AUDITORIA GERAL
DO ESTADO

SECRETARIA
DA FAZENDA

GOVERNO
DO ESTADO

ORIENTAÇÃO TÉCNICA N.º 02/2020

MANUAL DO PROGRAMA DE GESTÃO DE RISCOS

Abril 2020

Auditor Geral do Estado – AGE
Luís Augusto Peixoto Rocha

Gerente de Controle Preventivo e Transparência - GEPRE
Alberto Novais de Queiróz

EQUIPE GEPRE
Ana Luiza Vasconcellos
Cristiane Márcia Veloso de Carvalho
José Raimundo Mota
Sônia Magnólia de Carvalho

DIAGRAMAÇÃO
Gerência de Controle Preventivo e Transparência - GEPRE

HISTÓRICO DE REVISÕES

VERSÃO	DATA	DESCRIÇÃO
1	01/04/2020	Elaboração do Documento

QUADROS

FIGURAS

SUMÁRIO

1. Apresentação

Este Manual, elaborado pela Auditoria Geral do Estado (AGE), através da Gerência de Controle Preventivo e Transparência – GEPRE, é uma publicação destinada à prática e disseminação da gestão de riscos, com o objetivo de apresentar, de forma sintética, os conceitos e princípios que norteiam o tema, além de servir como guia para os agentes e gestores na implantação do **Programa de Gestão de Riscos (PGR).**

A metodologia adotada no PGR tem por finalidade orientar a identificação, avaliação e adoção de respostas aos riscos dos processos da unidade, bem como instruir sobre o monitoramento e acompanhamento das medidas de controle instituídas.

O Manual (**Orientação Técnica - OT AGE n.º 02/2020**) atualiza e substitui a OT AGE n.º 01/2019 - Gestão de Riscos, que orienta o processo de implantação do Programa de Gestão de Riscos (PGR), instituído pela Portaria Sefaz nº 162/2018, nos órgãos e entidades do Poder Executivo Estadual.

Este documento está disponível para consulta no site da Secretaria da Fazenda (SEFAZ) e tem como expectativa servir como guia na implantação do PGR, auxiliando gestores e colaboradores a controlar e mitigar riscos, contribuindo para a melhoria dos processos internos.

2. Introdução

Você já ouviu falar em gestão de riscos no setor público?

As atividades de qualquer organização envolvem riscos que, se não gerenciados, podem se materializar e comprometer a capacidade de gerar, preservar ou entregar valor.

A gestão de riscos pode ser definida como um processo sistemático de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Risco é a 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.

No contexto governamental os riscos podem ter impactos de grande escala. A capacidade de antever, identificar e lidar com situações de risco, elaborando um plano de respostas, é um sinal de maturidade gerencial. Assim sendo, a Gestão de Riscos auxilia o gestor a antecipar os problemas e a se preparar para enfrentá-los da melhor maneira possível. Constitui-se, portanto, elemento importante para a boa governança, pois contribui para reduzir as incertezas que envolvem a definição da estratégia e dos objetivos das organizações públicas e, por conseguinte, o alcance de resultados em benefício da sociedade.

3. O Programa de Gestão de Riscos (PGR) e sua estrutura de governança

O Programa de Gestão de Riscos (PGR) foi instituído na Bahia em 2018, sob a coordenação da Auditoria Geral do Estado (AGE), e se constitui em uma metodologia reconhecida como boa prática de aperfeiçoamento da gestão. Programas semelhantes já estão implantados nos órgãos e entidades da União e em diversos Estados da Federação, e sua adoção vem sendo reiteradamente recomendada pelos órgãos de controle (TCU, CGU, TCEs etc.).

Na Bahia, o PGR está disciplinado pela **Portaria Sefaz nº 162/2018**, inspirada na **Norma ABNT NBR ISO 31000:2018**, que estabelece princípios e diretrizes para a implantação da Gestão de Riscos. No âmbito Federal, a gestão de riscos está estabelecida na **Instrução Normativa Conjunta MP/CGU nº 01**, de 10/05/2016.

O PGR possui ainda os seguintes referenciais normativos:

- Committee of Sponsoring Organizations of the Treadway Commission – COSO 2013 - Internal Control - Integrated Framework (ICIF);
- Orientação Técnica AGE n° 01/2017 - Guia Referencial dos Controles Internos da Gestão.

A gestão de riscos é parte fundamental para a estruturação de um **Programa de Integridade** nas organizações. Nesse sentido, deve-se compreender que existem situações, processos e áreas em que há um risco maior do interesse privado sobrepor-se ao interesse público e, portanto, toda organização deve conhecer previamente quais são essas situações para buscar formas de evitá-las ou mitigá-las.

Desse modo, o PGR se constitui em importante mecanismo para atenuar riscos à **Integridade**, identificando ações ou omissões que possam favorecer à ocorrência de fraudes, solicitação ou recebimento de vantagem indevida, abuso de posição ou poder, utilização de recursos públicos em favor de interesses privados ou atos de corrupção, atuando na prevenção de riscos que possam afetar a reputação da organização.

A **Integridade pública**[1] refere-se ao alinhamento consistente e à adesão de valores, princípios e normas éticas comuns para sustentar e priorizar o interesse público sobre os interesses privados no setor público.

3.1. Objetivos do PGR

- Aumentar a probabilidade de atingimento dos objetivos dos processos selecionados.
- Estimular gestão proativa que antecipe e previna ocorrências capazes de afetar os objetivos organizacionais.
- Identificar e tratar riscos dos processos.
- Melhorar a governança, o controle interno da gestão e a qualidade do gasto público.
- Melhorar a prevenção de perdas e a gestão de incidentes.
- Prezar pelas conformidades legal e normativa dos processos organizacionais.

[1] Extraído do sítio da OCDE - Organização para a Cooperação e Desenvolvimento Econômico.

3.2. Adesão

O PGR deve ser considerado como instrumento do processo de governança e liderança e, consequentemente, é indispensável contar com o **patrocínio e o apoio do dirigente máximo** da organização, a fim de assegurar que seus objetivos sejam plenamente alcançados.

A adesão ao PGR deverá ser formalizada pelo dirigente máximo de cada unidade aderente junto ao Auditor Geral do Estado.

Durante a implantação do Programa ficarão suspensos eventuais trabalhos de auditoria da AGE que tenham como objeto os processos em que estejam sendo aplicada a metodologia do PGR, **exceto** aqueles oriundos de denúncias ou de solicitação do próprio dirigente.

3.3. Comitê de Gestão de Riscos (CGR) e Grupo de Trabalho (GT)

Cada organização que aderir ao PGR, denominada **Unidade Aderente (UA)**, deverá constituir um **Comitê de Gestão de Riscos (CGR)**, principal estrutura estratégica de governança do Programa, **de caráter permanente**, e que deve se reportar diretamente ao dirigente máximo da UA.

Em função dos processos selecionados para serem objeto do Programa serão constituídos, ainda, **Grupos de Trabalho (GTs)**, **de caráter temporário**, que atuarão diretamente nas etapas de aplicação da metodologia dentro de cada processo.

Serão constituídos tantos GTs quantos forem necessários em função dos processos que serão objeto da Gestão de Riscos.

3.3.1. Comitê de Gestão de Riscos (CGR)

Comitê de Gestão de Riscos - CGR

Constituição

Instrumento formal (portaria, p. ex.) expedido pelo Dirigente máximo da UA.

Composição

Preferencialmente, ser composto por 3(três) servidores, dentre os quais:

- O Coordenador da Coordenação de Controle Interno (CCI) ou unidade equivalente, que o coordenará;
- Um representante da Assessoria de Planejamento e Gestão (APG) ou unidade equivalente;
- Um representante da Assessoria do Dirigente máximo do órgão.

