CGU
Controladoria-Geral da União

METODOLOGIA DE GESTÃO DE RISCOS

Sumário

Lista de Abreviaturas e Siglas

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
CGI	Comitê de Governança Interna
CGRI	Comitê Gerencial de Riscos e Integridade
CGU	Controladoria-Geral da União
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CRG	Corregedoria-Geral da União
DGI	Diretoria de Gestão Interna
DIGOV	Diretoria de Governança
DTI	Diretoria de Tecnologia da Informação
ISO	*International Organization for Standardization*
NBR	Norma Brasileira
NGRI	Núcleo de Gestão de Riscos e Integridade
OGU	Ouvidoria-Geral da União
PGR	Política de Gestão de Riscos
SCC	Secretaria de Combate à Corrupção
SFC	Secretaria Federal de Controle
STPC	Secretaria de Transparência e Combate à Corrupção

1 Introdução

Este documento apresenta os fundamentos, a estrutura e a Metodologia de Gestão de Riscos da 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 2020-2023, definido por meio da Portaria nº 182, de 22 de janeiro de 2020:

> *Gestão Estratégica – Modernizar a gestão estratégica por meio do fomento às melhores práticas de governança, segurança e comunicação organizacional.*

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, validada por meio da realização de oficinas-piloto de gerenciamento de riscos.

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 melhoria para a 1ª versão da Metodologia de Gestão de Riscos da CGU.

Nessa segunda versão da Metodologia foram necessários os seguintes ajustes:

1. Para que o processo de gerenciamento de riscos seja aplicado em diferentes níveis da organização de forma estratégica, integrada, sistematizada, e aproveitando-se da oportunidade do lançamento da metodologia de gestão de processos da CGU, a Gestão de Riscos se integrará à Gestão de Processos, otimizando os esforços operacionais e possibilitando um entendimento mais completo dos processos da CGU ao analisar também seus principais riscos, orientando ao final num Plano de Ação mais completo, que além de otimizar o processo, trata de forma integrada seus principais riscos.

2. Devido à alteração da estrutura regimental da CGU (Decreto nº 9.681/2019) e da estrutura de governança da CGU (Portaria CGU nº 665/2019), foi necessária a revisão das competências complementares do Comitê de Governança Interna, do Comitê Gerencial de Riscos e Integridade (CGRI), do Núcleo de Gestão de Riscos e

Integridade (NGRI) e das Unidades Organizacionais, por meio da publicação das Portarias CGU nº 1.163 e 1.164, ambas publicadas em 21 de março de 2019.

3. Durante as oficinas realizadas, o NGRI pôde analisar as dificuldades que os servidores tiveram na utilização da 1ª versão da metodologia, além de analisar as sugestões dadas por esses servidores. Nesse sentido diversas modificações de melhorias estão presentes nessa 2 ª versão:
    a. Alteração do nome de algumas etapas da metodologia com a finalidade de evitar conflitos com as normas ISO 31.000 e COSO ERM;
    b. Diminuição na quantidade e melhoria na clareza dos critérios para o cálculo do nível de risco organizacional;
    c. Avaliação do custo e eficiência dos controles presentes no processo e verificação quanto a efetividade deles na mitigação de riscos; e
    d. Simplificação no cálculo do risco residual.
    e. Dar publicidade internamente aos critérios utilizados no cálculo do nível de risco organizacional.
    f. Inserção de informações necessárias para o cálculo da probabilidade em dias.

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 são apresentadas no Manual Operacional de Gestão de Riscos da CGU, publicado na página da Intracgu.

2 Fundamentos da Gestão de Riscos da CGU

2.1 Parâmetros legais e frameworks

A base teórico-conceitual da Metodologia de Gestão de Riscos da CGU está pautada basicamente em *frameworks* internacionais e em normativos e referências nacionais de gestão de riscos e controles internos, dos quais destacam-se:

- COSO Report. Internal Control: Integrated Framework. 1992;
- COSO - ERM - Enterprise Risk Management, 2004;
- ABNT NBR ISO 31.000: 2009, Gestão de Riscos - Princípios e Diretrizes;
- ABNT NBR ISO 31010:2009, Gestão de Riscos - Técnicas para o processo de avaliação de riscos;
- ABNT NBR ISO 31.000: 2018, Gestão de Riscos - Princípios e Diretrizes;
- Instrução Normativa Conjunta CGU/MP nº 01, de 10/5/2016;
- Declaração de Posicionamento do IIA - Instituto dos Auditores Internos: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.

Com o objetivo de se destacar a importância da gestão de riscos no processo de definição da estratégia da organização e na condução de seus resultados, o COSO 2004 foi atualizado em 2017, sendo reintitulado Enterprise risk management – integrating with strategy and performance (Gerenciamento de riscos corporativos - integrando-se à estratégia e ao desempenho).

Nessa mesma direção, em 2017, foi atualizada 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 Governança Interna e pela alta administração, 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.

Tem-se também 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, diretrizes, 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 31000:2018, o propósito da estrutura de Gestão de Riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da Alta Direção

A ISO trata dos componentes Liderança e comprometimento, Concepção, Implementação, Avaliação, Melhoria e Integração.

Na CGU, o componente Liderança e comprometimento é demonstrado pelas ações do Comitê de Governança Interna 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.

A Implementação e Avaliação 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 da Implementação e Avaliação podem impactar na estrutura e na metodologia de Gestão de Riscos da CGU, é prevista uma revisão anual desses componentes (Melhoria). 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 Governança Interna e pelo Comitê Gerencial. A PGR/CGU delega ao Núcleo de Gestão de Riscos, 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.

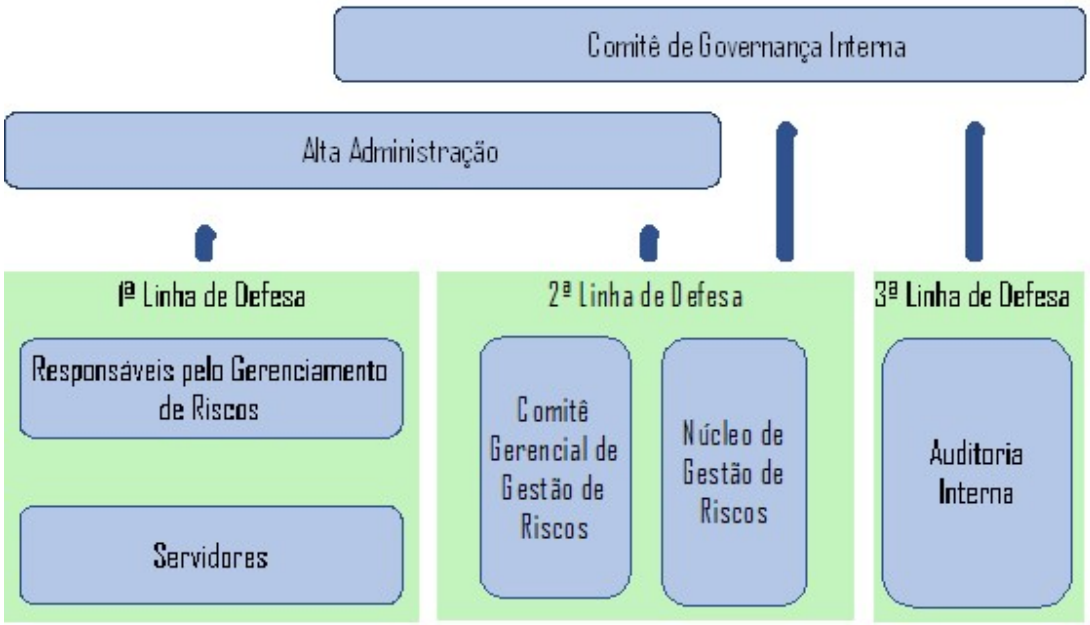
Em relação a 3ª linha de defesa, há a singularidade da CGU de exercer as funções de auditoria interna dos órgãos e entidades do Poder Executivo Federal, o que demanda solução não-convencional para o exercício da função de auditoria interna em sua própria estrutura. A Medida Provisória nº 870/2019 atribuiu, à Secretaria de Controle Interno da Secretaria-Geral da Presidência da República, a competência de atuar como órgão de controle Interno da CGU.

