METODOLOGIA DE GESTÃO DE RISCOS

DA PRESIDÊNCIA DA REPÚBLICA

PRESIDÊNCIA DA REPÚBLICA
Jair Messias Bolsonaro

VICE-PRESIDÊNCIA DA REPÚBLICA
Antonio Hamilton Martins Mourão

CASA CIVIL
Ciro Nogueira

SECRETARIA DE GOVERNO
Flávia Arruda

SECRETARIA-GERAL
Luiz Eduardo Ramos Baptista Pereira

GABINETE DE SEGURANÇA INSTITUCIONAL
Augusto Heleno Ribeiro Pereira

GABINETE PESSOAL
Celio Faria Junior

ASSESSORIA ESPECIAL DO PRESIDENTE DA REPÚBLICA
João Henrique Nascimento de Freitas

SECRETARIA ESPECIAL DE ASSUNTOS ESTRATÉGICOS
Flávio Augusto Viana Rocha

SUMÁRIO

I. APRESENTAÇÃO

Segundo o Decreto nº 9.203/2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, a **gestão de riscos é um dos elementos que compõe os mecanismos da governança pública destinado a fornecer uma segurança razoável à organização quanto ao atingimento dos seus objetivos.** Esse Decreto estabelece, em seu art. 4º, inciso VI, a gestão de riscos como uma das diretrizes da governança e preconiza, no artigo 17, que

> *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. (BRASIL, 2017, grifo nosso).*

Diante disso, a Presidência da República, por meio do Comitê Integrado de Governança da Presidência da República (Cigov/PR), instituiu a **Política de Gestão de Riscos da Presidência da República - PGR/PR** (Resolução nº 3, de 6 de dezembro de 2021), que estabelece os princípios, as diretrizes e os mecanismos relativos à Gestão de Riscos no âmbito dos órgãos da Presidência da República e, supletivamente, da Vice-Presidência da República.

A PGR/PR é o resultado da união dos esforços das casas palacianas, no sentido de desenvolver uma cultura de gestão de riscos, com os objetivos de: (i) assegurar aos tomadores de decisão, em todos os níveis da estrutura organizacional, o acesso tempestivo às informações quanto aos riscos a que está exposta a organização; (ii) aumentar a probabilidade de alcance dos objetivos organizacionais, reduzindo os riscos a níveis aceitáveis; e (iii) agregar valor à organização por meio da melhoria dos

processos de tomada de decisão e do tratamento adequado dos riscos e seus impactos negativos.

Conceitualmente, segundo a ABNT NBR ISO 31000:2018, o **risco** é o efeito da incerteza nos objetivos, e de acordo com a IN MP/CGU nº 01/2016, risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e probabilidade.

A **gestão de riscos**, por sua vez, é a arquitetura necessária (princípios, objetivos, estrutura, competências e processos) para se gerenciar riscos eficazmente (CGU, 2017). A ABNT NBR ISO 31000:2018 a define como sendo **atividades coordenadas** para dirigir e controlar uma organização no que se refere a riscos. Gerenciar riscos, portanto, é um processo contínuo, que flui pela organização, permeando-a em todos os níveis e unidades. Esse gerenciamento é formulado para identificar eventos em potencial, cuja ocorrência poderá afetar a organização, sendo capaz de propiciar razoável garantia quanto ao alcance dos objetivos.

Este documento, portanto, apresenta a Metodologia de Gestão de Riscos da PR, um trabalho conjunto entre os órgãos da Presidência e Vice-Presidência da República, elaborado com o objetivo de direcionar, de forma coordenada, a gestão dos riscos em suas unidades, a partir de procedimentos simplificados e passíveis de evidenciação, com vistas a reduzir os riscos que possam comprometer o cumprimento de sua missão institucional.

II. FUNDAMENTOS DA GESTÃO DE RISCOS

O conteúdo deste documento é destinado ao contexto da gestão de riscos e controles internos e observa um conjunto de normas e regulamentações, **frameworks** e referências internacionais relacionadas à temática, dos quais destacam-se:

- Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal;
- Resolução Cigov nº 3, de 6 de dezembro de 2021, que institui a Política de Gestão de Riscos da Presidência da República;
- Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal;
- ABNT NBR ISO 31.000: 2018, Gestão de Riscos - Princípios e Diretrizes;
- COSO[1] II GRC - **Enterprise Risk Management Integrating with Strategy and Performance** (2017);
- ABNT ISO GUIA 73:2009, Gestão de Riscos: Vocabulário;
- Guia Prático de Gestão de Riscos para a Integridade da CGU, de 2018;
- Modelo das Três Linhas do IIA[2] 2020 – Uma atualização das Três Linhas de Defesa.

A partir dos referenciais supracitados foram extraídos alguns conceitos essenciais para o entendimento do tema e do processo de gerenciamento dos riscos, descritos no art. 2º da PGR/PR, ressaltados a seguir:

I - **accountability**: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram, os quais

[1] *Committee of Sponsoring Organizations of the Treadway Commission.*
[2] *The Institute of Internal Auditors.*

evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

II - apetite a risco: nível de risco que uma organização está disposta a aceitar no contexto da condução de determinada(o) política, estratégia, plano, sistema, programa, projeto, ação, esforço ou recurso;

III - auditoria interna: atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização;

IV - controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável e suficiente a que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;

b) cumprimento das obrigações de accountability;

c) cumprimento das leis e regulamentos aplicáveis; e

d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa, essencialmente, aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica;

V - gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, o qual contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, sendo destinado a fornecer segurança razoável à efetiva realização de seus objetivos;

VI - **governança pública:** conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

VII - **matriz de risco:** ferramenta para classificar e apresentar riscos definindo faixas para consequência e probabilidade;

VIII - **modelo de três linhas**: modelo desenvolvido pelo **The Institute of Internal Auditors** (IIA), cujo objetivo é o de ajudar organizações na identificação de estruturas e processos que melhor auxiliem no atingimento dos objetivos, propiciando uma governança forte e o efetivo gerenciamento de riscos;

IX - **nível de risco**: magnitude de um risco expressa em termos da combinação das consequências e de suas probabilidades;

X - **objetivo organizacional**: situação que se deseja alcançar de forma a evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização ou, na falta desses, evidenciar êxito no cumprimento das atribuições legais da organização;

XI - **processo de trabalho**: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

XII - **risco**: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

XIII - **risco inerente**: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

XIV - **risco residual**: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco; e

XV - tolerância ao risco: disposição da organização ou parte interessada em suportar o risco após o tratamento do risco a fim de atingir seus objetivos. Pode ser influenciada por requisitos legais ou regulatórios.

FATORES CRÍTICOS DE SUCESSO PARA A GESTÃO DE RISCOS

Fatores Críticos de Sucesso (FCS) são aqueles essenciais para o sucesso ou fracasso no alcance de determinado objetivo, referem-se às barreiras e aos facilitadores que influenciam determinada prática (BULLEN; ROCKART, 1981).

Assim sendo, a seguir estão listados os FCS para o Sistema de Gestão de Riscos da PR:

- Pleno apoio e compromisso da alta direção;
- Engajamento de pessoas que garantam um panorama suficientemente completo do órgão/entidade e seus riscos;
- Identificação e descrição dos riscos com o detalhamento necessário para sua análise;
- Avaliação dos riscos com base em uma apreciação realista de sua probabilidade e impacto;
- Documentação precisa;
- Revisão periódica;
- Comunicação efetiva que garanta o desenho de controles apropriados;
- Estabelecimento de mecanismos de supervisão/controle adequados;
- Adequação do processo à realidade do órgão/entidade[3];
- Compartilhamento de conhecimento e experiências com outros órgãos/entidades;
- Orientação para mudanças de mentalidade e estímulo ao comportamento íntegro na organização.[4]

[3] Cumpre ressaltar que o processo de gestão de riscos deverá se adequar às especificidades normativas relacionadas a riscos de cada unidade, de forma a se evitar duplicidade de processos e redundância de procedimentos.

[4] SELINŠEK, 2015 apud CGU, 2018.

III. PRINCÍPIOS, DIRETRIZES E OBJETIVOS DA GESTÃO DE RISCOS DA PR

De acordo com a Política de Gestão de Riscos da PR, arts. 3º, 4º e 5º, são os seguintes princípios, diretrizes e objetivos que orientam o processo de Gestão de Riscos da PR:

A. PRINCÍPIOS DA GESTÃO DE RISCOS

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

II - estabelecimento de níveis adequados de exposição a riscos;

III - observância da relação custo-benefício para a adoção dos controles internos, aplicando-se a análise da proporcionalidade em relação ao risco;

IV - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, mantendo sua subordinação aos interesses públicos;

V - utilização do mapeamento de riscos para apoio à tomada de decisão;

VI - monitoramento e melhoria contínua do desempenho e dos processos de gestão de risco, controle e governança;

VII - apoio e comprometimento da alta administração, e da liderança de todos os níveis de gestão, obtendo-se o engajamento de todo o corpo funcional;

VIII - consideração dos fatores humanos e culturais; e

IX - capacitação de agentes públicos e comunicação contínua.