Competências

1. Promover ações para disseminar internamente a cultura de Gestão de Riscos;
2. Definir o(s) processo(s) da(s) área(s) finalística(s) que será(ão) objeto do Programa;
3. Indicar os integrantes do(s) Grupo(s) de Trabalho (GTs), com perfil, conhecimento e disponibilidade para participar dos treinamentos e capacitações, bem como do desenvolvimento dos trabalhos;
4. Validar o trabalho efetuado pelos GTs, em especial a Listagem de Riscos e o Plano de Ação elaborados;
5. Acompanhar os trabalhos dos GTs por meio de reuniões periódicas;
6. Estabelecer uma política de reavaliação periódica do Programa e monitorar continuamente o seu desenvolvimento;
7. Fomentar a capacitação dos servidores em Gestão de Riscos;
8. Articular com o Dirigente máximo da UA a indicação dos responsáveis pela implantação do Plano de Ação;
9. Reportar à AGE todas as ações voltadas para a Gestão de Riscos.

3.3.2. Grupo de Trabalho (GT)

Grupo de Trabalho - GT

Constituição

Instrumento formal (portaria, p.ex.) expedido pelo Dirigente máximo da UA.

Composição

- Servidores responsáveis pelos processos selecionados e/ou detenham conhecimento acerca dos seus fluxos e aspectos técnicos, indicados pelo CGR, com perfil, conhecimento e disponibilidade para participar de reuniões e desenvolvimento dos trabalhos;
- Um representante da Coordenação de Controle Interno ou unidade equivalente.

Competências

1. Mapear e analisar os processos objeto da Gestão de Riscos;
2. Identificar os riscos dos processos analisados;
3. Analisar e avaliar os riscos identificados;
4. Elaborar Plano de Ação para implantação das medidas de controle necessárias para tratar os riscos mapeados e submetê-lo ao CGR;
5. Participar das capacitações necessárias para a implantação do Programa;
6. Revisar os produtos elaborados conjuntamente com a equipe da AGE, reunindo-se internamente com os seus membros.

4. Estratégia de implantação da Gestão de Riscos através do PGR

A implantação da Gestão de Riscos através do PGR nas UAs pressupõe duas medidas prévias fundamentais: a **capacitação** dos integrantes da UA e a **seleção dos processos** que serão objeto da metodologia.

4.1. Capacitação das Unidades Aderentes

Compete à AGE promover capacitações sobre **Gestão de Riscos na Administração Pública** e sobre **Mapeamento de Processos** com o objetivo de dotar os participantes, integrantes das UAs, dos instrumentos metodológicos e conceitos básicos da gestão de riscos.

4.2. Seleção dos processos

Para o Programa de Gestão de Riscos (PGR) ser considerado implantado em determinada UA é fundamental que seus principais processos-chave tenham sido identificados e devidamente submetidos e tratados como objeto da metodologia.

O conceito mais imediato de processo organizacional é o de transformação, uma vez que se considera **processo** qualquer atividade ou conjunto de atividades inter-relacionadas ou interativas que **transforma** insumos, que são as entradas, em produtos, que se referem às saídas (ISO 9000:2015).

Figura 1: Representação gráfica de processo

Antes da implantação do Programa propriamente dito, é necessário que a Unidade Aderente (UA) selecione o processo que será objeto da avaliação de riscos. A seleção deve ser criteriosa e objetiva para que o processo escolhido seja relevante para a organização e esteja diretamente relacionado com sua atividade-fim.

Preferencialmente, devem ser **pré-selecionados** processos que possuam as seguintes características constantes na Figura 2.

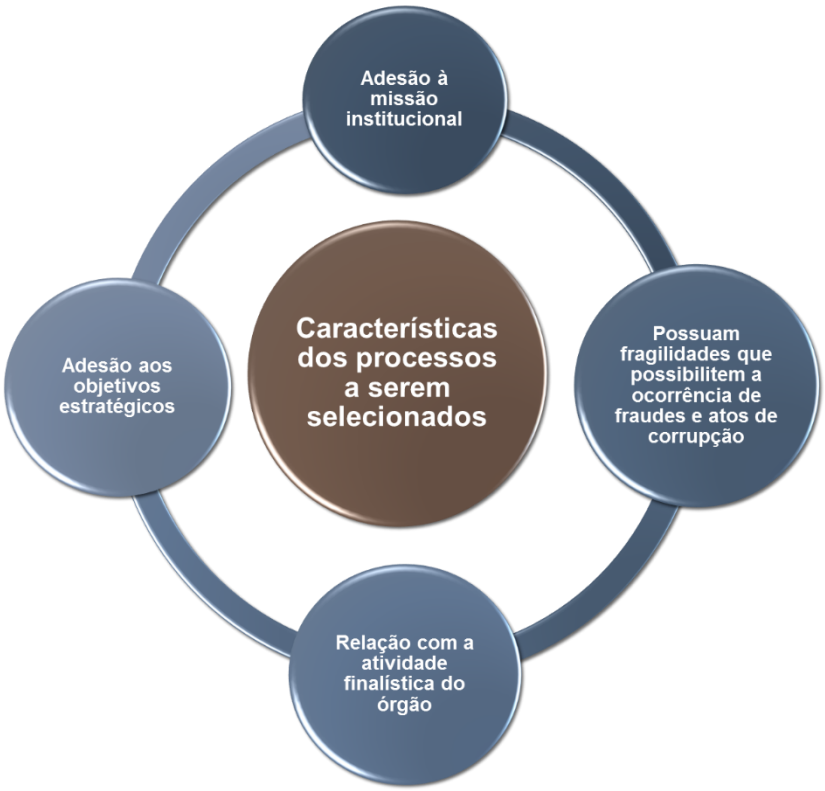


Figura 2: Características dos processos a serem selecionados

Visando promover a hierarquização e identificação dos processos mais críticos e prioritários com vistas à aplicação da metodologia do PGR, recomenda-se a utilização da **Matriz BASICO**[2] por tratar-se de artefato simples e de fácil entendimento.

Nessa Matriz foi acrescentado o critério **(S) Segurança**, com o objetivo de contemplar **riscos de integridade**, ou seja, aqueles relacionados à possibilidade de ocorrência de fraudes e atos de corrupção, englobando situações como recebimento/oferta de propina, desvio de verbas, abuso de poder/influência, nepotismo, conflito de interesses, uso indevido e vazamento de informação sigilosa e outras práticas antiéticas.

Essa ferramenta adaptada é apenas um direcionador para priorização de processos, devendo seus resultados serem utilizados como um norteador para sua seleção. Em última instância, caberá ao CGR definir os processos que serão objeto do PGR.

A **Matriz BASICO(S)** permite ranquear processos estratégicos de acordo com seu nível de impacto em uma organização, selecionando os mais relevantes, conforme 7 critérios apresentados no Quadro 1.

[2] A matriz de priorização BASICO foi desenvolvida com base no balanço Custos x Benefícios x Exequibilidade, por Charles Kepner e Benjamin Tregoe, em 1981, e é uma ferramenta da Qualidade que funciona para determinar os processos que apresentam maior prioridade, dentro de critérios pré-estabelecidos e procura contemplar todos os tipos de clientes da organização.

A ferramenta possui pontuação com **notas de 1 a 5** que serão aferidas durante a análise dos processos. Após a avaliação de todos os critérios é feito o somatório de cada uma das opções consideradas e a **hierarquização** é definida em função dos totais obtidos.

Os processos em que a pontuação do critério **Segurança (S)** for maior ou igual a 3 deverão ser considerados prioritários, independentemente da pontuação total obtida. No caso de empate, o item **Segurança (S)** será utilizado como critério de desempate e subsequentemente, **Cliente externo (usuário final) (C)**.