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 Governança Interna 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 665/2019.

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 Portaria nº 1.163 de 20 de março de 2019 atualizou a estrutura de governança relativa à Gestão de Riscos e ao Programa de Integridade da CGU, conforme as seguintes competências:

3.1.1. Comitê de Governança Interna (Art. 2º da Portaria nº 1.163 de 20 de março de 2019)

- Estabelecer diretrizes, objetivos, iniciativas, indicadores relativos à Gestão de Riscos e ao Programa de Integridade;
- Realizar o monitoramento e a avaliação da Gestão de Riscos e do Programa de Integridade;
- Aprovar a Política e a Metodologia de Gestão de Riscos e suas revisões;
- Aprovar anualmente o Plano de Integridade da CGU;
- Monitorar a evolução dos níveis de riscos e o desempenho das respectivas medidas de controle implementadas;
- Definir os níveis de apetite a risco dos processos organizacionais;
- Aprovar, no que couber, as medidas de tratamento a serem implementadas nos processos organizacionais;
- Aprovar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;

- Garantir o apoio institucional para promover a Gestão de Riscos e o Programa de Integridade, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores; e
- Supervisionar a atuação das demais instâncias da Gestão de Riscos e do Programa de Integridade.

3.1.2. Comitê Gerencial de Riscos e Integridade (Art. 4º da Portaria nº 1.163 de 20 de março de 2019)

- Auxiliar o CGI na execução de suas competências;
- Avaliar a proposta da Política e da Metodologia de Gestão de Riscos e suas revisões;
- Monitorar a evolução dos níveis de riscos e o desempenho das respectivas medidas de tratamento implementadas;
- Auxiliar o CGI na definição dos níveis de apetite a risco dos processos organizacionais;
- Avaliar, no que couber, as medidas de tratamento a serem implementadas nos processos organizacionais;
- Avaliar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos; e
- Exercer outras atividades definidas pelo CGI.

3.1.3. Núcleo de Gestão de Riscos (Art. 6º da PGR da Portaria nº 1.163 de 20 de março de 2019)

- Realizar as funções de secretaria-executiva do CGI nas ações estratégicas relacionadas à Gestão de Riscos e ao Programa de Integridade;
- Exercer a presidência do CGRI;
- Propor a definição e revisão das diretrizes, objetivos, iniciativas e indicadores relativos à Gestão de Riscos e ao Programa de Integridade;
- Coordenar as ações relacionadas à Gestão de Riscos e ao Programa de Integridade;
- Elaborar relatórios gerenciais de monitoramento e avaliação para subsidiar a atuação do CGI e do CGRI;
- Propor a Política e a Metodologia de Gestão de Riscos e suas revisões;
- Elaborar anualmente o Plano de Integridade da CGU;
- Monitorar a evolução dos níveis de riscos e o desempenho das respectivas medidas de tratamento implementadas;
- Dar suporte à identificação, análise e avaliação dos riscos e à proposição das medidas de tratamento a serem implementadas;
- Definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;

- Realizar, com o apoio da DTI, a gestão do Painel de Monitoramento de Riscos da CGU;
- Promover a comunicação, a articulação e a cooperação técnica entre as unidades da CGU para o adequado desempenho da Gestão de Riscos e do Programa de Integridade;
- Promover ações de orientação e treinamento internos em temas relativos à Gestão de Riscos e ao Programa de Integridade;
- Promover ações de divulgação relacionadas à Gestão de Riscos e ao Programa de Integridade; e
- Observar as orientações estabelecidas pela STPC quanto aos procedimentos de estruturação, execução e monitoramento do Programa de Integridade.

3.1.4. Demais Unidades Organizacionais (Art. 7º da PGR da Portaria nº 1.163 de 20 de março de 2019)

- Elaborar anualmente o Plano de Gestão de Riscos, em conformidade com as diretrizes estabelecidas pelo CGI e orientações do NGRI;
- Propor ações a serem incluídas no Plano de Integridade da CGU para assegurar a existência de condições mínimas para o exercício da boa governança;
- Implementar as ações previstas no Plano de Integridade da CGU;
- Fornecer ao NGRI documentos e informações necessárias à execução de suas atividades;
- Monitorar a evolução dos níveis de riscos e o desempenho das respectivas medidas de tratamento implementadas; e
- Aprovar a periodicidade máxima do ciclo do processo de gerenciamento de riscos para os processos organizacionais sob sua responsabilidade.

3.2 Integração aos processos organizacionais

De forma a possibilitar a integração da Gestão de Riscos à Gestão de Processos, primeiro foi necessário compreender de forma detalhada tanto o processo de Gerenciamento de Processos como o processo de Gerenciamento de Riscos.

Por esse motivo ambos processos foram pilotos da metodologia de Gestão de Processos da CGU. Primeiro gerenciou-se o processo de gerenciamento de processos, posteriormente o de gerenciamento de riscos.

De forma geral esse trabalho trouxe melhorias substanciais para ambos processos, cabendo destacar as seguintes:

- Manualização dos processos
- Melhor entendimento das etapas e dos fluxos dos processos
- Melhor entendimento do papel dos atores nos processos

- Otimização das etapas dos processos
- Dimensionamento do custo operacional (HH) e temporal dos processos.
- Automação de partes dos processos

Além dessas melhorias verificou-se que ambos processos apresentavam diversas similaridades, afinal trata-se de processos transversais que atuam em outros processos organizacionais e apresentam o mesmo produto final (Plano de Ação), com focos distintos (melhoria do processo e tratamento de riscos). Além de monitorarem a execução do plano de ação e prestarem conta para as instâncias de governança.

Dessa forma, optou-se por integrar ambos os processos, buscando uma otimização do custo operacional e uma redução no impacto para as áreas executoras dos processos organizacionais.

A estratégia adotada para a seleção dos processos foi elaborada pela Diretoria de Governança – DIGOV, baseando-se em critérios pré-estabelecidos, e posteriormente validados pelo CGI. Destaca-se que um dos critérios utilizados foi a percepção de riscos dos membros do CGI.

Assim, o gerenciamento de riscos irá acontecer de forma simultânea ao gerenciamento de processos nesses processos selecionados.

Entende-se que essa será a estratégia adotada até que todos os processos tenham sido gerenciados (previsão mínima para 2024), nesse momento o NGRI deverá adotar critérios de priorização próprio para a seleção dos processos anualmente. Essa metodologia deverá ser atualizada na ocasião de forma a incluir tais critérios.