B. DIRETRIZES DA GESTÃO DE RISCOS

I - ser sistematizado, iterativo e colaborativo, com base nos contextos internos e externos, e nos objetivos institucionais da organização, considerando os fatores humanos e culturais;

II - ser aplicado a cada processo de trabalho que compõe a cadeia de valor da organização, sejam eles finalísticos, de apoio ou gerenciais;

III - ser realizado em ciclos anuais, compreendendo a hierarquização e a priorização dos processos de trabalho, assim como a avaliação, o tratamento e o monitoramento dos respectivos riscos identificados;

IV - disseminar as informações necessárias ao fortalecimento da cultura e da valorização dos controles internos da gestão; e

V - desenvolver continuamente os agentes públicos da Presidência da República em gestão de riscos.

C. OBJETIVOS DA GESTÃO DE RISCOS

I - assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar, se for o caso, questões relativas à delegação;

II - aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis; e

III - agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

IV. SISTEMA DE GESTÃO DE RISCOS DA PR

Segundo o Modelo de Três Linhas, a **governança de riscos é formada pelo corpo administrativo** que garante que as estruturas e processos adequados estejam em vigor para uma governança eficaz e que os objetivos e as atividades organizacionais estejam alinhados com os interesses priorizados pelas partes interessadas (art. 8º da PGR/PR):

a) como os processos serão hierarquizados e priorizados;

b) como os riscos serão identificados, avaliados, tratados, comunicados e monitorados;

c) como será medido o desempenho da gestão de riscos, para sua melhoria contínua;

d) quais ferramentas serão utilizadas para a execução da gestão de riscos; e

e) quais tipologias de riscos podem afetar o alcance dos objetivos da Presidência da República.

De acordo com a PGR/PR, art. 9º, integram o Sistema de Gestão de Gestão de Riscos da PR os seguintes instrumentos:

a) a política de gestão de riscos;

b) a metodologia de gestão de riscos;

c) o processo corporativo de gerenciamento de riscos;

d) a ferramenta de gestão de riscos vinculada aos processos de trabalho; e

e) a capacitação continuada em gestão de riscos, incluída no plano de capacitação da Presidência da República.

A. MODELO DE TRÊS LINHAS DA PR

O Sistema de Gestão de Riscos da PR baseia-se na concepção do Modelo das Três Linhas, desenvolvido pelo The Institute of Internal Auditors (IIA), e está organizado da seguinte forma, conforme demonstrado na figura 1 (art. 12 da PGR/PR):

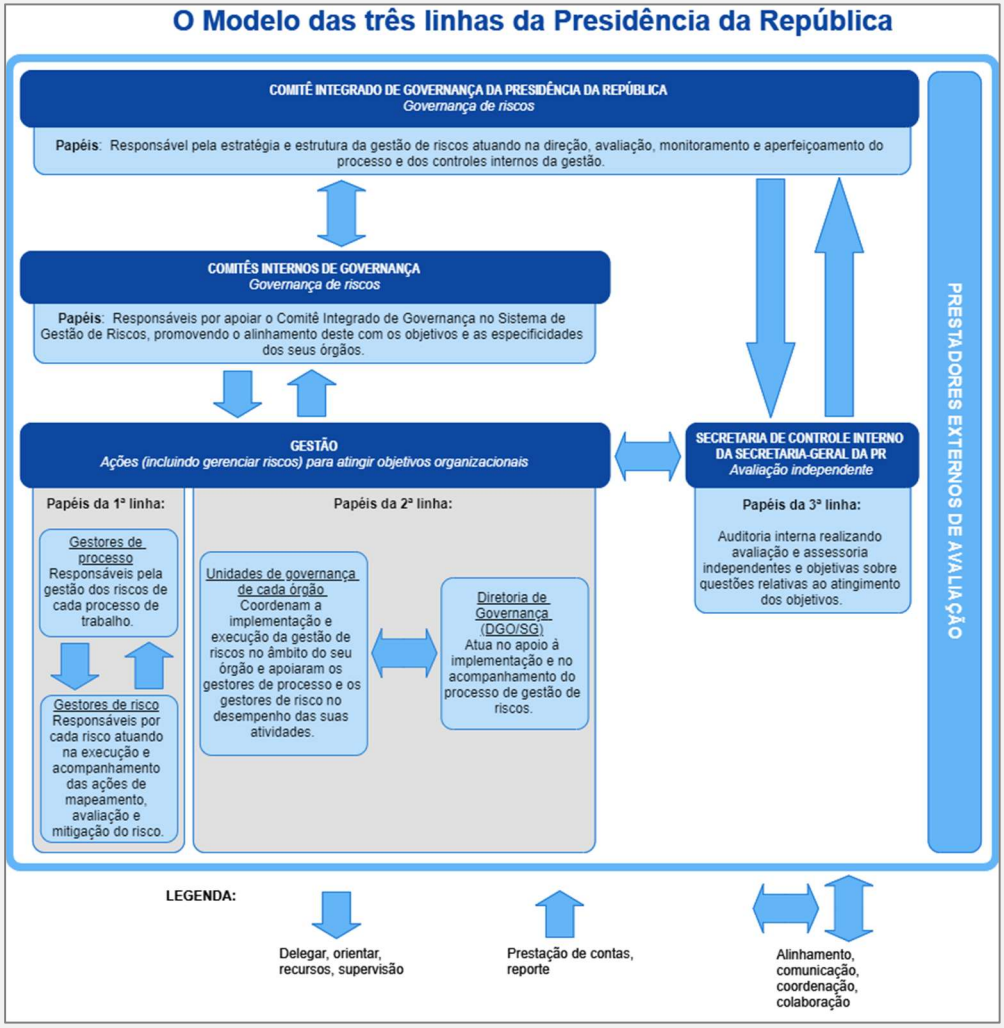

Figura 1 – Sistema de Gestão de Riscos da PR.

1. Governança de riscos

Segundo o Modelo de Três Linhas, a **governança de riscos é formada pelo corpo administrativo** que garante que as estruturas e processos adequados estejam em vigor para uma governança eficaz e que os objetivos e as atividades organizacionais estejam alinhados com os interesses priorizados pelas partes interessadas.

A Governança de Riscos na PR é desempenhada por:

a) **Comitê Integrado de Governança da Presidência da República**, responsável pela estratégia e estrutura da gestão de riscos da Presidência da República, que atuará na direção, avaliação, monitoramento e aperfeiçoamento do processo e dos controles internos da gestão; e

b) **Comitês internos de governança dos Órgãos da Presidência da República**, responsáveis por apoiar o Comitê Integrado de Governança da Presidência da República no Sistema de Gestão de Riscos, promovendo o alinhamento deste com os objetivos e as especificidades dos seus órgãos.

2. Gestão de riscos em primeira linha

Os papéis da primeira linha estão mais diretamente alinhados **com a entrega de produtos e/ou serviços aos clientes da organização,** incluindo funções de apoio. Sendo assim, é na primeira linha que ocorrem as atividades relacionadas à implementação e execução do processo de gestão de riscos.

Na PR, a Gestão de riscos em primeira linha é desempenhada pelos:

a) **gestores de processo:** responsáveis pela gestão dos riscos de cada processo de trabalho; e
b) **gestores de risco**: responsáveis por cada risco mapeado, formalmente identificado, que atuarão na execução e acompanhamento das ações de mapeamento, avaliação e mitigação do risco, de acordo com as suas competências.

3. Gestão de riscos em segunda linha

À Gestão de riscos em segunda linha cabe fornecer expertise, apoio, monitoramento e questionamento sobre temas relacionados à riscos. Seu papel é o de prover assistência à gestão de riscos em primeira linha.

Esse papel, na PR, é desempenhado por:

a) **unidades de governança representantes de cada órgão** que compõe o Comitê Integrado de Governança da Presidência da República que coordenam a implementação e execução da gestão de riscos no âmbito do seu órgão e apoiam os gestores de processo e os gestores de risco no desempenho das suas atividades; e
b) **Diretoria de Governança da Secretaria-Executiva da Secretaria-Geral (DGO/SG)**, que atua no apoio à implementação e no acompanhamento do processo de gestão de riscos da PR.

4. Gestão de riscos em terceira linha

A terceira linha da gestão de riscos é composta pela **Auditoria Interna** da organização e tem como responsabilidade **prestar avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos**, bem como reportar suas descobertas à gestão e ao órgão de governança para promover e facilitar a melhoria contínua.

A Gestão de riscos em terceira linha na PR é constituída pela auditoria interna no âmbito da PR, atividade exercida pela **Secretaria de Controle Interno da Secretaria-Geral da Presidência da República (Ciset)**.

B. COMPETÊNCAS E RESPONSABILIDADES

A Resolução nº 3/2021, do Cigov, estabelece as seguintes competências e responsabilidades para a efetivação do Sistema de Gestão de Riscos da PR:

1. Compete ao **Cigov/PR** (art. 13 da PGR/PR):

I - aprovar a Política de Gestão de Riscos da Presidência da República e suas revisões;

II - aprovar a metodologia de Gestão de Riscos da Presidência da República e suas revisões;

III - aprovar a avaliação dos indicadores críticos de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da Presidência da República;

IV - produzir o apoio institucional para a promoção da Gestão de Riscos, em especial os seus instrumentos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo das lideranças e servidores da Presidência da República;

V - aprovar as estratégias propostas para tratamento dos riscos críticos da Presidência da República;

VI - implementar o alinhamento da gestão de riscos ao Programa de Integridade da Presidência da República; e

VII - supervisionar, em conjunto com os Comitês Internos de Governança, a implantação e a execução da Gestão de Riscos nos órgãos da Presidência da República.