MATRIZ DE HIERARQUIZAÇÃO DE PROCESSOS – BASICOS		
	CRITÉRIO	**DESCRIÇÃO**
B	**Benefícios para a organização (B)**	Impacto que o processo tem para os resultados da organização. Quanto mais vantagens estiverem associadas a um processo, maior nota ele recebe e quanto menos vantagens, a nota atribuída é menor.
A	**Abrangência dos resultados (A)**	Representa o total de servidores/colaboradores da organização que serão beneficiados com as melhorias do processo. Quanto maior o número de pessoas impactadas, maior deve ser a nota e quanto menor o número menor a nota.
S	**Satisfação dos servidores/colaboradores (S)**	Considera o quanto um processo pode afetar a experiência dos servidores/colaboradores. Quanto mais o processo impactar positivamente na satisfação dos mesmos, maior a nota recebida. Se menores os impactos, menor a nota recebida.
I	**Investimentos necessários (I)**	Recursos financeiros necessários para realizar o processo. Deve-se considerar o valor dispendido com a equipe envolvida, o custo dos materiais necessários, além do valor para sua execução. Se forem dispendidos muitos recursos no processo, ele deve receber uma nota mais alta. Do contrário, ele deve receber nota mais baixa.
C	**Cliente externo (usuário final) (C)**	Grau de impacto do processo na satisfação do usuário final. Quanto mais positivo for o impacto do resultado do processo no usuário final, maior a nota atribuída. Quanto menor o impacto, menor a nota.
O	**Operacionalização (O)**	Refere-se ao grau de facilidade em realizar o processo, ou seja, a sua viabilidade técnica. Quanto mais fácil for executar o processo, maior nota ele deve receber. Quanto mais difícil, menos pontos ele recebe. O processo pode ser mais ou menos difícil de ser conduzido devido a restrições legais, falta de domínio de tecnologia, alta resistência às mudanças etc.
S	**Segurança (S)**	Contempla riscos de integridade, ou seja, aqueles relativos a ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção, englobando situações como recebimento de propina, desvio de verbas, abuso de poder, nepotismo, conflito de interesses, vazamento de informação sigilosa e outras práticas antiéticas. Essas situações tendem a ser observadas nos processos em que há manifesto interesse privado sobre os seus produtos/resultados, a exemplo de: contratações, fiscalizações, licenciamentos, cobrança de taxas, aprovação de crédito, aplicação de multas etc. Quanto maior a exposição à quebra de integridade, maior nota o processo receber. Quanto menos exposto, uma nota menor.

Quadro 1 – Matriz de priorização de processos aplicada ao PGR

4.3. Ciclo de implantação da Gestão de Riscos através do PGR

O ciclo de implantação da Gestão de Riscos corresponde a execução das etapas do PGR em um ou mais processos, agregando aprendizado para a aplicação da metodologia em novos ciclos, melhorando gradativamente o nível de maturidade da organização em relação ao tratamento dos riscos.

A Gestão de Riscos é considerada implantada na UA quando seus principais processos estratégicos forem submetidos ao Programa de Gestão de Riscos (PGR) em um ciclo contínuo. Quanto mais processos-chave tenham sido tratados pela metodologia do PGR, maior será considerada a maturidade da UA em termos de gestão de riscos.

A atuação da AGE no processo de análise de riscos através do PGR varia em função do nível de maturidade em que se encontra a UA em relação à experiência e capacidade de replicação da metodologia do Programa, conforme quadro a seguir.

MATURIDADE DA ORGANIZAÇÃO EM RELAÇÃO À GESTÃO DE RISCOS			
NÍVEL	**ESPECIFICAÇÃO**	**ATUAÇÃO DA AGE**	
		OBJETIVO	**ABRANGÊNCIA**
Inicial (N1)	Nível **inicial** de maturidade que compreende o **primeiro processo** da organização a ser objeto de avaliação pela metodologia de gestão de riscos. Os servidores das UAs envolvidos nesta atividade ainda não possuem domínio da metodologia aplicada.	**Assessoramento direto** às Unidades Aderentes (UAs), em um trabalho conjunto, orientando quanto à aplicação da metodologia e uso da ferramenta adotada.	Durante **todo o período** de implantação do PGR, incluindo o monitoramento da execução do Plano de Ação (PA).
Intermediário (N2)	Nível **intermediário** de maturidade, quando os servidores das UAs, envolvidos nesta atividade, ainda **não se encontram** plenamente aptos a replicar a metodologia, embora já a tenham aplicado em processos anteriores.	**Acompanhamento das atividades** – Via de regra, após a conclusão da análise do primeiro processo, a atuação da AGE junto à UA passa a ser de acompanhamento das ações do CGR relativas à análise de riscos de outros processos.	Restrita às **etapas e produtos mais significativos** da metodologia, Listagem de Riscos, Mensuração dos Riscos Residuais e Plano de Ação (PA), incluindo o monitoramento da execução do PA.
Avançado (N3)	Nível **avançado** de maturidade, quando os servidores das UAs, envolvidos nesta atividade **encontram-se** aptos a replicar a metodologia em novos processos. Somente nas UAs habilitadas neste nível a gestão de riscos será considerada plenamente incorporada ao seu processo de governança, consolidando-se, assim, a implantação o PGR.	**Monitoramento** do Programa de Gestão de Riscos.	Acompanhamento do Programa e **assessoria mediante demanda** da UA**.**

Quadro 2 – Nível de maturidade organizacional aplicada ao PGR

A figura a seguir representa graficamente a evolução da maturidade do ciclo de implantação da Gestão de Riscos:

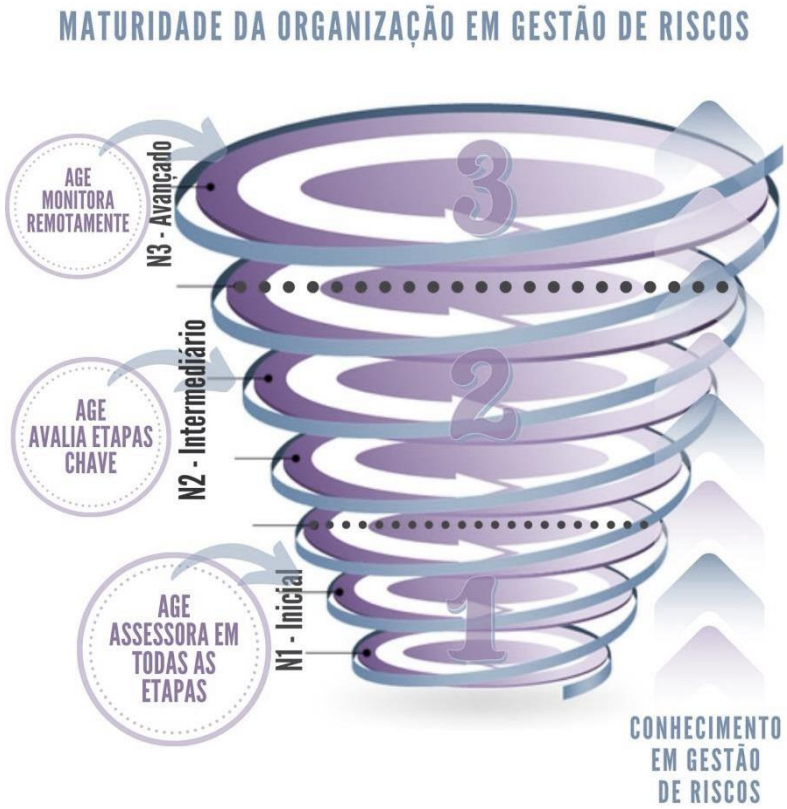


Figura 3: Ciclo de implantação da Gestão de Riscos

Cabe ao CGR avaliar o nível de maturidade em relação à gestão de riscos em que se encontra sua unidade, o que definirá o grau de atuação da AGE em novos ciclos e processos do PGR.