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. O Núcleo de Gestão de Riscos irá apoiar sempre que possível nesse processo através de capacitações e participação ativa no processo.

Os recursos operacionais e tecnológicos necessários para apoiar a condução das atividades de Gestão de Riscos da CGU estão definidos no “Manual do processo de gerenciamento de riscos corporativos”, resultante da Gestão de Processos.

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, painéis gerenciais (*Business Intelligence* – BI), etc.

Trimestralmente o NGRI elaborará boletim informativo sobre os principais resultados dos trabalhos para o CGRI e CGI.

3.5 Capacitação

Com a integração da Gestão de Riscos à Gestão de Processos, o NGRI e o Escritório de Processos irão realizar capacitação em Gestão de Processos e Gestão de Riscos para os servidores que farão parte do Grupo de Gerenciamento de Processo e Riscos – GGP e para os líderes de processo.

4 Metodologia de Gestão de Riscos

A Metodologia de Gestão de Riscos 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 Metodologia de Gestão de Riscos da CGU é **orientada a processo organizacional** e obedece a um **modelo de aplicação e integrado à gestão de processos**. Ou seja, serão priorizados os processos selecionados para serem gerenciados pelo escritório de processos da CGU. **Processos que não foram selecionados, podem ter seus riscos gerenciados**, desde que obedecida essa metodologia e disponibilizado o resultado final ao NGRI e ao escritório de processos. Nesse último caso, o NGRI poderá auxiliar no processo dependendo de sua capacidade operacional.

Se já possuir metodologia própria, a unidade organizacional deve, justificar os motivos de sua utilização, visto que a Política de Gestão de Riscos determina o alinhamento de todas as metodologias à metodologia aprovada pelo CGI.

"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 Governança Interna

(...)

§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)"*

Atendendo tais diretrizes, a metodologia de Gestão de Riscos da CGU apresenta o seguinte ciclo:

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

Fonte: Núcleo de Gestão de Riscos e Integridade – NGRI

4.1 Plano de Gestão de Riscos

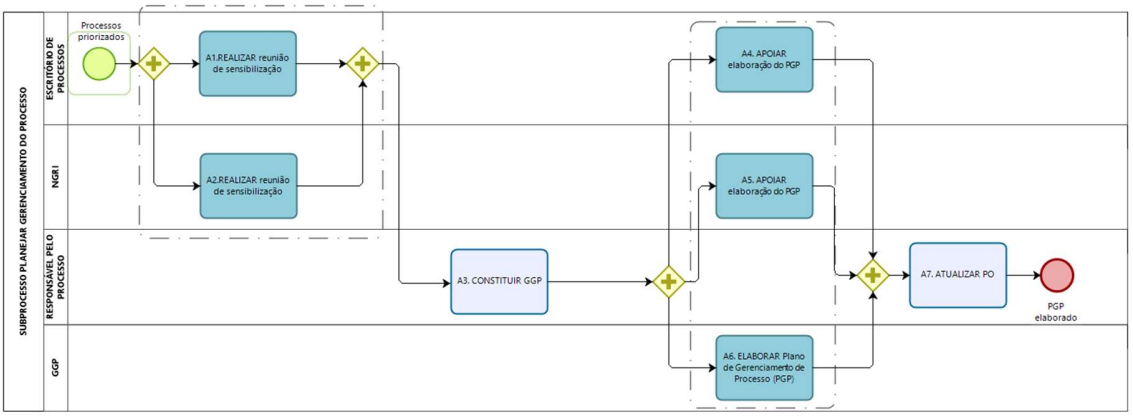
Entende-se por Plano de Gestão de Riscos, todo o planejamento e trabalhos necessários que antecedem a execução das etapas de gerenciamento de riscos. Para que se tenha êxito nas etapas posteriores é necessário que nessa etapa definam-se os seguintes pontos:

- Processos a serem gerenciados
- Responsável pelo processo
- Grupo de Gerenciamento do Processo
- Cronograma das atividades

Além desses pontos é necessário sensibilizar as partes bem como capacitar os membros do GGP.

A figura 3 apresenta o fluxo da etapa “Planejar Gerenciamento de Processo”, que é o equivalente a essa etapa no Gerenciamento de Processo

Figura 3: S.1 Etapa Planejar Gerenciamento de Processo



Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

4.2 Entendimento do Contexto

É nessa etapa que o processo organizacional é conhecido e analisado levando-se em consideração o ambiente interno e externo da CGU.

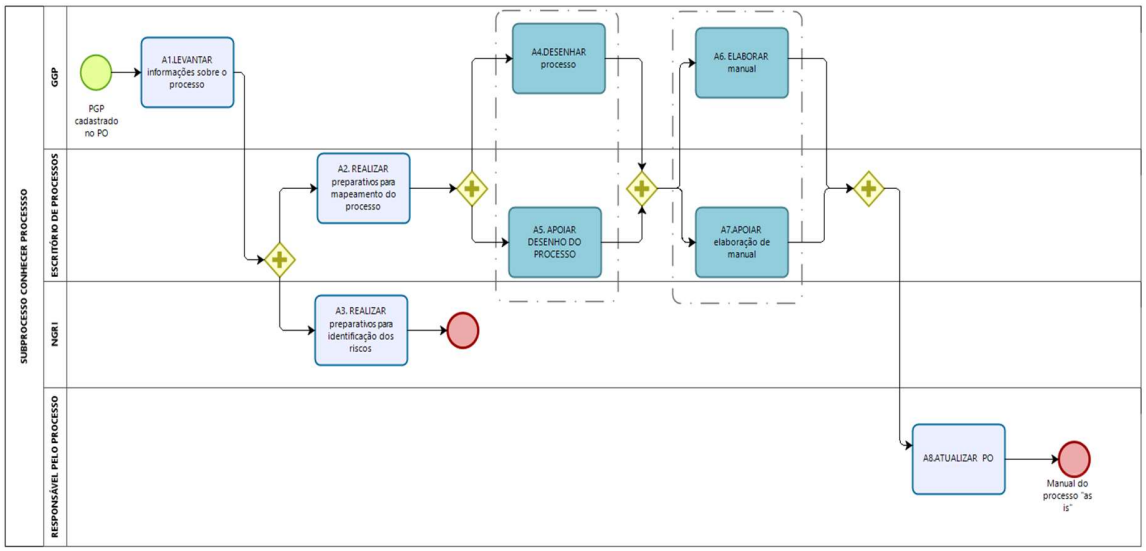
Para que essa etapa possa subsidiar as próximas etapas, é necessário uma compreensão completa do processo levantando-se no mínimo as seguintes informações:

- Clientes
- Fluxo do processo
- Infraestrutura utilizada
- Legislação correlacionada
- Principais objetivos do processo
- Principais problemas do passado
- Recurso humano utilizado
- Sistemas informatizados
- Partes interessadas
- Ambiente Externo (Cenário político, social, financeiro, legal, tecnológico, econômico, etc.)
- Tendências de mercado

No gerenciamento de processos tanto a etapa “Conhecer Processo” quanto a etapa “Analisar Processo e Riscos” contribuem com esse levantamento de informações e melhor compreensão do processo.