2. Compete aos **Comitês internos de governança** (art. 14 da PGR/PR):

I - auxiliar a alta administração de seu órgão na implementação da Política e da Metodologia de Gestão de Riscos da Presidência da República, e suas revisões;

II - promover e acompanhar, no âmbito do seu órgão, a implementação das medidas, dos mecanismos e das práticas relacionadas à Gestão de Riscos definidos pelo Comitê Integrado de Governança da Presidência da República; e

III - recomendar ao Comitê Integrado de Governança da Presidência da República medidas para o aprimoramento da Gestão de Riscos na Presidência da República.

3. Compete à **DGO/SG** (art. 15 da PGR/PR):

   I - apoiar a implementação da Política de Gestão de Riscos e acompanhar a sua aplicação, no âmbito da PR;

   II - coordenar a elaboração e validação das propostas dos instrumentos e artefatos produzidos pela Gestão de Riscos da Presidência da República, para aprovação do Cigov/PR;

   III - acompanhar e avaliar os indicadores de desempenho para a Gestão de Riscos; e

   IV - garantir o apoio institucional para promover a Gestão de Riscos, em especial os seus instrumentos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo das lideranças e servidores da PR, no âmbito de cada Unidade.

4. Compete às **Unidades de Governança dos órgãos da PR** (art. 16 da PGR/PR):

   I - contribuir na elaboração e validação das propostas dos instrumentos e artefatos produzidos pela Gestão de Riscos da Presidência da República;

   II - acompanhar a efetividade das ações e dos controles internos propostos para tratamento dos riscos críticos da sua unidade, e sugerir melhorias;

   III - elaborar os indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da sua unidade;

   IV - colaborar no apoio institucional para promoção da Gestão de Riscos e o desenvolvimento contínuo das lideranças e servidores da Presidência da República no âmbito da sua unidade; e

   V - informar ao Comitê Interno de Governança do seu Órgão sobre assuntos que possam impactar o desempenho da Gestão de Riscos.

5. Compete à **Ciset** realizar avaliações independentes e oferecer assessoramento às unidades para o aprimoramento dos processos de governança, de gestão de riscos e de controles internos da gestão.

6. Compete ao **gestor de risco**, a disponibilização das informações adequadas sobre os riscos ao gestor de processo e aos demais níveis da organização.
7. Compete aos **gestores de processo** aplicar o gerenciamento de riscos nos processos de trabalho pelos quais são responsáveis.

C. ESTABELECIMENTO DE LIMITES DE EXPOSIÇÃO A RISCOS

Compete à Alta Administração definir o estabelecimento dos limites de exposição a riscos que a PR está disposta a aceitar.

O Guia da CGU declara que "**o estabelecimento desses limites, que pode ser tratado em termos de apetite a risco ou tolerância ao risco, é necessário para que seja realizada a etapa de avaliação de riscos e sejam definidas as medidas de tratamento de riscos**." (CGU, 2018).

Diante da particularidade de cada casa palaciana, na Presidência da República, cabe aos Comitês internos dos seus órgãos a definição dos níveis de apetite a risco dos seus processos organizacionais.

D. INSTRUMENTO PARA REGISTRO DO PROCESSO

A CGU orienta que "**todo o modelo para a gestão de riscos de um processo organizacional precisa ser registrado. A partir da implementação da gestão de riscos, a ocorrência de eventos não desejáveis deve ser devidamente justificada à luz dos registros realizados**" (CGU, 2018).

Isso posto, a implementação e execução do processo de gestão de riscos da PR será realizada por meio de ferramenta institucional a ser definida no âmbito do Cigov/PR.

Até a definição da ferramenta mencionada no parágrafo anterior, as áreas poderão se utilizar de outros meios hábeis para o cumprimento do disposto nesta metodologia.

V. GESTÃO DE RISCOS: TEORIA E PRÁTICA

Conforme a norma ABNT ISO 31000:2018, o **processo de gestão de riscos** envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de: (i) estabelecimento do contexto no qual a gestão de riscos será executada; (ii) avaliação dos riscos, que compreende a identificação, a análise e a avaliação dos mesmos; (iii) tratamento dos riscos; (iv) monitoramento de riscos e controles; e (v) comunicação sobre riscos com as partes interessadas, internas e externas, conforme apresentado na figura a seguir:

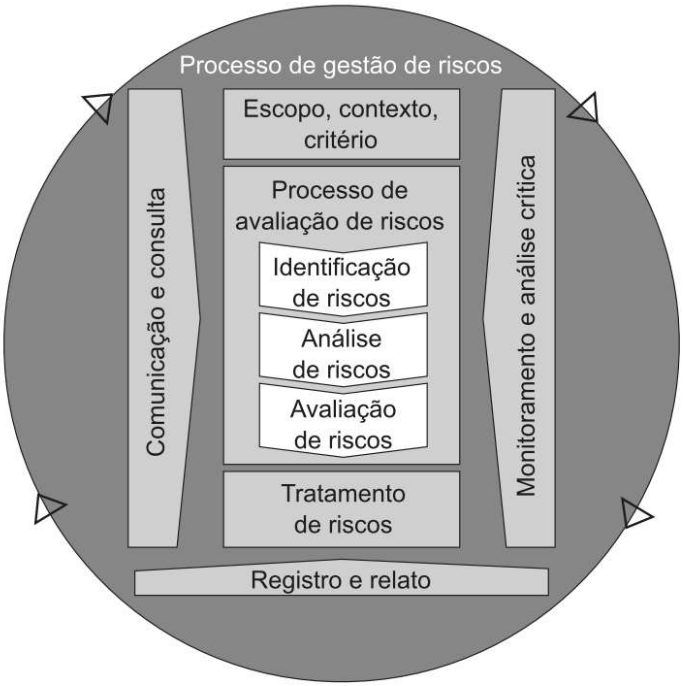

Figura 2 – Processo de Gestão de Riscos.

Esse processo deve ser parte integrante da gestão e da tomada de decisão, incorporado na estrutura, operações e processos da organização, e aplicado nos níveis estratégicos, táticos e operacionais.

Sendo assim, considerando essa norma e as diretrizes estabelecidas pela PGR/PR, a metodologia de gestão de riscos da PR é constituída de cinco etapas:

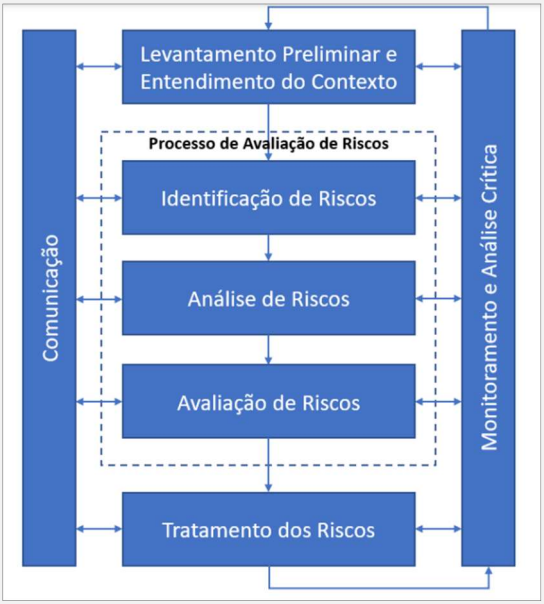

Figura 3 – Processo de Gestão de Riscos da PR.

A. **Estabelecimento do contexto** – que envolve a definição do escopo, a análise dos contextos externo e interno, e a definição dos critérios de risco;
B. **Processo de avaliação de riscos** – que compreende a identificação, a análise e a avaliação dos riscos;
C. **Tratamento dos riscos** – que envolve a seleção de opções de tratamento dos riscos e a preparação do plano de tratamento dos riscos;
D. **Monitoramento de riscos** - que envolve o acompanhamento e a verificação do desempenho ou da situação dos elementos da gestão de riscos; e
E. **Comunicação de riscos** - que compreende a identificação das partes interessadas e o compartilhamento de informações relacionadas à gestão de riscos entre essas partes.

Cabe ressaltar que, conforme diretriz da PGR/PR, art. 4º, inciso II, o processo de gestão de riscos deve ser aplicado a cada processo de trabalho que compõe a cadeia de valor da organização.

Para tanto, para a aplicação desta metodologia convém que os macroprocessos/processos das unidades estejam claramente definidos e priorizados pelos Comitês Internos de Governança de cada órgão da PR, considerando aspectos como orçamento envolvido, criticidade, etc.

Este capítulo, portanto, apresenta as etapas para a execução do **processo de gestão de riscos da PR**, desde o estabelecimento do contexto, que inclui a seleção do processo de trabalho, até o monitoramento e a comunicação de riscos.