A cada novo processo avaliado pela metodologia do PGR, as UAs deverão **informar previamente** a AGE para devido registro e acompanhamento.

O fluxo básico de implantação do PGR está representado a seguir (Figura 4):

FLUXO BÁSICO DE IMPLANTAÇÃO DO PGR:

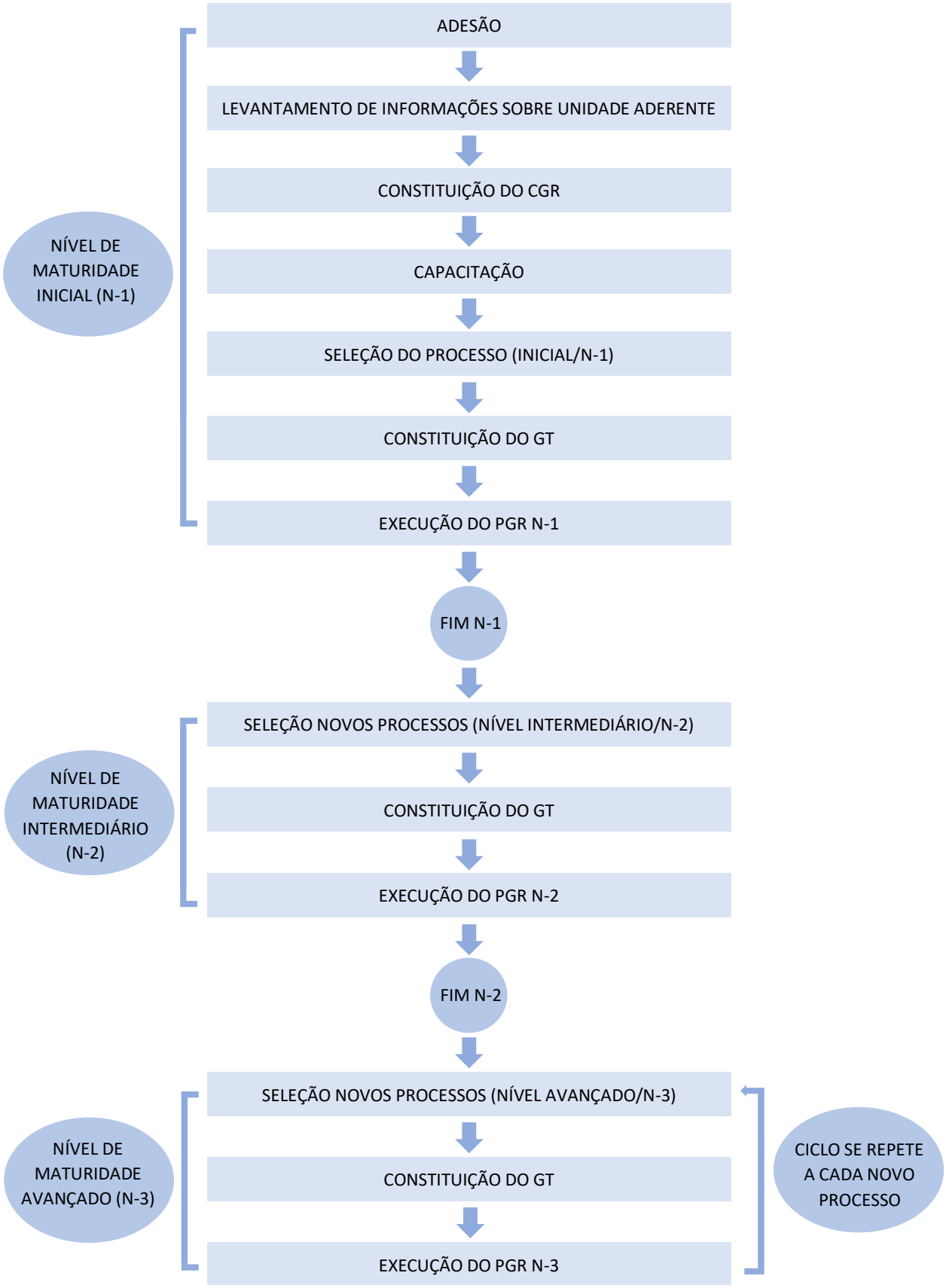


Figura 4: Fluxo básico de implantação do PGR

5. Metodologia da Gestão de Riscos

A metodologia adotada pela AGE no Programa de Gestão de Riscos (PGR) está baseada na Norma ABNT ISO 31000:2018, devidamente adaptada às peculiaridades da administração pública estadual, resultando em ferramenta prática, de fácil aplicação e que oferece resultados em curto prazo.

A metodologia do PGR deve ser aplicada para cada processo selecionado pela Unidade e compreende 7 (sete) etapas a seguir descritas:

5.1. Análise de contexto

Esta etapa inicia-se com a confirmação do processo selecionado, **precisamente delimitado** (início, meio e fim) e envolve a sua compreensão e **mapeamento** (se for o caso), identificação dos seus objetivos e definição dos contextos interno e externo para o gerenciamento dos riscos.

A unidade deverá fornecer informações para subsidiar a análise dos ambientes interno e externo da organização que serão registradas na ferramenta de gestão de riscos adotada.

A partir dessa etapa o Grupo de Trabalho (GT), com o apoio da equipe da AGE (que varia de acordo com o nível de maturidade da UA, conforme Quadro 2), iniciará o preenchimento da ferramenta padrão utilizada pelo PGR, que se estenderá até o Plano de Ação e o posterior monitoramento.

A estimativa é que o cronograma de execução das etapas do PGR dure, no máximo, 03 meses, com reuniões periódicas entre o Grupo de Trabalho (GT) e atuação da AGE conforme Quadro 2. Essa estimativa pode variar em função do comprometimento dos integrantes do GT em participar das reuniões de trabalho, do nível de maturidade da organização e da complexidade do processo objeto do PGR.

Segue abaixo o passo a passo para execução dessa etapa:

	Mapear o processo selecionado para entendimento do seu funcionamento, detalhando as entradas, saídas, ações e competências. Deve ter como foco a identificação de pontos de fragilidade passíveis de riscos de controle, de modo que seu nível de detalhamento não deve abranger minúcias relacionadas com a descrição pormenorizada do processo. **Atenção:** O que se pretende não é mapear ou redesenhar formalmente o processo de trabalho avaliado, mas sim conhecê-lo, identificar com clareza seus objetivos e as fontes de riscos presentes em suas atividades. A preocupação deve ser descrever como ele é efetivamente executado, desde seu início até a sua finalização com a entrega do produto final. **O mapeamento do processo pode ser dispensado, caso já tenha sido devidamente elaborado e esteja atualizado**.
	Utilizar a Análise **SWOT** (forças, oportunidades, fraquezas e ameaças) (Figura 3) como instrumento para identificar cenários internos e externos com potencial de impactar positiva ou negativamente os objetivos estratégicos da organização.
	Definir o **contexto interno** em que o processo se desenvolve, identificando as forças (a serem conservadas) e fraquezas (a serem eliminadas ou atenuadas), levando em consideração atributos tangíveis (pessoas, equipamentos, materiais) e intangíveis (cultura, processos, valores, conhecimento).

