riscos recebe propostas para inclusão, atualização ou exclusão dos critérios, as avalia e se manifesta sobre essas propostas.

b) Encaminhamento dos critérios para validação do Comitê Gerencial

O Núcleo de Gestão de Riscos encaminha ao Comitê Gerencial a proposta com:

- As propostas de critérios;
- A manifestação do Núcleo de Gestão de Riscos sobre a proposta.

A avaliação de cada membro do Comitê Gerencial deve ser aprovada pelo dirigente máximo da respectiva unidade organizacional antes do retorno ao Núcleo de Gestão de Riscos.

3 *Analytic Hierarchy Process* ou Análise Hierárquica de Processos (AHP). A AHP foi desenvolvida por Tomas L. Saaty no início da década de 70 e é um método amplamente utilizado e conhecido no apoio à tomada de decisão, para a resolução de conflitos negociados em problemas com múltiplos critérios (SAATY, T. Método de análise hierárquica. São Paulo: McGraw-Hill, 1991). Na CGU, as rodadas para o cálculo da AHP têm o apoio de uma planilha (disponível em http://bpmsg.com), que é distribuída para todos que participarão da definição dos pesos dos critérios.

c) Definição dos pesos para os critérios

O Núcleo de Gestão de Riscos organiza a planilha da AHP com a nova lista de critérios. Cada membro do Comitê Gerencial deve preencher essa planilha com sua proposta de pesos, e sua avaliação deve ser aprovada pelo dirigente máximo da respectiva unidade organizacional antes do retorno ao Núcleo de Gestão de Riscos.

d) Consolidação dos pesos

O Núcleo de Gestão de Riscos consolida os pesos propostos para os critérios e encaminha os valores finais para aprovação do Comitê de Gestão Estratégica.

e) Reavaliação dos níveis dos riscos dos processos

Para manter a comparabilidade dos riscos de todos os processos organizacionais, os riscos que já foram avaliados devem ser reavaliados, considerando o novo rol de critérios de Avaliação Estratégica e seus novos pesos.

MINISTÉRIO DA TRANSPARÊNCIA E

CONTROLADORIA-GERAL DA UNIÃO

BOLETIM INTERNO - EXTRA

ELISA MIDORI OKAMURA
Chefe de Serviço/SECAD/COGEP/DGI

De acordo. Autorizo a publicação.
Em 04 de abril de 2018

SIMEI SUSÃ SPADA
Coordenadora-Geral de Gestão de Pessoas