A. ETAPA 1 – ESTABELECIMENTO DO CONTEXTO

O propósito desta etapa é **personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado**. Nesta etapa ocorre a definição do escopo do processo, a compreensão dos contextos externo e interno e a definição e critérios para a gestão dos riscos. (ABNT, 2018).

O estabelecimento de um contexto para a gestão de riscos envolve o entendimento da organização, dos seus objetivos, do ambiente interno e do controle interno, com o fim de obter uma visão dos fatores que podem influenciar a capacidade da organização para atingir sua missão institucional, bem como fornecer parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas.

O TCU orienta, em seu Manual de Gestão de Riscos, que

> *o estabelecimento do contexto deve seguir os seguintes passos:*
>
> - *identificar quais objetivos ou resultados devem ser alcançados;*
> - *identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;*
> - *identificar as pessoas envolvidas nesses processos e especialistas na área;*
> - *mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.);*
> - *definir os objetos de gestão de risco mais importantes para a sua unidade ou trabalho;*
> - *definir os objetivos/resultados de cada objeto. (TCU, 2018)*

A.1. Definição do escopo

De acordo com a norma ABNT ISO 31000:2018, a gestão de riscos ocorre no contexto dos objetivos da organização e devem estar alinhados ao planejamento estratégico e à cadeia de valor do órgão. A estratégia de

uma instituição, normalmente representada por meio de mapas estratégicos, contém a missão, a visão e os valores do órgão, o conjunto dos objetivos estratégicos assumidos, os indicadores e as metas vinculadas a esses objetivos.

O guia **Dez passos para a boa governança**, do TCU, indica como uma boa prática que a Alta Administração "**assegure que o processo de gestão de riscos seja incorporado aos demais processos organizacionais, a começar do planejamento estratégico, de forma a subsidiar a tomada de decisão e garantir o alcance dos objetivos**" (TCU,2021).

O Guia de Gestão Estratégica do Ministério da Economia, por sua vez, orienta a construção de um conjunto de projetos, programas e processos, denominado portfólio estratégico, para o alcance dos objetivos estratégicos da organização (ME, 2020). É, portanto sobre o planejamento estratégico, os objetivos, processos e projetos planejados que, normalmente, se desenvolve a gestão de riscos.

Sendo assim, para a execução do processo de gestão de riscos da PR, devem ser mapeados os processos, projetos e iniciativas que tenham relevância para o atingimento dos resultados planejados.

É importante que a organização tenha clareza sobre o escopo em consideração para a gestão de riscos e sobre os objetivos pertinentes a serem considerados, e o seu alinhamento aos objetivos organizacionais.

Deve-se observar, entretanto, que,

> *ainda que a gestão de riscos deva ser parte integrante de todos os processos organizacionais (princípio previsto pela ABNT ISO 31000:2018), ela não deve ser aplicada a todos os seus processos com a mesma intensidade, visto que os recursos da organização são limitados. Naturalmente o investimento na gestão de riscos deve ser maior nos processos que mais entregam ou devem entregar valor para as partes interessadas, bem como nas atividades de suporte que podem estar limitando a capacidade de entrega dos processos finalísticos. (TCU,2018)*

Portanto, quando se define a gestão de riscos em uma organização, a **priorização de processos organizacionais é importante para orientar a alocação de recursos para a gestão de riscos**, bem como quando se planeja uma estratégia gradual de implantação dessa abordagem (TCU, 2018).

Nesse ponto, a Cadeia de Valor é uma ferramenta que representa graficamente os principais macroprocessos do órgão, finalísticos e de suporte, que impulsionam suas ações para a realização do planejamento estratégico e para a entrega de valor à sociedade.

Assim é recomendável que a Cadeia de Valor ou os macroprocessos das unidades sejam conhecidos e priorizados, permitindo a definição de um escopo a partir do qual a gestão de riscos seja executada de forma gradual e bem-sucedida.

Ressalta-se que é recomendado que os processos organizacionais priorizados estejam minimamente documentados e alinhados à Política de Governança de Processos da PR, de forma a permitir a aplicação da metodologia. Portanto, sugere-se que possuam pelo menos as seguintes informações:

- **Diagrama do processo modelado** em notação BPMN (***Business Process Model and Notation***) – seguindo o padrão de documentação de processos estabelecidos na Metodologia de Gestão de Processos da PR - que contemple as principais etapas, atividades, produtos e atores envolvidos;
- **Objetivos gerais e específicos representados na descrição do processo** e nos elementos do diagrama – declaração de objetivos que permite a identificação vinculada dos riscos;
- **Responsável** – área da organização e dirigente na qual encontra-se a competência principal para a realização do processo em questão;
- **Periodicidade** - quantas vezes o processo é realizado e a sua média de duração em horas, dias, semanas etc.

A.2. Análise dos contextos externo e interno

A análise de contexto do processo de gestão de riscos, segundo a ABNT ISO 31000:2018, deve ser estabelecida a partir da compreensão dos ambientes externo e interno nos quais a organização opera. O **Committee of Sponsoring Organizations of the Treadway Commission** (COSO) descreve a análise do ambiente como sendo a base para todos os outros componentes da gestão de riscos, a qual *"compreende muitos elementos, inclusive os valores éticos da organização, a competência e o desenvolvimento de pessoal, a filosofia da administração para a gestão de riscos, e como são atribuídas alçada e responsabilidade".*

Em outras palavras, deve-se estabelecer o contexto para que possa entender o ambiente em que seu processo de gerenciamento de risco opera.

O exame do **contexto externo** da organização inclui os impactos que os fatores externos podem ter nas operações da organização e na sua capacidade de atingir os objetivos estratégicos.

O exame do **contexto interno** envolve, entre outras coisas, os objetivos, estrutura, capacidades, processos, recursos e partes interessadas.

Ressalta-se que os contextos externo e interno devem ser examinados regularmente, quando a estrutura e os processos de gerenciamento de riscos são revisados, para garantir que quaisquer alterações sejam identificadas em tempo hábil e que os tratamentos e prioridades para a resposta aos riscos possam ser revisados, se necessário.

Sugere-se que essa análise seja realizada por meio da ferramenta denominada ***Análise SWOT***, onde se coleta e registra as informações relacionadas aos cenários externos e internos, a serem levados em consideração, sobre o ambiente específico da atividade ao qual o processo de gestão de riscos é aplicado, bem como sobre a própria política de gestão de riscos.

O acrônimo **SWOT** é uma sigla em inglês dos termos **Strengths** (pontos fortes), **Weaknesses** (pontos fracos), **Opportunities** (oportunidades) e **Threats** (ameaças). Em cada quadrante da matriz são registradas a sua

relação com o objeto analisado. Os quadrantes representados na figura a seguir orientam as questões a serem observadas:

Figura 4 – Análise de SWOT.

Para auxiliar esta etapa, o TCU propõe o seguinte quadro, que pode ser utilizada como modelo:

Quadro 1 - Descrição do Contexto da Unidade/Diretoria/Serviço/Processo/Atividade (etc.)

CONTEXTO INTERNO:	CONTEXTO EXTERNO
Principais resultados:	Principais stakeholders e seus interesses:
Processos de trabalho relevantes:	Recursos externos:
Pessoas chave:	Relevância dos resultados/entregas:
Fatores que afetam os resultados:	Relevância dos resultados/entregas para a sociedade:
Recursos tecnológicos:	Setores ou entidades parceiros:
(...)	(...)

A.3. Definição de critérios de risco

A ABNT ISO 31000:2018 orienta que, para a aplicação do processo de gestão de riscos, a **organização especifique a quantidade e o tipo de risco que pode ou não assumir em relação aos objetivos** e que **estabeleça critérios para avaliar a significância do risco,** para apoiar os processos de tomada de decisão.

Um conjunto de critérios de risco padrão é necessário para que todos na organização tenham um entendimento comum de como avaliar a importância de um risco.

Os critérios de risco **devem refletir os valores, objetivos e recursos da organização e devem ser consistentes com as políticas e declarações sobre gestão de riscos. Devem, ainda, ser estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas (ABNT, 2018).**

Podem representar requisitos regulamentares ou legais; níveis mínimos de serviço, ou padrões estabelecidos pela organização. Uma vez desenvolvidos, os critérios de risco devem ser documentados e comunicados às partes interessadas.

É recomendado que os critérios de risco considerem:

- a natureza e o tipo de incertezas que podem afetar resultados e objetivos (tanto tangíveis quanto intangíveis);
- como as consequências (tanto positivas quanto negativas) e as probabilidades serão definidas e medidas;
- fatores relacionados ao tempo;
- consistência no uso de medidas;
- como o nível de risco será determinado;
- como as combinações e sequências de múltiplos riscos serão levadas em consideração;
- a capacidade da organização. (ABNT, 2018)

Sendo assim, o portfólio de processos e projetos, mapeados na etapa de definição do escopo, deve ser priorizado por esse conjunto de critérios de risco estabelecidos pelo Comitê Interno de Governança de cada órgão da PR, observando esta metodologia.

B. ETAPA 2 – PROCESSO DE AVALIAÇÃO DE RISCOS

B.1. IDENTIFICAÇÃO DE RISCOS

De acordo com a norma ABNT ISO 31000:2018, o propósito da ***identificação de riscos*** é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos.