A figura 4 apresenta o fluxo da etapa “Conhecer Processo”:

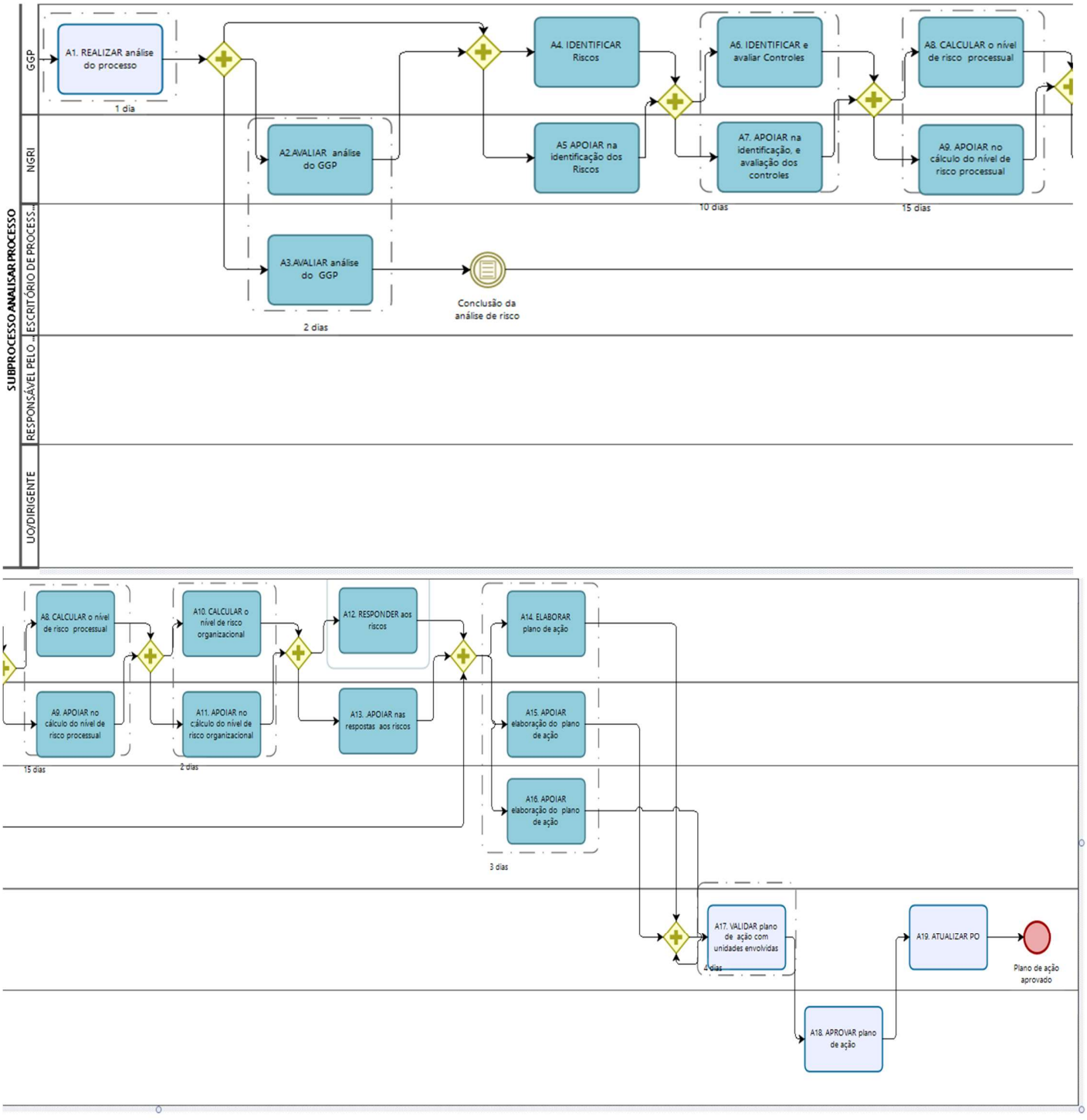
Figura 4: S.2 Conhecer Processo



Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

A figura 5 apresenta o fluxo da etapa “Analisar Processo e Riscos”. É importante destacar que apenas a análise do processo pertence a essa etapa de Entendimento do Contexto para a Gestão de Riscos:

Figura 5: S.3 Analisar Processo e Riscos



Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

4.3 Identificação de 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.

DICA: Os problemas do passado podem muitas vezes serem vistos como possíveis riscos futuros, sugere-se iniciar a lista de riscos a partir desses problemas.

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

- Objetivo do processo/subprocesso organizacional 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.

    O NGRI pode, a seu critério, categorizar um determinado risco em outras categorias de risco caso entenda ser necessário essa visão nos relatórios/painéis gerenciais.

- Causas: motivos que podem promover a ocorrência do risco;
- Consequências: resultado a ocorrência do risco afetando o objetivo do processo;

Para a identificação das causas é importante uma análise das diversas fontes de riscos existentes no processo, tais como:

a) Processo - Decorrente de diretrizes estratégicas e da formalização/modelagem de processos, incluídos os métodos, procedimentos e regulamentações de planejamento, execução, controle e monitoramento. Os mecanismos de comunicação e repositório de conhecimento também se enquadram nesta fonte.
b) Pessoas - Decorrente de operações humanas, onde são requeridas condutas apropriadas, competências, conhecimentos e habilidades
c) Externa - Decorrente do ambiente externo à organização como desastres naturais, conjuntura político-econômica, imprevisibilidade de fornecedores
d) Infraestrutura – Decorrente dos recursos de infraestrutura física ou lógica (sistemas de TI) da organização,
e) Recursos humanos ou financeiros – Decorrente da disponibilidade de recursos humanos ou financeiros

4.4 Identificação e Avaliação dos Controles

Após a identificação dos riscos, causas e consequências, é necessário identificar quais controles estão presentes no processo e mitigam os riscos identificados. Os controles devem ser classificados em:

- 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.
- Controles detectivos: controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

Após se identificar todos os controles associados aos riscos identificados é importante tentar identificar outros controles presentes no processo, possibilitando a identificação de outros riscos ou até mesmo de controles puramente burocráticos

Após a identificação de todos os controles, poderá ser feito um estudo mais aprofundado dos mecanismos de controle presentes no processo. Esse estudo tem como finalidade identificar controles ineficazes e ineficientes.

Para isso algumas perguntas devem ser respondidas:

1. Existem outros controles presentes nesse subprocesso? Caso existam, esses controles estão associados aos riscos identificados?

   Essa pergunta ajudará tanto na identificação de outros controles como de outros possíveis riscos. Além disso caso seja identificado controles aos quais a equipe técnica não consiga identificar um risco associado a ele, é bem possível que tal controle seja uma burocracia excessiva no subprocesso.

   Riscos e controles identificados nessa pergunta devem ser inseridos na planilha da mesma forma que na etapa anterior.

2. Na visão da equipe técnica, os controles identificados são eficazes? Caso a resposta seja negativa, é possível corrigir esses controles de forma a torna-los eficazes?

   Essa pergunta ajudará a avaliar os controles existentes no subprocesso. As informações aqui obtidas deverão ser utilizadas na construção do Plano de Tratamento de forma a otimizar os controles presentes, seja excluindo ou corrigindo os controles ineficazes.