PASSO A PASSO	Definir o **contexto externo**, identificando fatores extrínsecos à organização, ou seja, os atributos do ambiente que envolvem a execução do processo, como oportunidades (aspectos que se deve aproveitar) e ameaças (evitar ou atenuar exposição), levando em consideração, por exemplo, legislação, tecnologia, mercado, aspectos sociais e econômicos, dentre outros.
	Identificar, preliminarmente, os **perigos**, listando os principais elementos que podem vir a afetar o processo e apontando suas causas e consequências. **Atenção:** Os **perigos** serão obtidos a partir das "fraquezas" e "ameaças" levantadas na Análise SWOT, ou seja, a relação de "perigos" corresponde, inicialmente, a essas informações levantadas na SWOT. Entretanto, outros perigos poderão ser incluídos nessa listagem, independentemente de terem ou não sido identificados na etapa anterior. **Atenção: as "consequências" dos perigos correspondem aos "riscos"** e deverão ser descritas com detalhes suficientes para sua correta contextualização como "riscos".
	Concluir a Análise de Contexto e validar o resultado desta etapa em reunião específica com o CGR.

Para identificar, no ambiente interno, as forças e fraquezas, ou seja, os pontos fortes e fracos associados aos processos em análise, bem como para analisar e registar as possíveis influências do ambiente externo sobre esses processos, buscando identificar ameaças e oportunidades, o PGR utiliza a análise SWOT (Figura 5), que se constitui em uma ferramenta usualmente empregada para fazer avaliação de cenário e objetivar a análise de contexto. Estas informações, por sua vez, vão contribuir para o levantamento posterior da listagem de perigos.

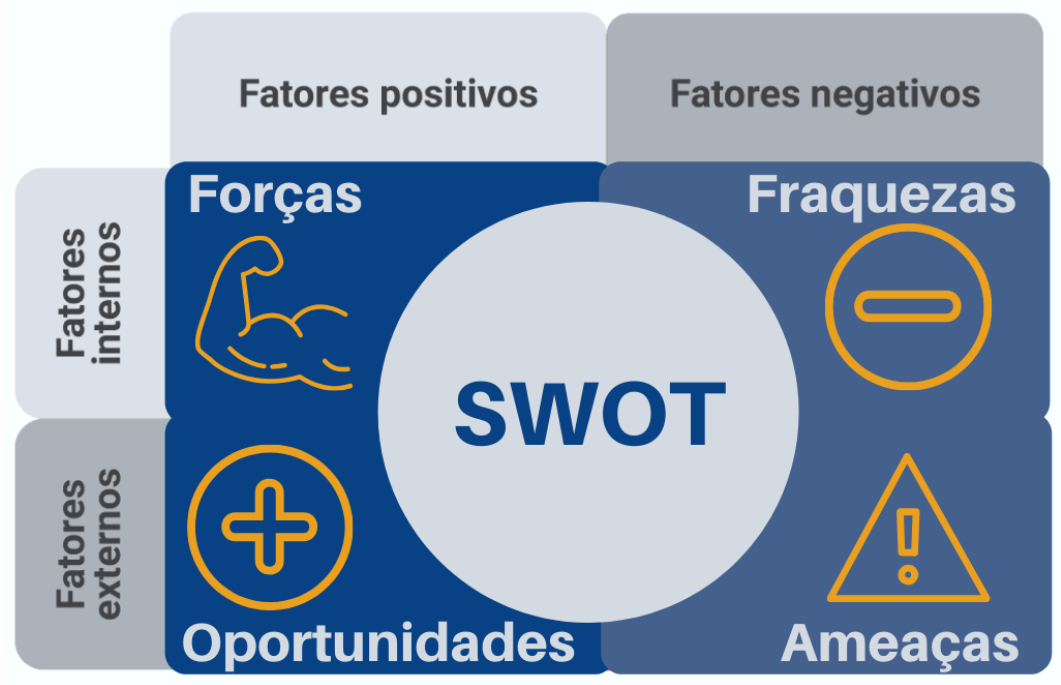


Figura 5: Análise SWOT

Os resultados dessa etapa deverão ser registrados em planilha específica, conforme modelo a seguir (Figura 6):

ANÁLISE DE CONTEXTO		
ÓRGÃO/PROCESSO FOCO DA ANÁLISE:		
OBJETIVOS E METAS ASSOCIADOS AO ÓRGÃO/PROCESSO:		
LEGISLAÇÃO/NORMAS ASSOCIADAS:		
PARTES INTERESSADAS (PESSOAS, GRUPOS, ÓRGÃOS/ENTIDADES):		
MATRIZ SWOT		
AMBIENTE INTERNO		
FORÇAS	**FRAQUEZAS**	
AMBIENTE EXTERNO		
OPORTUNIDADES	**AMEAÇAS**	
ANÁLISE PRELIMINAR DE PERIGOS (listar principais elementos que podem gerar riscos ao processo a partir das “fraquezas” e “ameaças”)		
PERIGOS	**CAUSAS**	**CONSEQUÊNCIAS**

Figura 6: Planilha Análise de Contexto

5.2. Identificação dos riscos

A partir da **análise preliminar dos perigos** identificados na etapa anterior deverão ser realizados os seguintes passos:

PASSO A PASSO	Gerar, com base nas **consequências dos perigos**, uma listagem dos possíveis riscos.
	Apurar e registrar as **causas** dos riscos identificados, ou seja, as condições que dão origem à possibilidade de um evento ocorrer (**fatores de risco**). **Atenção:** Cada **causa** deve ser registrada em linha separada porque, quando da elaboração do Plano de Ação, cada uma será objeto de tratamento específico.
	Apurar e registrar as **consequências** dos riscos identificados, ou seja, os resultados ou os efeitos de um evento de risco sobre os objetivos do processo.
	Testar a coerência dos riscos identificados, aplicando a **sintaxe** constante na Figura 7 (Diagrama Bowtie).

A coerência dos riscos identificados deve ser testada aplicando-se a **sintaxe** constante na Figura 7.