A finalidade da **identificação de risco é gerar uma lista abrangente de riscos baseada em eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos** (CGU, 2018). Portanto, os riscos inerentes a cada atividade da organização, em seus diferentes níveis, devem ser identificados e relacionados (CGU/MP, 2016).

Nesta etapa, fatores como fontes de risco, causa e eventos, ameaças, vulnerabilidades, mudanças de contextos, natureza e valor dos ativos e recursos, fatores temporais, consequências potenciais, dentre outros, devem ser considerados (ABNT, 2018).

Vários métodos podem ser usados para identificar riscos, incluindo:

- listas de verificação (listas de perigos, riscos e falhas de controle, com base na experiência, como avaliações de risco anteriores ou falhas anteriores);
- questionários de autoavaliação;
- métodos baseados em evidências, como revisões de dados históricos;
- abordagens sistemáticas baseadas em equipe envolvendo especialistas;
- auditorias ou inspeções físicas.

Ressalta-se que, para gerenciar o risco de forma eficaz na organização, os principais interessados devem ter conhecimento completo da gama de riscos que a organização enfrenta. Uma alternativa para esta etapa, segundo o TCU, é a utilização da técnica de **brainstorming** (tempestade de ideias), que permite a coleta e registro de um maior número de riscos (TCU, 2020).

Independentemente da técnica selecionada, a identificação de riscos deve ser parte integrante dos processos estratégicos, operacionais, e de planejamento.

A gestão de riscos deve fazer parte do dia a dia do órgão, e as partes interessadas devem ser envolvidas. Todos os riscos devem estar vinculados aos objetivos da organização, que devem ter sido identificados quando o contexto foi estabelecido.

A identificação de riscos deve ser um processo contínuo para capturar novos riscos à medida que surgirem, e também confirmar a validade

contínua dos riscos previamente identificados.

Após a identificação e registro dos riscos, deverão ser apontadas todas as suas causas e consequências significativas, associadas a determinado evento, conforme descrito a seguir.

B.1.1. Passo a Passo - Identificação de Riscos (figura 5):

a. Descreva o **Evento de Risco;**
b. Aponte, no campo **Causas**, todos os motivos para a possibilidade de ocorrência do risco;
c. Descreva as **Consequências**, ou seja, todos os efeitos negativos gerados pela ocorrência do risco, destacando se os objetivos estratégicos serão afetados;
d. Quanto a **Categoria do Risco**, classifique o risco de acordo com a tipologia de riscos apresentada no item B.1.2, a seguir.

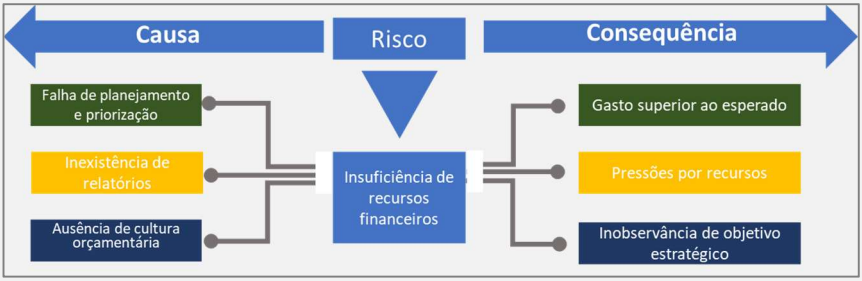

Figura 5 – Exemplo – Identificação de riscos.

***Obs:** Os riscos geralmente têm mais de uma causa, e pode ser necessário avaliar se o risco é melhor descrito e analisado ao ser combinado ou identificado separadamente.*

B.1.2. Tipologias de riscos:

Uma vez que os riscos são identificados, as organizações geralmente os classificam em categorias. Seguindo as orientações da Instrução Normativa Conjunta CGU/MP nº 1/2016, art. 18, a PR definiu que ao menos as seguintes tipologias de riscos que devem ser consideradas pelos órgãos da PR, no mapeamento dos seus riscos:

a. **riscos operacionais**: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiências ou inadequações de processos internos, pessoas, infraestrutura e sistemas;
b. **riscos de imagem/reputação do órgão**: eventos que podem comprometer a confiança da sociedade em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;
c. **riscos legais**: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;
d. **riscos financeiros/orçamentários**: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades;
e. **riscos de integridade:** eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela organização e a realização de seus objetivos.

Não obstante, conforme as especificidades de cada unidade da PR, essa metodologia permite a criação de subcategorias que melhor atendam suas necessidades. Desta forma pode-se, por exemplo, entre os riscos operacionais decidir-se por diferenciar aqueles relacionados a eventos cibernéticos; daqueles relativos à governança da unidade; bem como dos riscos operacionais associados a conformidade dos processos de trabalho.

Para o registro dos riscos identificados recomenda-se o uso de *template,* que contenha, ao menos, as informações apresentadas a seguir:

PRESIDÊNCIA DA REPÚBLICA

Responsável (eis) pela An
Período da Análise:

Mapeamento de Risco				
Dimensão/Processo	Identificação dos Riscos			
	Causas	Risco	Tipologia	Consequências

Figura 6 – Identificação dos Riscos.

B.2. ANÁLISE DE RISCOS

O propósito da ***Análise de riscos***, segundo definição da norma ABNT ISO 31000:2018, "***é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia".*** Ela fornece a base para a avaliação de riscos, bem como para a estratégia e as decisões quanto ao tratamento dos riscos (ABNT, 2018).

Nesta etapa, os riscos são analisados considerando a probabilidade de ocorrência e o seu impacto sobre os objetivos da organização. A combinação desses dois fatores (probabilidade x impacto) determina o **nível do risco**.

As figuras a seguir demonstram as escalas de Probabilidade e Impacto, a serem consideradas no momento da análise do risco.

Escala de Probabilidade:

A **probabilidade** é a chance de o evento ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado (TCU, 2020). Para sua mensuração, deve-se utilizar a escala qualitativa a seguir:

Probabilidade					
Aspectos Avaliativos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento **pode** ocorrer em algum momento	Evento **deve** ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias
Frequência Observada/Esperada	Muito baixa (< 10%)	Baixa (>=10% <= 30%)	Média (>30% <= 50%)	Alta (>50% <= 90%)	Muito alta (>90%)
Peso	1	2	3	4	5

Figura 7 – Escala de probabilidade.

a. **Muito baixa**: evento pode **ocorrer apenas** em circunstâncias excepcionais;
b. **Baixa**: evento **pode** ocorrer em algum momento;
c. **Média:** evento **deve** ocorrer em algum momento;
d. **Alta:** evento **provavelmente** ocorra na maioria das circunstâncias;
e. **Muito alta:** evento **esperado** que ocorra na maioria das circunstâncias.

Escala de Impacto:

O **impacto** mede o potencial comprometimento do objetivo/resultado (TCU, 2020). Assim como a probabilidade, sua mensuração é realizada por meio de uma escala qualitativa, conforme figura a seguir:

Impacto - Fatores para Análise						
Orientações para atribuição de pesos	Intervenção Hierárquica	Correição e Punição	Reputação	Negócios /Serviços	Articulação (Repercusão) Política	Peso
	20%	20%	20%	20%	20%	100%
	Exigiria a intervenção do Ministro	Há desdobramento de âmbito correicional, sendo aberto procedimento que acarretará a demissão de servidores e determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudia o alcance da missão institucional	Exigiria um enorme esforço de Articulação Política. Perda relevante de Apoio político	5-Muito alto
	Exigiria a intervenção do Secretário	Há desdobramento de âmbito correicional, sendo aberto procedimento que determine ações de caráter pucuniário (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance dos objetivos estratégicos	Exigiria um grande esforço de Articulação Política. Perda de apoio político	4-Alto
	Exigiria a intervenção do Diretor	Há desdobramento de âmbito correicional, sendo aberto procedimento que determine ações de caráter corretivo	Pode chegar à mídia provocando a exposição sem repercussão relevante	Prejudica o alcance dos objetivos da unidade	Exigiria um médio esforço de Articulação Política. Possibilidade de perda de apoio político.	3-Moderado
	Exigiria a intervenção do Coordenador	Algum desdobramento de âmbito correicional, podendo ser aberto procedimento que determine ações de caráter orientativo	Tende a limitar-se no máximo à Secretaria/Unidade do órgão	Prejudica o alcance das metas do processo	Exigiria um pequeno esforço de Articulação Política.	2-Baixo
	Seria alcançada no funcionamento normal da atividade	Pouco ou nenhum desdobramento de âmbito correicional	Impacto apenas interno (servidores envolvidos) / sem impacto	Pouco ou nenhum impacto nas metas do processo	Não haverá necessidade de esforço de Articulação Política.	1-Muito baixo

Figura 8 – Escala de impacto

Obs : *Observe as "**Orientações para a atribuição de pesos**" para identificar qual o peso que melhor se adequa a cada dimensão avaliada.*

Nível do Risco (NR):

O **nível do risco** é a magnitude de um risco expressa em termos da combinação das consequências e de suas probabilidades (ABNT, 2009).