3. O custo financeiro e/ou operacional de cada um dos controles identificados se justifica perante os riscos mitigados?

   Essa pergunta ajudará a identificar controles que apesar de mitigarem riscos, apresentam um custo financeiro e/ou operacional aquém do ideal, ou seja, não são eficientes. Os controles identificados nessa pergunta são fortes candidatos a serem substituídos por controles mais otimizados. O resultado dessa pergunta também será utilizado na construção do Plano de Tratamento.

É importante que seja feita uma associação entre os controles preventivos detectados e suas respectivas causas, assim como uma associação entre os controles de atenuação e recuperação e suas respectivas consequências. Essa associação será importante para a geração de relatórios gerenciais e alimentação do painel de riscos.

4.5 Cálculo dos níveis de risco

Nesta etapa, são calculados os níveis de risco dos eventos identificados pelo GGP, a partir de critérios de probabilidade e impacto. São realizados dois cálculos nessa etapa:

- Cálculo do nível de risco processual (foco no processo)
- Cálculo do nível de risco organizacional (foco na CGU)

4.5.1 Cálculo do nível de risco processual

O cálculo do nível de risco processual levará em consideração o impacto no processo em questão conforme pode ser visto nos quadros 3 e 4, que trazem as escalas de probabilidade e impacto, respectivamente:

Quadro 3: Escala de Probabilidade		
Probabilidade	**Descrição da probabilidade**	**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.	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, as circunstâncias indicam claramente essa possibilidade.	5

Fonte: Núcleo de Gestão de Riscos e Integridade – NGRI

Quadro 4: Escala de Impacto		
Impacto	**Descrição do impacto nos objetivos, caso o evento ocorra**	**Peso**
Muito baixo	**Mínimo** impacto nos objetivos do processo	1
Baixo	**Pequeno** impacto nos objetivos do processo.	2
Médio	**Moderado** impacto nos objetivos do processo, porém recuperável.	3
Alto	**Significativo** impacto nos objetivos do processo, de difícil reversão.	4
Muito Alto	**Catastrófico** impacto nos objetivos do processo, de forma irreversível.	5

Fonte: Núcleo de Gestão de Riscos e Integridade - NGRI

A multiplicação entre os valores de probabilidade e impacto irá definir o nível de risco processual, ou seja, o provável impacto nos objetivos do processo organizacional.

NR = NP x NI

em que:

NR = nível do risco

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 – 4,99
Risco Médio - RM	5 – 11,99
Risco Alto - RA	12 – 19,99
Risco Extremo - RE	20 – 25

Fonte: Núcleo de Gestão de Riscos e Integridade

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

Quadro 6: Matriz de Riscos						
IMPACTO	**Muito Alto 5**	5 RM	10 RM	15 RA	20 RE	25 RE
	Alto 4	4 RB	8 RM	12 RA	16 RA	20 RE
	Médio 3	3 RB	6 RM	9 RM	12 RA	15 RA

	Baixo 2	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RB	5 RM
		Muito Baixa 1	**Baixa 2**	**Média 3**	**Alta 4**	**Muito Alta 5**
		PROBABILIDADE				

Fonte: Gestão de Riscos – Núcleo de Gestão de Riscos e Integridade

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

1. Risco inerente – A equipe técnica deve imaginar o processo em questão sem nenhum mecanismo de controle implementado.
2. Risco residual – A equipe técnica deve imaginar o processo em questão com os atuais mecanismos de controle implementados.

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

4.5.2 Cálculo do nível de risco organizacional

Riscos residuais classificados como "Extremo" no cálculo anterior* (4.5.1) serão reavaliados 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 os critérios de impacto utilizados nessa etapa. O critério de probabilidade deverá ser um valor de 0% a 100%, que represente a estimativa da chance do risco se materializar em um ciclo do processo. *Além dos riscos classificados como "Extremo", riscos com as outras classificações (baixo, médio ou alto) podem ser objeto do Cálculo do Nível de Risco Organizacional (seção 4.10), desde que indicados pelo dirigente máximo da unidade ou pelo NGRI.

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 Governança Interna da CGU, para a priorização para tratamento de riscos de diferentes processos.

Durante essa etapa, 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 residuais 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[1]. Esse resultado será apresentado ao Comitê de Governança Interna por meio do painel de riscos.

Os resultados obtidos através do Cálculo do Nível de Risco Organizacional subsidiarão a priorização quanto à alocação de recursos para o atingimento de objetivos institucionais, que poderá refletir na revisão dos Planos de Ação dos riscos propostos pelas unidades.

O Apêndice I apresenta os critérios que devem ser utilizados nesse cálculo.

4.6 Respostas aos riscos

Nesta etapa, devem ser considerados os valores dos níveis de riscos calculados na etapa anterior para a priorização e otimização das respostas.

A faixa de classificação do risco deve ser considerada para a definição da atitude da unidade em relação à priorização para tratamento. O quadro 7 mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções (apetite ao risco).

Quadro 7: 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.

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

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 do Cálculo do Nível de Risco Organizacional (seção 4.10), comunicado ao Comitê de Governança Interna e ao dirigente máximo da unidade e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Governança Interna.	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 Governança Interna.

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 Governança Interna (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.

Cada risco 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 8

Quadro 8: 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 Governança Interna.
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: Núcleo de Gestão de Riscos – NGRI/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 Ação do ponto de vista do gerenciamento de riscos é um plano para a implementação das medidas de tratamento. Por isso, deve conter, pelo menos:

- Medida(s) de tratamento contemplada(s)e o risco relacionado que deseja tratar;

- Objetivos/benefícios esperados por medida de tratamento;
- Responsável pela implementação;
- Breve descrição sobre a implementação;
- Custo estimado para implementação;
- Data prevista para início da implementação;
- Data prevista para o término da implementação;

É importante que, em uma primeira abordagem da elaboração do Plano de Ação, avalie-se a necessidade de melhorar ou extinguir controles já existentes, utilizando os resultados da etapa "Avaliação dos controles processuais". 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 Ação 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.