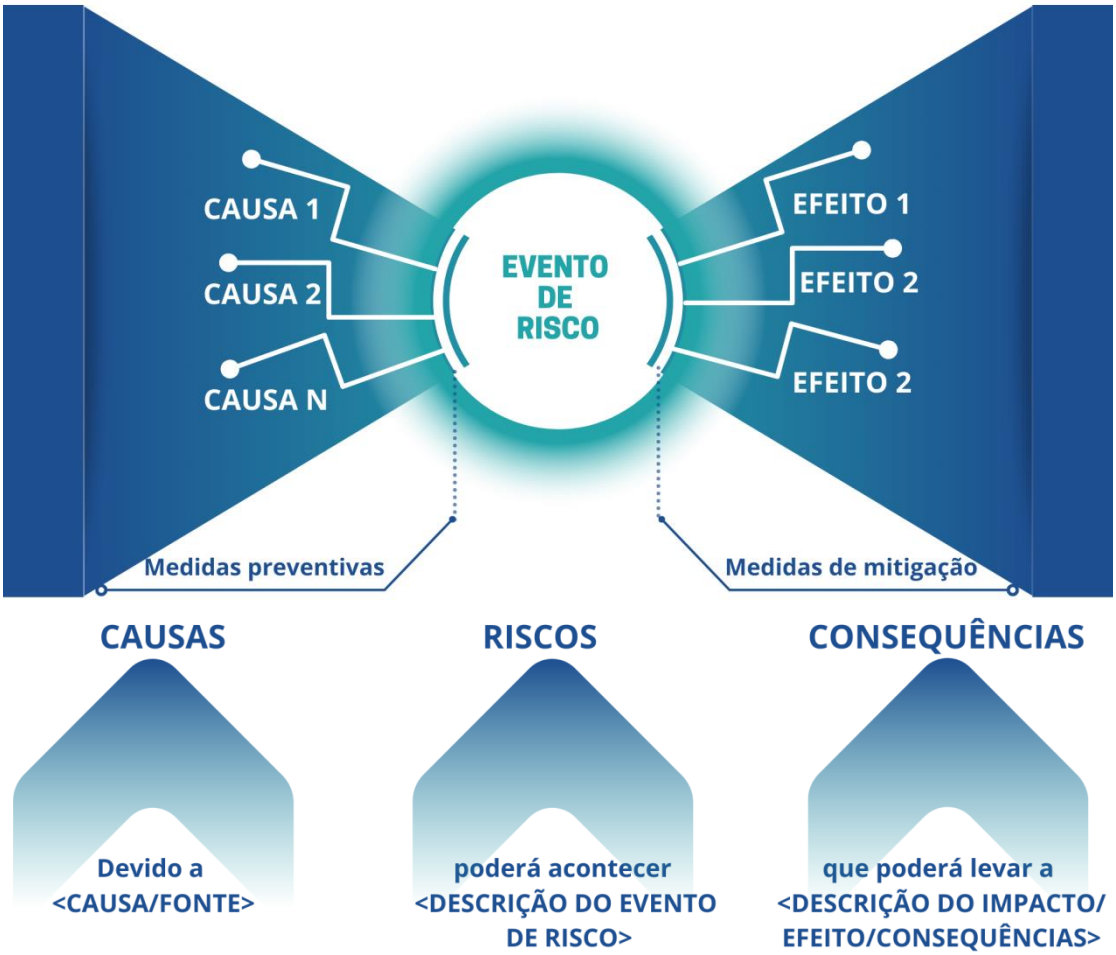


Figura 7: Diagrama Bowtie e a sintaxe de coerência dos riscos

Os riscos identificados nessa etapa, juntamente com suas **causas** e **consequências**, deverão ser registrados em planilha específica, conforme modelo a seguir (Figura 8):

LISTAGEM DE RISCOS

ÓRGÃO/ENTIDADE:			
PROCESSO:			
Nº	**RISCOS**	**CAUSA(S)**	**EFEITO(S)**
		Cada causa identificada deve ser descrita em uma linha, pois deverá ser objeto de tratamento individualizado	*Os efeitos podem ser descritos numa mesma linha*

Figura 8: Planilha Listagem de Riscos

Os riscos podem ser internos ou externos. A principal diferença entre essas categorias é que os **externos** decorrem do ambiente externo, não estando, portanto, sob controle da organização, enquanto os **internos** estão dentro da organização, o que possibilita, em princípio, uma maior ação sobre suas causas.

O Quadro 3 apresenta uma relação de **categorias de riscos** internos e externos:

ORIGEM	CATEGORIAS	DESCRIÇÃO	EXEMPLOS
EXTERNA	**POLÍTICA**	Quando ocorrem mudanças que resultem em descontinuidades de políticas públicas ou alteração de prioridades do governo.	- Descontinuidade de programas sociais. - Alteração de políticas de parcerias entre Estado e Organizações da Sociedade Civil.
	ECONÔMICA	Eventos relacionados à alterações de impacto na economia.	- Redução do preço do petróleo (queda da arrecadação). - Valorização cambial levando ao aumento do preço das importações (oportunidade para exportadores e risco para importadores e tomadores de empréstimos em moeda estrangeira). - Queda na arrecadação.
	SOCIAL	Mudanças demográficas com impacto na demanda de determinados serviços.	- Envelhecimento da população impactando a Previdência. - Aumento dos custos do SUS devido ao incremento da demanda por serviços geriátricos.
	TECNOLÓGICA	Eventos relacionados à evolução tecnológica aplicada aos processos.	- Obsolescência dos sistemas atuais levando à necessidade de renovações e custos imprevistos.
	AMBIENTAL	Refere-se a eventos (naturais ou não) que podem provocar danos à operação das organizações.	- Incêndios, enchentes e rompimentos de barragens. - Pandemias como a do coronavírus.
	LEGAL	Surgimento de dispositivos legais que imponham restrições (ou oportunidades) a determinados setores.	- Alteração da lei que regulamenta a distribuição de royalties do petróleo. - Mudanças nos critérios de distribuição do Fundo de Participação de Estados e Municípios.
INTERNA	**INFRAESTRUTURA**	Eventos relacionados a adequação da infraestrutura para execução do processo (instalações, equipamentos, modelo de gestão etc)	- Assunção de novas responsabilidades sem adequação da infraestrutura.
	PESSOAL	Eventos relacionados com a quantidade, qualidade e integridade dos recursos humanos.	- Carência de pessoal. - Falta de capacitação adequada. - Fraude cometida por servidor.
	PROCESSOS	Eventos relacionados com modificações de processos sem planejamento e avaliação dos impactos e sem divulgação adequada dos protocolos administrativos.	- Alteração de fluxos dos processos sem dimensionamento correto da nova demanda (previdência).
	TECNOLOGIA	Eventos relacionados com a adequação da tecnologia aos objetivos dos processos.	- Otimização da forma de coletar dados ou aplicar multas. - Implantação de sistema sem teste prévio.

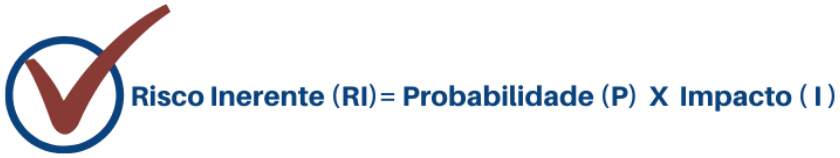
Quadro 3 – Categorias de Riscos - Adaptado de Miranda, Rodrigo Fontenelle. In: Implementando a Gestão de Riscos no Setor Público (2017)

Existem ainda riscos que extrapolam as categorias acima, podendo ser originados tanto interna como externamente, à exemplo dos riscos estratégicos, operacionais, de imagem, financeiros ou de regulação (vide glossário).

5.3. Mensuração dos riscos inerentes

De acordo com a ISO 31000:2018, **análise de riscos** é o processo de compreender a natureza e determinar o nível de risco. Ela fornece a base para a avaliação de riscos, bem como para as decisões quanto ao seu tratamento.

Nesta etapa serão analisados os **riscos inerentes**, ou seja, aqueles a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.



Segue abaixo o passo a passo para execução dessa etapa:

PASSO A PASSO	Estimar e registrar, com base no histórico e na percepção do analista, a **probabilidade** de ocorrência de cada risco levantado seguindo a escala constante no Quadro 4.
	Estimar o **impacto** de cada risco listado, seguindo a escala constante no Quadro 5.
	Atenção: Os valores atribuídos à **probabilidade** e ao **impacto** serão multiplicados, gerando o **risco inerente** de cada risco levantado. Exemplo: probabilidade de ocorrência igual a 3 (média) X impacto igual a 2 (pequeno) = risco inerente 6 (3x2). (Quadro 6).

A incerteza de eventos em potencial é avaliada a partir de duas perspectivas – **probabilidade** e **impacto**. A **probabilidade** representa a **possibilidade** de que um determinado evento ocorra, enquanto o **impacto** representa o seu **efeito.**

Os **riscos inerentes** são, portanto, expressos pela combinação da **probabilidade** da ocorrência do evento e de suas consequências e em termos da magnitude do **impacto** nos objetivos,

O Quadro 4 apresenta escala de **probabilidade** para sua mensuração.

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	Muito baixa	Baixa	Média	Alta	Muito alta
Peso	**1**	**2**	**3**	**4**	**5**

Quadro 4 – Escala de probabilidade adaptada do Manual de Gestão de Riscos e Controle Interno da Gestão do Ministério do Planejamento (2017)

O Quadro 5 apresenta os fatores que devem ser considerados para orientar a análise do **impacto** do evento de acordo com seus efeitos. Esses fatores estão subdivididos em dois níveis: **estratégico-operacional** e **econômico-financeiro.**

O **nível estratégico-operacional** está segmentado em 5 categorias:

a) **Esforço de gestão**: compreende a capacidade que a organização tem de governança e controle sobre o risco analisado.

b) **Regulação**: compreende a capacidade que o risco tem de propiciar ações sancionatórias contra a organização por parte de órgãos reguladores.

c) **Reputação**: corresponde ao potencial que o risco tem de afetar negativamente a imagem institucional da organização.

d) **Negócios/serviços à sociedade**: compreende a capacidade do risco comprometer a entrega de produto/serviço.

e) **Intervenção hierárquica**: compreende a capacidade que os riscos têm de exigir alçadas de interferência cada vez mais superiores para enfrentá-los, caso venham a ocorrer.