Seu cálculo é realizado de acordo com a matriz de calor apresentada na figura a seguir:

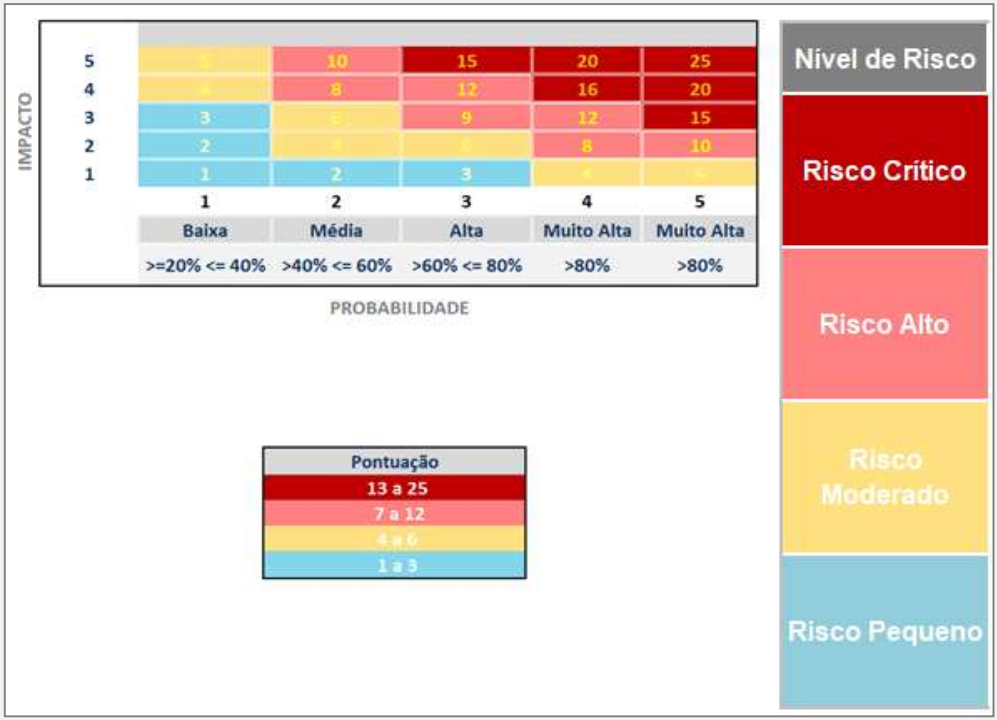

Figura 9 – Matriz de Calor por níveis de risco.

Obs: *Observe que a matriz ordena os* ***níveis de riscos do 1 ao 25****, calculado pela multiplicação dos valores considerados nas escalas anteriores (probabilidade X impacto), separando sua criticidade por cores.*

Destaca-se que o cálculo do nível do risco é realizado em **três subetapas**, analisando os riscos em dois cenários distintos: o **cálculo do nível do risco inerente**, onde não são considerados os mecanismos de controle implementados para reduzir a probabilidade de ocorrência do risco ou seus impactos; a **avaliação dos controles** existentes; e o **cálculo do nível do risco residual**, o qual considera o risco após a avaliação dos mecanismos de controle já implementados para reduzir sua ocorrência ou impactos.

B.2.1. Cálculo do risco inerente

Nesse momento, o exercício é analisar cada risco desconsiderando os controles pré-existentes. De acordo com a CGU, a diferença entre o valor do risco inerente e o risco residual demonstra a atual eficácia dos controles implementados na mitigação dos riscos identificados (CGU, 2018).

Utilizando as escalas demonstradas anteriormente, multiplica-se os valores de probabilidade e impacto encontrados, determinando o nível do risco inerente, conforme demonstrado a seguir:

NRI = NP x NI

onde

NRI = nível do risco inerente
NP = nível de probabilidade do risco
NI = nível de impacto do risco

Processo / Dimensão	Riscos	Probabilidade - Frequência Observada/Esperada					Impacto - Fatores de Análise						Nível de Risco Calculado (volte para a aba "Mapa de Riscos" e informe o "Descrição do Controle Atual"	
		Aspectos Avaliativos												
		Evento pode ocorrer apenas em circunstâncias excepcionais	Evento **pode** ocorrer em algum momento	Evento **deve** ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias	Intervenção Hierárquica	Correção e Punição	Revisão	Negócios e Serviços	Articulação (Repercussão) Política		Probabilidade x Impacto	Descrição
		<=20%	>20% <=40%	>40% <=60%	>60% <=80%	>80%	PESOS							
		1 Muito baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta	20%	20%	20%	20%	20%			
xx	xx			4			4	1	2	2	1	3	12	Risco Alto
xx	xx			5			4	2	4	4	4	4	20	Risco Crítico
xx	xx			5			5	4	4	4	4	4	20	Risco Crítico
xx	xx			5			4	3	5	5	4	4	20	Risco Crítico
xx	xx			5			4	3	3	3	1	3	15	Risco Crítico
xx	xx			5			3	1	2	2	1	2	10	Risco Alto
xx	xx			5			2	1	1	1	1	1	5	Risco Moderado
xx	xx			5			2	1	1	1	1	1	5	Risco Moderado
0	0						0	0	0	0	0	0	0	Risco Pequeno
0	0						0	0	0	0	0	0	0	Risco Pequeno
0							0	0	0	0	0	0	0	Risco Pequeno

Figura 10 – Matriz de cálculo de nível do risco inerente.

B.2.2. Avaliação dos controles existentes

De acordo com a Decreto nº 9.203/2017, art. 5º, inciso III, controle compreende processos estruturados para mitigar os possíveis riscos, com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos.

Portanto, dando sequência à análise do risco, o exercício agora é avaliar os controles existentes de acordo com os critérios demonstrados a seguir:

Avaliação dos controles existentes	
Avaliação	**Descrição da Avaliação**
(1) Inexistente	Controles existentes, mal desenhados ou mal implementados, isto é, não funcionais.
(2) 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.
(3) 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.
(4) Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
(5) Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.

Figura 11 – Critérios para avaliação dos controles.

B.2.3. Cálculo do risco residual

Considerando que o risco residual é o nível do risco remanescente após a aplicação de controles para reduzi-lo, um fator redutor foi atribuído a cada critério de avaliação dos controles existentes, conforme a tabela abaixo:

Tabela 1 – Critérios para avaliação dos controles

Avaliação dos Controles	Fator
(1) Inexistente	1
(2) Fraco	0,8
(3) Mediano	0,6
(4) Satisfatório	0,4
(5) Forte	0,2

Por conseguinte, o cálculo do risco residual é realizado automaticamente baseado na seguinte fórmula:

NRR = NRI x FR *onde*

NRR = nível do risco residual
NRI = nível do risco inerente
FR = Fator redutor do controle

Observe o modelo a seguir, o qual exemplifica o cálculo do risco residual:

PRESIDÊNCIA DA REPÚBLICA

Responsável (eis) pela Análise:
Período da Análise:

Mapeamento de Risco

Dimensão/ Processo	Avaliação dos Riscos								
	Risco	Risco Inerente		Identificação dos Controles Existentes (informe abaixo a "Descrição do Controle Atual")		Risco Residual		
		NRI	NR	Descrição do Controle Atual	Avaliação quanto a Operação do Controle	Fator	NRR	NR
0	0	8	Risco Alto	O controle atual consiste em...	(3) Mediano	0,6	4,8	Risco Moderado

Figura 12 – Exemplo cálculo do risco residual.

B.3 – AVALIAÇÃO DE RISCOS

A norma ABNT ISO 31000:2018 define a **avaliação de riscos** como **o processo de comparar os resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional**. O seu propósito é apoiar decisões (ABNT, 2018).

Nesse sentido, para que não haja desperdício de esforços, a CGU orienta que os riscos a serem inicialmente gerenciados precisam ser os mais

relevantes para a organização, isto é, os de maior impacto e probabilidade dentro de um limite previamente definido pela alta direção. Após realizada a avaliação de riscos, o órgão ou entidade pode estabelecer uma ordem de prioridade para o tratamento de riscos, de acordo com seu **apetite a risco**. (CGU, 2018).

Ressalta-se que **apetite a risco é o nível de risco que uma organização está disposta a aceitar** (MP/CGU, 2016). É importante que o apetite a risco do processo organizacional seja estabelecido no início do processo (CGU,2018). Portanto, é desejável que o nível do risco fique dentro dos limites desejáveis. O mapa de calor abaixo, exemplifica a faixa fora do limite de exposição (em amarelo), ou seja, fora do apetite ao risco estabelecido pela organização, onde é recomendável que seja aplicado o tratamento do risco:

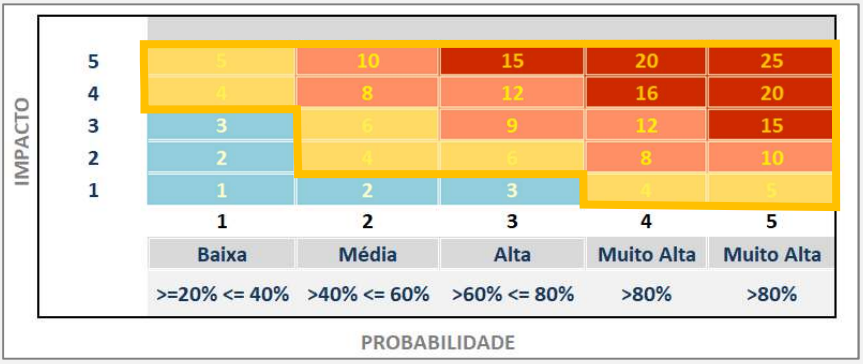

Figura 13 – Exemplo de faixa fora do limite de exposição a riscos.