4.6 Validação dos resultados

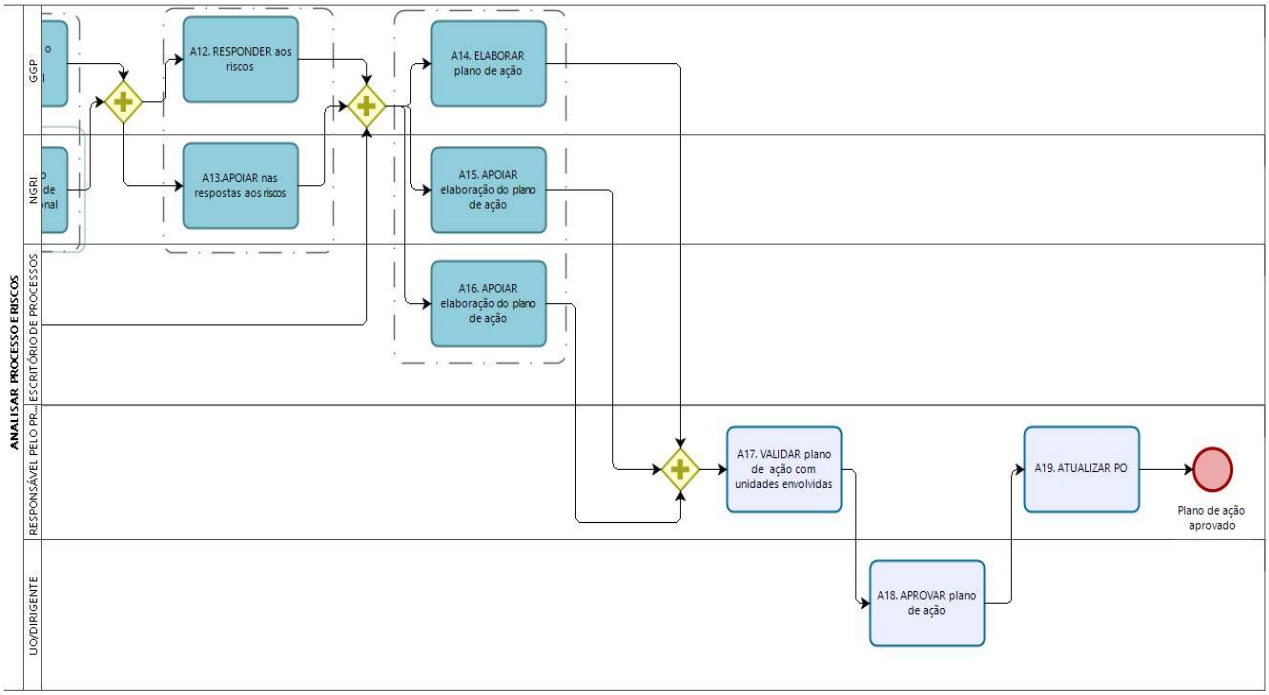
Os resultados das etapas anteriores e o plano de Ação devem ser aprovados pelo dirigente máximo da unidade.

Após a aprovação a unidade deve incluir tais ações em seu Plano Operacional.

Em caso de envolvimento de outras unidades para a implementação do plano de ação essa negociação entre unidades deve ser feita antes da aprovação do Plano de Ação. Cabe ao responsável pelo processo a validação das ações com as demais áreas.

A figura 6 apresenta o fluxo da etapa "Analisar Processo e Riscos", onde ocorre a aprovação do Plano de Ação.

Figura 6: S.3 Analisar Processo e Riscos



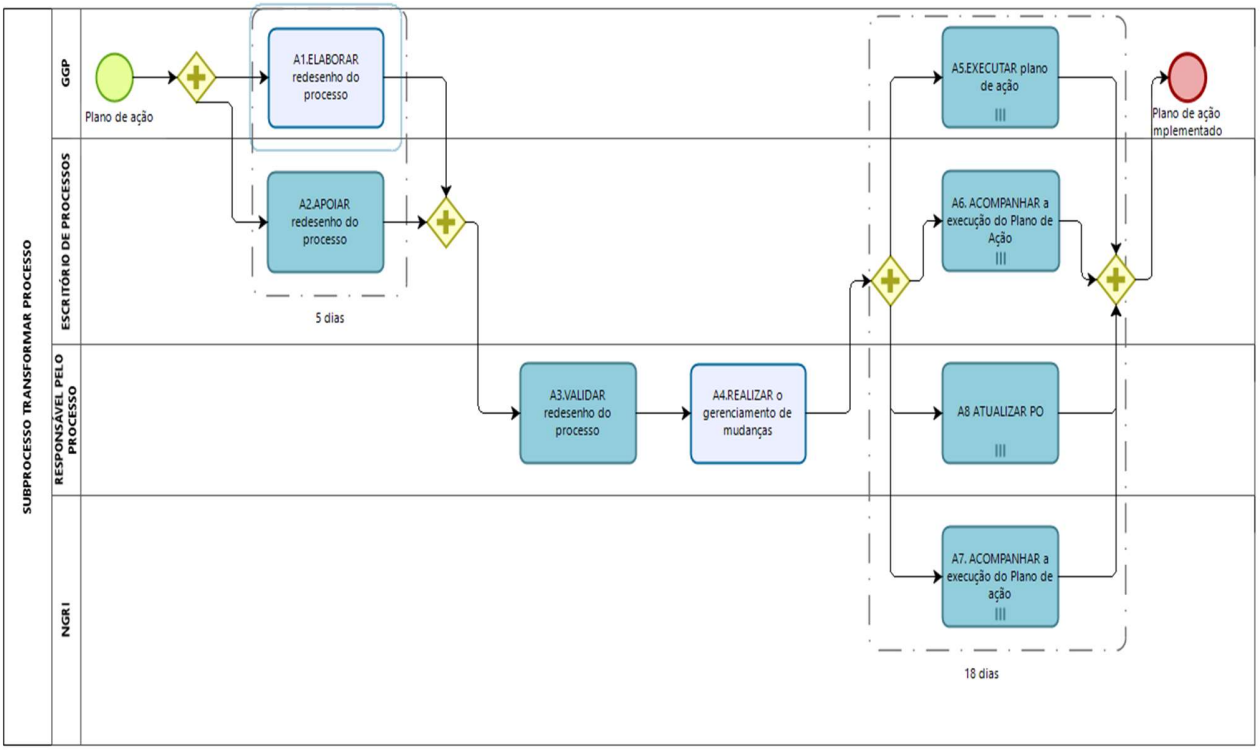
Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

4.7 Implementação do Plano de Ação

A implementação do Plano de Ação envolve a participação da unidade responsável pelo processo organizacional e possivelmente de outras unidades que também participem do processo ou que as ações necessárias sejam de sua respectiva competência. A responsabilidade primária pelo Plano de Ação permanece com o responsável pelo processo organizacional.

A figura 7 apresenta o fluxo da etapa “Transformar Processo”, que é o equivalente a essa etapa no Gerenciamento de Processo