Já o **nível econômico-financeiro** possui somente uma categoria, denominada "**orçamentário**", que corresponde ao volume de recursos comprometidos caso o risco venha, de fato, a se materializar.

A ferramenta utilizada pelo PGR para avaliar o **impacto** do risco pode isolar ou desconsiderar um ou mais desses fatores, se o analista os considerar irrelevantes ou de difícil avaliação.

	Impacto						
	Estratégico-Operacional					Econômico-Financeiro	
	Esforço de Gestão Governabilidade sobre o risco	Regulação Sanção de órgãos regulatórios	Reputação Comprometimento da imagem institucional	Negócios/Serviços à Sociedade Entrega de produto ou serviço	Intervenção Hierárquica Alçada de interferência	Orçamentário Recursos envolvidos	Dimensão do impacto
Orientações para atribuição de notas ao impacto do risco	Evento com potencial para levar o negócio ou serviço ao colapso	Determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão do Estado	Exige a intervenção do Governador	> = 25%	**5 Catastrófico**
	Evento crítico, mas que com a devida gestão pode ser suportado	Determina ações de caráter pecuniário (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance da missão da Unidade	Exige a intervenção do Secretário	> = 10% < 25%	**4 Grande**
	Evento significativo que pode ser gerenciado em circunstâncias normais	Determina ações de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos	Exige a intervenção do Superintendente	> = 3% < 10%	**3 Moderado**
	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Determina ações de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo	Exige a intervenção do Coordenador/Diretor	> = 1% < 3%	**2 Pequeno**
	Evento cujo impacto pode ser absorvido por meio de atividades normais	Pouco ou nenhum impacto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas	Seria alcançada no funcionamento normal da atividade	< 1%	**1 Insignificante**

Quadro 5 – Escala de Impacto adaptada do Manual de Gestão de Riscos e Controle Interno da Gestão do Ministério do Planejamento (2017)

Esses fatores servem para nortear a avaliação do **impacto** de cada risco. Para fins de definição da nota final do impacto deve-se considerar como preponderante o fator ao qual se atribuiu a **maior dimensão**. P.ex: se o impacto do risco foi avaliado como "catastrófico" (nota 5) em termos de "governabilidade", ou seja, capaz de levar o serviço ao colapso, mesmo que a avaliação dos demais fatores tenha alcançado nota mínima (1 – insignificante) deve-se considerar o impacto geral como "catastrófico" (nota 5).

Após as estimativas de **probabilidade (P)** e de **impacto (I)** serão calculados os **riscos inerentes (P x I),** de acordo com a matriz do Quadro 6:

Matriz de Riscos

LEGENDA DO NÍVEL/FAIXA DE RISCO: CRÍTICO ALTO MODERADO PEQUENO		PROBABILIDADE (P)				
		1 MUITO BAIXA	2 BAIXA	3 MÉDIA	4 ALTA	5 MUITO ALTA
IMPACTO (I)	5 CATASTRÓFICO	5 (P X I)	10	15	20	25
	4 GRANDE	4	8	12	16	20
	3 MODERADO	3	6	9	12	15
	2 PEQUENO	2	4	6	8	10
	1 INSIGNIFICANTE	1	2	3	4	5 (P X I)

Quadro 6 – Matriz de Riscos (Probabilidade x Impacto)

O nível ou faixa de risco expressa a magnitude de determinado evento de risco, em termos de combinação de seu **impacto** e **probabilidade**. Cada nível ou faixa de risco está representado por uma área com cores específicas na Matriz do Quadro 6 (**Crítico**: vermelho; **Alto**: laranja; **Moderado**: amarelo; e **Pequeno**: verde).

A mensuração dos **riscos inerentes** efetuada nessa etapa deverá ser registrada em planilha específica, conforme modelo a seguir:

MENSURAÇÃO DOS RISCOS INERENTES																
ÓRGÃO / ENTIDADE:																
PROCESSO:																
RISCOS		**Probabilidade estimada de ocorrência Peso: 1 a 5**							**Impacto estimado sobre os objetivos do processo Peso: 1 a 5**							**MATRIZ DE RISCOS**
		Probabilidade estimada de ocorrência Peso: 1 a 5	Escala de **probabilidade** de ocorrência						Impacto estimado sobre os objetivos do processo Peso: 1 a 5	Escala de **impacto** estimado						**Valor do Risco Inerente (P X I)**
			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			Evento cujo impacto pode ser absorvido por meio de atividades normais	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Evento significativo que pode ser gerenciado em circunstâncias normais	Evento crítico, mas que com a devida gestão pode ser suportado	Evento com potencial para levar o negócio ou serviço ao colapso	
			1	2	3	4	5			1	2	3	4	5		
			Muito baixa	Baixa	Média	Alta	Muito Alta			Insignificante	Pequeno	Moderado	Grande	Catastrófico		
1	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	5	Muito Alta						4	*Grande (Seguir orientações do Quadro 5 para efetuar essa mensuração)*						20
2																
3																
4																
n																

Figura 9: Planilha Mensuração dos Riscos Inerentes

5.4. Identificação e avaliação dos controles internos existentes

5.4.1. Conceito de controles internos da gestão

Referem-se ao 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 para o atingimento dos objetivos (IN Conjunta MP/CGU nº 01/2016).

5.4.2. Tipologia de controles

Só existem controles porque existem riscos a serem tratados. O tratamento do risco pode ser classificado em pelo menos dois tipos de controles: os preventivos e os corretivos.

Controles preventivos são aqueles estabelecidos para limitar a possibilidade de um risco vir a se materializar. Quanto maior for a necessidade de que um resultado indesejável não surja, mais importante se torna implementar esse tipo de controles. Exemplo: *segregação de funções* para reduzir o risco de erros ou fraudes.

Controles corretivos são aqueles utilizados para corrigir resultados indesejáveis que já foram realizados. Exemplo: *Plano de Contingência*, que é o meio pelo qual as organizações planejam a continuidade ou recuperação de suas atividades após o acontecimento de eventos que não puderam ser evitados (rompimento de barragens; surtos de pandemias etc).

Independentemente do tipo de controle a ser implementado, ao se projetar um controle é importante que ele seja proporcional ao risco e de acordo com o apetite ao risco da organização. Deve-se também atentar para a relação custo-benefício do controle, ou seja, o benefício proporcionado deve ser maior do que o custo de sua implementação.