***OBS:** Cabe lembrar que, conforme mencionado no item IV.C, cabe aos Comitês internos de cada órgão palaciano a definição dos níveis de apetite a risco dos seus processos organizacionais.*

C. ETAPA 3 – TRATAMENTO DOS RISCOS

De acordo com a norma ABNT ISO GUIA 73:2009, **tratamento de riscos** é o processo para **modificar o risco**. É nesta fase que serão definidas as respostas aos riscos identificados, analisados e avaliados.

Nesta etapa também são planejadas as medidas de tratamento do risco com o intuito de reduzir o seu impacto e a sua probabilidade de ocorrência.

A norma ABNT ISO 31000:2018 aborda as seguintes opções para tratar o risco:

- **evitar o risco** ao decidir não iniciar ou não continuar com a atividade que dá origem ao risco;
- **assumir ou aumentar o risco** de maneira a perseguir uma oportunidade;
- **remover a fonte de risco**;
- **mudar a probabilidade**;
- **mudar as consequências**;
- **compartilhar o risco** (por exemplo, por meio de contratos, compra de seguros);
- **reter o risco** por decisão fundamentada.

A PR, portanto, estabeleceu quatro possíveis respostas aos riscos, conforme figura 14, apresentada a seguir

Figura 14 – Possíveis respostas aos riscos.

Ressalta-se que, conforme orientação da CGU,

> *quando se trata de riscos, a perspectiva não deve ser a de garantir sua eliminação, pois se está lidando com a incerteza. Portanto, na maioria das vezes,* ***serão tomadas ações para minimizar ou mitigar o risco, por meio de medidas que visam reduzir o impacto e/ou probabilidade do risco, resultando em níveis aceitáveis***

> ***do risco**, compatível com o que a organização possa lidar sem maiores danos (CGU, 2018).*

Diante disso, após selecionar a resposta adequada à realidade da organização, uma série de medidas de tratamento do risco (mecanismos de controle) deverão ser elencadas, considerando sua viabilidade, custo, esforço, benefícios, tempestividade, consequências e etc.

Sobre o assunto, a CGU destaca ainda que,

> *os mecanismos de controle devem ser concebidos e implementados para assegurar que as respostas aos riscos sejam executadas de forma apropriada e tempestiva. **É fundamental dimensionar os controles às reais necessidades da organização,** tendo em vista que a implantação de controles para riscos de baixo impacto e baixa probabilidade de ocorrência pode tornar a administração pública desnecessariamente burocrática e lenta. **Os controles internos devem auxiliar, e não impedir, a realização dos objetivos da organização**. (CGU,2017)*

As opções de tratamento escolhidas devem integrar um **plano de tratamento de riscos,** onde constarão informações claras e relevantes, das ações propostas e de como serão implementadas as medidas de mitigação do risco, para que seja compreensível para todos os envolvidos e para que sua execução seja monitorável.

Esse plano deve definir a ordem de prioridade para a implementação de cada ação de tratamento, bem como identificar: (a) o tipo e o objetivo da ação; (b) os responsáveis pela implementação; (c) como as ações serão implementadas, os recursos requeridos; (d) as restrições; e (e) o cronograma.

Ressalta-se que o processo de tratamento é cíclico e também pode introduzir novos riscos que precisem ser gerenciados. Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos, para assegurar que as diferentes formas de tratamento se tornem e permaneçam eficazes (ABNT, 2018).

O modelo a seguir apresenta um exemplo de **plano de tratamento de riscos**, conforme mencionado anteriormente:

				O que?			Onde?	Quem?	Como?		Quando?		
				Controle Proposto / Ação Proposta									
Processo/Dimensão	Risco	Nível de Risco Residual	Resposta a Risco	Descrição	Tipo	Objetivo	Área Responsável pela Implementação	Responsável Implementação	Como será Implementado	Intervenientes	Previsão de implementação	Status	
		Risco Moderado	Reduzir		Preventiva							Não iniciado	

Figura 15 – Exemplo de Plano de tratamento de riscos.

LEGENDA

- ✓ Processo/dimensão: Definido conforme item "A.1. Definição do escopo"
- ✓ Risco: Identificados conforme item "B1 – Identificação de Riscos".
- ✓ Nível de Risco Residual: Nível de Risco Inerente x Fator Redutor do Controle (conforme tabela 1).
- ✓ Resposta ao Risco: Evitar, Reduzir, Compartilhar ou Aceitar (conforme Figura 14).
- ✓ Descrição: Detalhamento da ação/controle de resposta ao risco.
- ✓ Tipo: Seleção do tipo do controle que pode ser "Preventivo" ou "Corretivo" (conforme item C.2)
- ✓ Objetivo: Escolher entre as opções "Melhorar controle existente" ou "Adotar controle novo"
- ✓ Área Responsável e Responsável implementação: Definição dos responsáveis pelo controle.
- ✓ Como será implementado: Definição da forma de execução da ação.
- ✓ Intervenientes: Definição do que pode dificultar a ação;
- ✓ Previsão de implementação: Definição dos prazos para a implantação do controle.
- ✓ Status: Escolher entre as opções "Não iniciado", "Em andamento", "Concluído" ou "Atrasado".

C.1. Passo a Passo - Seleção de opções de tratamento dos riscos

a. Para descrever a **Resposta a Risco**, selecione um risco da listagem de Eventos de Risco identificados e determine a resposta ao risco, adequada ao nível do risco residual e o apetite ao risco definido pelo Cigov/PR, conforme as opções apresentadas na figura 14.

C.2. Passo a Passo – Plano de tratamento de riscos

a. Para criar o **Plano de tratamento de riscos**, selecione um risco da listagem de Eventos de Risco e preencha o "Plano de Ação" com os controles propostos, para o seu tratamento, conforme figura 15.

Obs.: Os tipos de controles serão classificados em:
- **Preventivos**: quando tem a função de evitar que o evento de risco ocorra (atuam nas **causas** do risco); ou
- **Corretivos**: quando tem a função de mitigar as consequências advindas da materialização do evento de risco (atuam nas **consequências** do risco).

D. ETAPA 4 – MONITORAMENTO E ANÁLISE CRÍTICA

A etapa de monitoramento de riscos é essencial para a eficácia da gestão de riscos. Isso porque, segundo explica o COSO, o gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo. As respostas a risco que se mostravam eficazes anteriormente podem tornar-se inócuas; as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou os objetivos podem mudar (COSO, 2007).

A finalidade desta etapa, de acordo com a ABNT ISO 31000:2018, é **assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo** (ABNT,2018). O TCU, por sua vez, destaca que esta etapa tem como objetivos:

> (a) ***detectar mudanças no contexto externo e interno***, *incluindo alterações nos critérios de risco e no*

> *próprio risco, **que podem requerer revisão dos tratamentos de riscos e suas prioridades**, assim como identificar riscos emergentes;*
> *(b) obter informações adicionais para **melhorar a política, a estrutura e o processo de gestão de riscos**;*
> *(c) **analisar eventos** (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos **e aprender com eles**; e*
> *(d) **assegurar que os controles sejam eficazes** e eficientes no projeto e na operação. (TCU, 2018 apud ABNT, 2009 – grifo nosso)*

Adicionalmente, a IN MP/CGU nº 1/2016, no art. 16, inciso VIII, refere-se ao monitoramento como a etapa onde **avaliamos a qualidade do processo de gestão de riscos e dos controles internos da gestão, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente**, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.

Para tanto, é necessário que o monitoramento e a análise crítica sejam executados de forma contínua e em todas as etapas do processo de gestão de riscos, de forma a aprimorar e aumentar o seu desempenho, levando a instituição a um nível mais alto de maturidade na gestão de riscos.

Isto posto, a seguir estão detalhadas as atividades que contemplam esta etapa.

D.1. Monitoramento contínuo

Atividade frequente, **de responsabilidade dos gestores de primeira e segunda linha**, de acompanhamento e supervisão, contínua e periódica, da implementação e do desempenho da gestão de riscos, bem como dos resultados das ações mitigadoras, assegurando que os riscos sejam mantidos nos níveis aceitáveis e que os controles permaneçam eficazes.

Os **indicadores-chave de desempenho da gestão de riscos (IDR)** e os **indicadores-chave de riscos (ICR)**, constituem ferramentas para o apoio desta atividade, conforme apresentado na figura 16.

Entende-se por **indicadores-chave de desempenho da gestão de riscos** como os **números, percentagens ou razões estabelecidas, para monitorar as variações no desempenho em relação à meta para o cumprimento de objetivos estratégicos e operacionais relevantes para o negócio** (TCU, 2018).