Figura 7: S.4 Transformar Processo



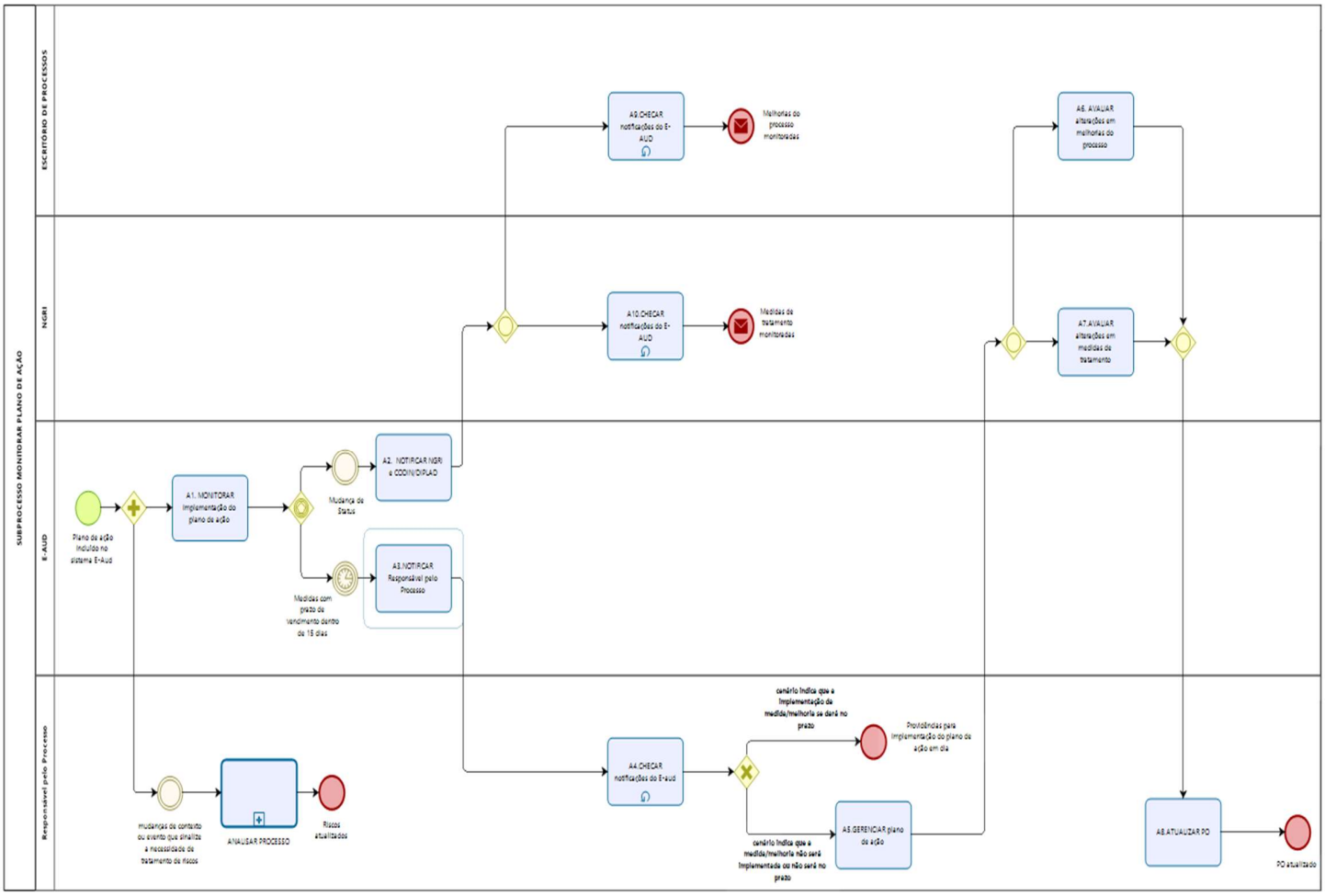
Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

4.8 Comunicação e Monitoramento

Segundo a ISO 31000:2018, durante todas as etapas do processo de gerenciamento de riscos, é importante comunicar as partes interessadas.

Além da comunicação já apresentada nas etapas anteriores, após elaboração do Plano de Ação, o NGRI irá monitorar sua implementação conforme a figura 8 que apresenta a etapa "Monitorar Plano de Ação" do Gerenciamento de Processo.

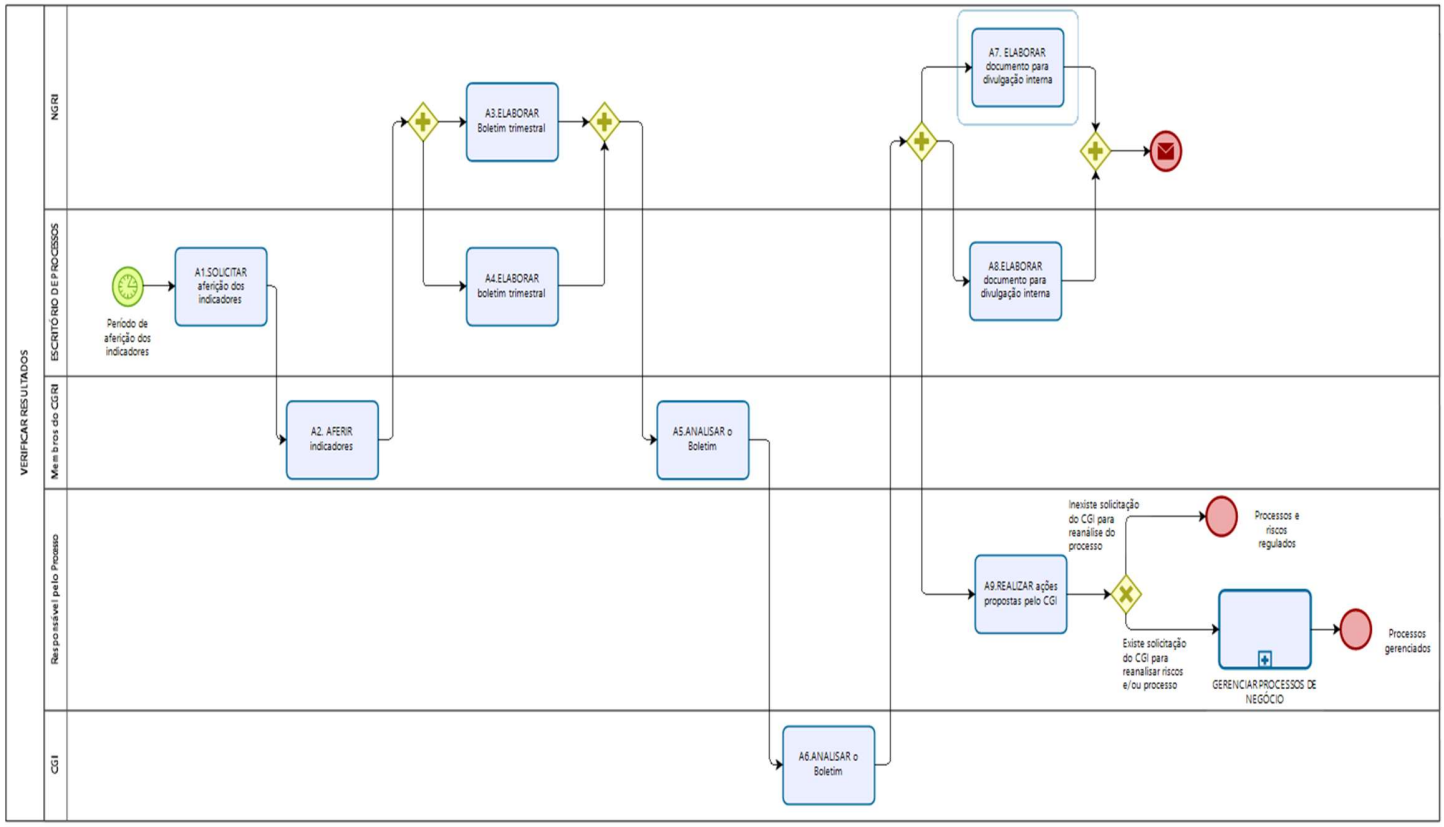
Figura 8: S.6 Monitorar Plano de Ação



Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

Além do monitoramento do plano de ação o NGRI irá reportar trimestralmente as instâncias de governança com as informações mais importantes dos trabalhos realizados no trimestre, conforme figura 9, que apresenta a etapa “Verificar Resultados” do Gerenciamento de Processo.

Figura 9: S.7 Verificar Resultados



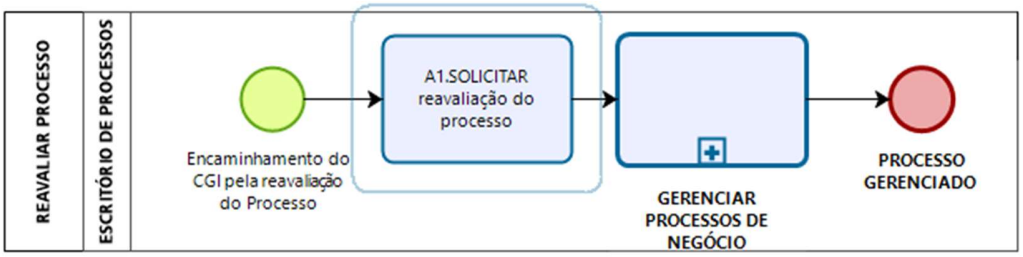
Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

4.9 Ciclo de reavaliação

A qualquer tempo, o CGI pode decidir por reavaliar parte ou todo processo organizacional, bem como executar a metodologia completa ou apenas algumas etapas.

A figura 10 mostra a etapa “Reavaliar Processo” do Gerenciamento de Processo.

Figura 10: S.8 Reavaliar Processo



Fonte: Núcleo de Gestão de Riscos – NGRI/CGU e Diretoria de Governança - DIGOV.

5. Referências Bibliográficas

ABNT. **Gestão de Riscos – Princípio e diretrizes. NBR ISO 31000**. Associação Brasileira de Normas Técnicas. 2018.

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 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 182,** de 22 de dezembro de 2020, que aprova o Planejamento Estratégico da CGU para o quadriênio 2020-2023.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos.**

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade.**

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. 2017.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Risk Assessment in Practice.**

IIA. The Institute of Internal Auditors. **Modelo das 3 três linhas do IIA 2020 – Uma atualização das três linhas de defesa.**

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

Apêndice I – Critérios utilizados no Cálculo do Nível de Risco Organizacional

A etapa de Cálculo do Nível de Risco Organizacional utiliza critérios de avaliação específicos para a dimensão de 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 impacto. Cada critério possui alternativas, com valores entre 0% e 100%.

Critérios de Impacto para o Cálculo do Nível de Risco Organizacional			
	Missão Institucional	Imagem Institucional	Orçamentário/Financeiro
100%	MI 10 - Após o ocorrido, um ou mais aspectos da missão institucional da CGU entrariam em colapso (participação social, controle interno governamental e combate à corrupção).	II 10 - A imagem da CGU seria totalmente prejudicada, resultando num descrédito da maioria da população brasileira. O fato provavelmente chamará atenção da mídia nacional e internacional.	OR 10 >= R$ 25.000.000
80%	MI 08 - Após o ocorrido, um ou mais aspectos da missão institucional da CGU apresentariam um considerável retrocesso (participação social, controle interno governamental e combate à corrupção).	II 08 - A imagem da CGU seria fortemente prejudicada, resultando num descrédito de boa parcela da sociedade brasileira. O fato provavelmente chamará atenção da mídia nacional e local.	OR 08 >= R$ 10.000.000 < R$ 25.000.000
60%	MI 06 - Após o ocorrido, um ou mais aspectos da missão institucional da CGU apresentariam um pequeno retrocesso (participação social, controle interno governamental e combate à corrupção).	II 06 - A imagem da CGU seria moderadamente prejudicada, resultando num descrédito de uma parcela especifica da população brasileira. O fato provavelmente chamará atenção da mídia local.	OR 06 >= R$ 3.000.000 < R$ 10.000.000
40%	MI 04 - Após o ocorrido, um ou mais aspectos da missão institucional da CGU apresentariam uma evolução tímida perto de seus potenciais de crescimento; ou (participação social, controle interno governamental e combate à corrupção).	II 04 - A imagem da CGU seria levemente prejudicada, resultando num descrédito de uma pequena parcela da população brasileira. O fato talvez chamará atenção da mídia local.	OR 04 >= R$ 1.000.000 < R$ 3.000.000
20%	MI 02 - Após o ocorrido, um ou mais aspectos da missão institucional da CGU apresentariam uma evolução um pouco aquém do esperado (participação social, controle interno governamental e combate à corrupção).	II 02 - A imagem da CGU seria prejudicada apenas na visão dos envolvidos no fato, não haverá descredito por parte da sociedade. O fato dificilmente chamará atenção da mídia.	OR 02 < R$ 1.000.000
0%	MI 00 - Nenhuma abrangência dos efeitos na missão da CGU.	II 00 - A imagem da CGU se mantém intacta seja pela não gravidade do ocorrido, ou pelas ações possíveis de reparação, ou mesmo pela impossibilidade da sociedade vir a conhecer o fato.	OR 00 - Sem impacto financeiro/orçamentário.

Fonte: Núcleo de Gestão de Riscos e Integridade – NGRI/CGU.

A definição dos critérios utilizados no Cálculo do Nível de Risco Organizacional 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.

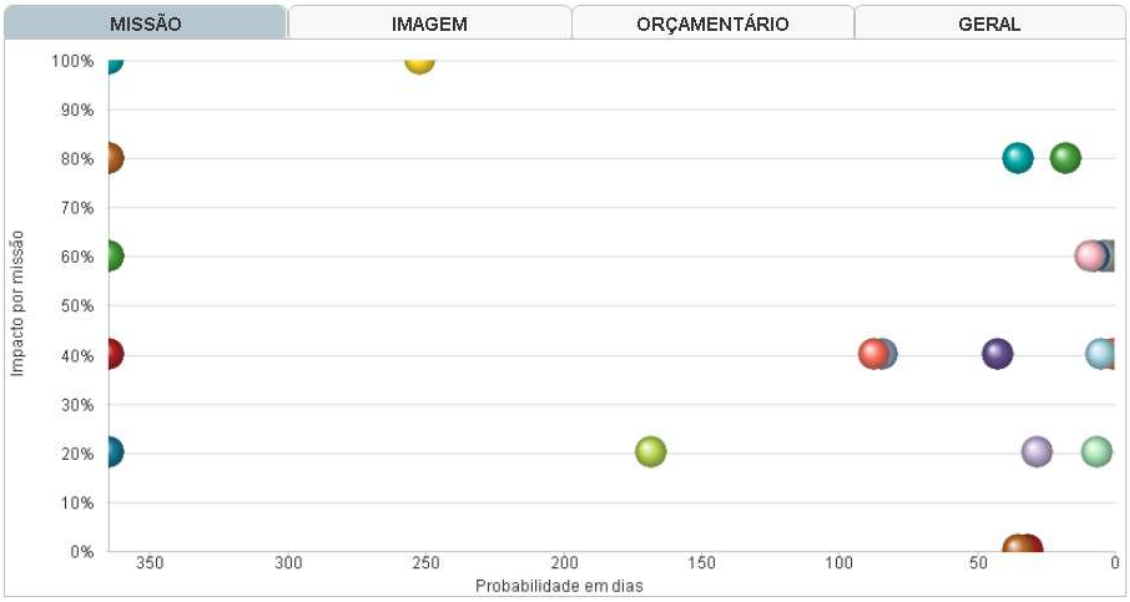
A avaliação de cada membro do Comitê Gerencial deve ser aprovada pelo dirigente máximo da respectiva unidade organizacional antes do retorno ao Núcleo de Gestão de Riscos.

c) 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.

O resultado dessa etapa será visualizado no painel de riscos da CGU, permitindo uma visão individual das 3 dimensões de impacto e uma consolidada, conforme figura 11.

Figura 11: Painel de Riscos



Fonte: Núcleo de Gestão de Riscos – NGRI/CGU