Esses indicadores são importantes porque servem de subsídio à tomada de decisão, tanto dos gestores de primeira e segunda linha, quanto das instâncias responsáveis pela governança dos riscos (os Comitês Internos de Governança dos órgãos da PR e o Cigov/PR).

Nesse sentido, é importante que os órgãos da PR, apoiados por suas unidades de governança, avaliem seus IDRs, com base em seus processos de trabalho onde é realizada a gestão de riscos, buscando informações sob quatro perspectivas:

i. **implementação:** dedicados a monitorar a situação da implantação dos controles;
ii. **eficiência:** dedicados a monitorar a viabilidade do controle quanto aos prazos, custo, escopo e planejamento;
iii. **eficácia:** dedicados a monitorar se o controle implementado cumpre o propósito determinado, ou seja, se os resultados esperados estão sendo alcançados
iv. **efetividade:** são, na verdade, indicadores do próprio objetivo. Visam monitorar o impacto da gestão de riscos sobre o objetivo organizacional.

Ressalta-se que, durante essa atividade os gestores **devem assegurar que o registro do risco esteja sempre atualizado, bem como que os resultados das ações mitigadoras mais recentes sejam documentados (TCU,2018).**

É importante destacar que alguns indicadores devem ser comuns às unidades da Presidência da República, sendo recomendados pela DGO,

mediante aprovação do CIGOV, onde serão considerados aspectos como: o estágio da implantação da política de gestão de riscos no órgão; a periodicidade da avaliação dos riscos pelo Comitê Interno de Governança; a maturidade do processo gestão de riscos no órgão, dentre outros.

Adicionalmente, **os gestores de primeira linha** podem dispor dos **indicadores-chave de risco (ICR)** que são métricas que podem ser usadas para detectar possíveis mudanças nos riscos de uma organização. Em geral, os ICRs usam dados e informações, correlacionados com fatores de risco específicos ou estratégias de mitigação, para fornecer **visões prospectivas sobre tendências de risco**; ou podem funcionar como sinais de alerta precoce em relação à materialização de riscos monitorados.

Os ICRs fornecem informações em tempo hábil acerca de eventos ou condições que podem desencadear riscos. Eles se diferenciam dos indicadores de desempenho, pois se antecipam à materialização dos riscos, enquanto os indicadores de desempenho focam em riscos que já ocorreram para fornecer uma visão sobre o desempenho alcançado (BASLEY et al., 2010 apud TCU, 2020).

Em resumo, os ICRs podem ajudar a organização a gerenciar os riscos críticos e a identificar riscos emergentes, adotando ações proativas (BASLEY et al., 2010, apud TCU, 2020).

Na figura 16 abaixo estão apresentados exemplos de IDR e ICR:

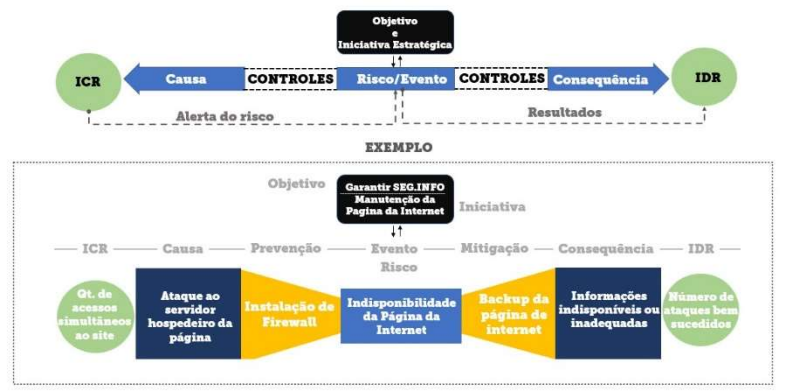

Figura 16 – Exemplo de ICR e IDR.

D.2. Análise crítica

Atividade de avaliação e registro dos resultados do monitoramento. Incluem análises, comparações de informações, ocorrências imprevistas e inconsistências que determinem medidas corretivas ou outras (COSO, 2007). Esta atividade é de responsabilidade dos **gestores de primeira e segunda linha** e devem ser realizadas de forma **cíclica e periódica**.

A análise crítica deve responder questões como:

a. **situação:** o resultado identificado no monitoramento é bom ou ruim?
b. **comparação:** a situação do resultado ficou igual ao resultado anterior ou alterou?
c. **explicação:** por que a situação do resultado melhorou, piorou ou ficou igual ao resultado anterior?
d. **ações:** em caso de piora, quais ações serão implementadas para melhorar o resultado?
e. **expectativas:** qual a expectativa para os resultados na próxima medida?

Ressalta-se que o art. 16 da PGR/PR atribui aos gestores de segunda linha, mais especificamente às unidades de governança dos órgãos da PR, a competência de **acompanhar a efetividade das ações e dos controles internos propostos para tratamento dos riscos críticos da sua unidade, e sugerir melhorias,** bem como informar aos comitês internos de governança sobre assuntos que possam impactar o desempenho da Gestão de Riscos.

Compete, também, à Diretoria de Governança, **acompanhar e avaliar os indicadores de desempenho para a gestão de riscos**, conforme art. 15 da PGR/PR.

A análise crítica feita por essas últimas instâncias tem um enfoque mais estratégico, contemplando uma visão mais integrada dos riscos e considerando, por exemplo, se o sistema de gestão de riscos tem contribuído para o alcance dos objetivos institucionais.

D.3. Avaliações independentes

Atividade realizada por meio de **auditoria interna ou externa com o enfoque voltado diretamente à eficácia da estrutura e do processo de gestão de riscos**, em todos os níveis relevantes das atividades organizacionais (TCU, 2018).

O objetivo da auditoria de gestão de riscos é **(i) determinar o nível de maturidade da gestão de riscos da organização, (ii) identificar os aspectos que necessitam ser aperfeiçoados**, e **(iii) emitir relatório detalhado sobre os aspectos e uma conclusão geral sobre a maturidade** (TCU, 2018).

Na PR, esta atividade é de responsabilidade da **gestão de riscos em terceira linha,** exercida pela Ciset.

E. ETAPA 5 – COMUNICAÇÃO DE RISCOS

Comunicar riscos é fornecer as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco, sob pena de ele se materializar plenamente. (TCU, 2020).

A IN Conjunta MP/CGU nº 1/2016 orienta, em seu art. 16, inciso VII, que

> *informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos. (MP/CGU, 2016).*

Complementarmente, a ABNT ISO 31000:2018 relata que o objetivo desta etapa é:

- **comunicar atividades e resultados de gestão de riscos** em toda a organização;

- fornecer informações tempestivas para a tomada de decisão;
- melhorar as atividades de gestão de riscos;
- auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

Cabe ressaltar, entretanto, que as restrições de acesso às informações em razão da sensibilidade de seu conteúdo e da classificação quanto ao grau de sigilo devem ser observadas por todos os servidores da PR e demais partes envolvidas.

Portanto, o fluxo de informações da gestão de riscos da PR ocorrerá de acordo com o estabelecido no Sistema de Gestão de Riscos da Presidência da República, expresso no art. 12 da PGR/PR, conforme demonstrado na figura 1 deste documento (Modelo de três linhas da PR).

Essa comunicação deverá ser realizada observando os procedimentos de segurança, de acordo com a sensibilidade ou classificação da informação.

REFERÊNCIAS

- ABNT NBR ISO 31000. *Gestão de riscos* — Princípios e diretrizes. Rio de Janeiro, nov. 2009a. ISBN 978-85-07-01838-4.
- ISO GUIA 73:2009. Gestão de Riscos – Vocabulário. Rio de Janeiro, 2009b.
- BRASIL. Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. *Diário Oficial da União*, Brasília, DF, seção 1, p. 3, 23 nov. 2017a.
- Guia Técnico de Gestão Estratégica v1.0; Brasília; ME; SEDGG; SEGES, 2019. Versão 1/2020.
- Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. *Diário Oficial da União*, Brasília, DF, 11 mai. 2016.
- MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO - CGU. Portaria CGU nº 1.089, de 25 de abril de 2018. Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. *Diário Oficial da União*, Brasília, DF, ed. 80, seção 1, p. 81, 26 abr. 2018a.
- *Metodologia de Gestão de Riscos*. Brasília, abr. 2018b.
- *Manual para implementação de programas de integridade: orientações para o setor público*. Brasília, jul. 2017b.
- Manual de Gestão de Riscos do TCU. 2ª Edição. Brasília. 2020.
- SELINŠEK, L. Corruption Risk Assessment in Public Institutions in South East Europe: Comparative Study and Methodology. Saravejo: Regional Cooperation Council, 2015.
- TRIBUNAL DE CONTAS DA UNIÃO – TCU. Roteiro de Avaliação de Maturidade da Gestão de Riscos. Brasília: TCU, Secretaria e Métodos e Suporte ao Controle Externo, 2018. 164 p.
- TCU. Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU / Tribunal de Contas da União. Edição 3 - Brasília: TCU, Secretaria de Controle Externo da Administração do Estado – SecexAdministração, 2020.
- *Metodologia de Gestão de Riscos da CGU - versão 2.0.* Brasília. 2021.