A lista a seguir apresenta, a título de exemplo, uma relação de controles internos que podem ser utilizados no tratamento dos riscos:

- **Aplicação de *checklists*:** elaboração e implantação de listas de verificações, de modo a conferir, previamente, se todas as etapas do processo formal foram seguidas e responsabilizando, mediante aposição de assinatura, o servidor executante (p.ex: *checklist* sobre cumprimento de todas as exigências legais relativas à concessão de licenças e outorgas).
- **Atribuição de autoridade e limites de alçada**: definição formal e clara de quem tem autoridade para tomar determinadas decisões, com delimitação de até onde vai esse poder (p.ex: assinatura de contratos a partir determinados valores somente pelo Dirigente máximo).
- **Capacitação e treinamento**: estabelecimento de programa de capacitação permanente dos servidores, tendo em vista mantê-los aptos a executarem corretamente os processos sob sua responsabilidade.
- **Comunicação, publicidade e transparência**: implantação de diretrizes voltadas para tornar públicas as ações e decisões gerenciais, de modo a assegurar a transparência dos atos e contribuir para o controle social dos processos (p.ex: publicação em portal de informações de interesse público, como agenda de Dirigentes, renúncias de receitas; parcerias celebradas; relação de processos administrativos disciplinares abertos e situação).
- **Estruturação adequada**: manutenção de estrutura física e de pessoal adequadas para realização da atividade, tendo em vista a quantidade e a qualidade dos recursos necessários para atender ao volume e à complexidade inerentes a cada processo.
- **Formalização de manuais e procedimentos**: definição formal de normas e procedimentos a serem cumpridos pelos executores de determinados processos, com regras explícitas sobre como proceder e realizar as atividades de forma a cumprir todos os requisitos de gestão, inclusive o controle (p.ex: procedimentos operacionais padrões; descrição e fluxograma de processos).
- **Programas de contingência**: planejamento de ações a serem implementadas em caso de eventos que comprometam os objetivos estratégicos da organização, podendo a chegar à paralisação total ou parcial das atividades (p.ex: apagões; bug de sistemas; pandemias; greves prolongadas etc).
- **Rastreamento do serviço realizado ou material entregue (qualidade e quantidade)**: realização de procedimentos para rastrear a execução do processo, de modo a aferir se o mesmo foi realizado dentro dos parâmetros definidos, em especial quanto à qualidade e quantidade (p.ex: entrevistas com gestores, empregados de prestadores de serviços, servidores e usuários; pesquisa de satisfação; mecanismo de controle social; inventário e contagem física; comparativo entre o planejado e o executado; circularização).
- **Relatórios de acompanhamento**: reporte periódico dos registros de verificação dos processos efetuado por terceiros (em geral pela segunda e terceira linha de defesas), de modo a aferir sua conformidade com os critérios e normas, em especial com os indicadores de desempenho (p. ex: relatórios de monitoramento e acompanhamento do PPA).
- **Revisão por terceiros**: atribuição de responsabilidade a terceiros, não envolvidos na execução do processo, para revisar os atos e procedimentos dos executores, atestando e/ou emitindo parecer prévio sobre o cumprimento das normas, legislações, procedimentos e demais requisitos de controle (p.ex: parecer de assessoria jurídica; submissão de atos à convalidação prévia de comitês e conselhos; parecer de fiscal de contrato).
- **Rotação de pessoal**: promoção de rodízio de funções para assegurar disseminação e compartilhamento de conhecimento sobre os processos internos, de modo a evitar concentração de habilidades e competências em poucos servidores e minimizar os riscos de tornar a organização dependente e vulnerável.
- **Segregação de funções**: separação de atividades/atribuições entre servidores responsáveis por fases distintas de um processo crítico.
- **Sistemas informatizados**: implantação de controles informatizados e, se for o caso, com mecanismos automáticos capazes de sinalizarem e até impedirem realização de operações atípicas, não conformes ou ilegais, de acordo com parâmetros previamente definidos (p.ex: sistema para acompanhar cobrança e arrecadação de receitas).
- **Testes de conformidade/inspeção**: verificação à base de testes (por amostra ou por totalidade) de pontos específicos de controle definidos previamente para cada processo, tendo como critério normas internas, boas práticas de gestão e/ou legislações específicas.
- **Utilização de senhas individuais**: atribuição de senhas individuais de acesso a sistemas e bancos de dados, de modo a evitar utilização por pessoas não autorizadas a manipular dados e informações dos processos; registrar trilha de acessos e identificar os responsáveis por alterações e atualizações.

- **Visitas e controle *in loco***: realização de visita aos locais onde os processos se realizam, de modo a verificar se todos os requisitos e obrigações legais e normativas estão sendo devidamente seguidas (p.ex: visitar local da execução da prestação do serviço para atestar cumprimento de obrigações conforme contrato).

5.4.3. Avaliação dos controles internos existentes

Uma vez mensurado o **risco inerente** é necessário identificar e avaliar os **controles existentes** que respondam aos eventos de riscos identificados, quanto ao seu **Desenho** (ou seja, em relação à formalização e adequação) e **Operação** (ou seja, em relação à sua institucionalização e efetiva execução).

Devem ser relacionados e descritos os controles internos existentes para cada um dos riscos identificados, observando que um mesmo controle pode ser utilizado para tratar mais de um risco.

Após essa etapa deve ser **avaliada**, com base em discussões realizadas com os responsáveis pelos processos e na percepção do analista, **a efetividade dos controles internos existentes para cada risco**, de acordo com as escalas constantes no Quadro 7.

AVALIAÇÃO DOS CONTROLES EXISTENTES

Quanto ao Desenho	
Nota	**Descrição**
1	Não há sistema de controle
2	Há procedimentos de controles, mas não são adequados e nem estão formalizados
3	Há procedimentos de controles formalizados, mas não estão adequados (insuficientes)
4	Há procedimentos de controles adequados (suficientes), mas não estão formalizados
5	Há procedimentos de controles adequados (suficientes) e formalizados
Quanto a Operação	
Nota	**Descrição**
1	Não há procedimentos de controle
2	Há procedimentos de controle, mas não são executados
3	Os procedimentos de controle estão sendo parcialmente executados
4	Os procedimentos de controle são executados, mas sem evidência de sua realização
5	Procedimentos de controle são executados e com evidência de sua realização

Quadro 7 – Escala de avaliação dos controles existentes

As notas apuradas quanto ao **Desenho** e **Operação** devem ser multiplicadas para se obter a **Matriz de Avaliação de Controles Existentes**, conforme Quadro 8.

MATRIZ DE AVALIAÇÃO DE CONTROLES EXISTENTES

OPERAÇÃO \ DESENHO	1	2	3	4	5
2	4	6	8	10	
3	6	9	12	15	
4	8	12	16	20	
5	10	15	20	25	

Quadro 8 – Matriz de Controles Internos (Desenho e Operação)

As notas apuradas na **Matriz de Avaliação de Controles Existentes (Desenho x Operação)** devem ser **convertidas** na escala da **Tabela FAC - Fatores de avaliação dos controles internos**, identificando-se o fator (FAC) correspondente, conforme Quadro 9.

TABELA FAC - FATORES DE AVALIAÇÃO DOS CONTROLES INTERNOS			
DESCRIÇÃO	**NÍVEL DO CONTROLE**	**NOTAS DO QUADRO 8**	**FATOR (FAC)**
Ausência completa de controle (**neste caso, o risco inerente permanecerá inalterado)**	**INEXISTENTE**	**1 a 5**	**1**
Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual **(controle reduz em 20% o risco inerente)**	**FRACO**	**6 a 10**	**0,8**
Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou ferramentas não são adequados **(controle reduz em 40% o risco inerente)**	**MEDIANO**	**12 e 15**	**0,6**
Controle normatizado e, embora passível de aperfeiçoamento, se sustenta por ferramentas adequadas e mitiga o risco razoavelmente **(controle reduz em 60% o risco inerente)**	**SATISFATÓRIO**	**16 e 20**	**0,4**
Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de "melhor prática" **(controle reduz em 80% o risco inerente)**	**FORTE**	**25**	**0,2**

Quadro 9 – Fatores de Avaliação dos Controles Internos (FAC)

5.5. Mensuração dos riscos residuais

Etapa em que é avaliado o risco a que uma organização está exposta **após** a avaliação dos controles internos relacionados a cada risco.

COMO MENSURAR OS RISCOS RESIDUAIS?

Risco Residual (RR) = Risco Inerente (RI) X Fator da Avaliação do Controle (FAC)

PASSO A PASSO	Multiplicar os valores atribuídos ao **risco inerente** (calculados na planilha da Figura 9) pelo F**ator de avaliação do controle (FAC) –** Quadro 9 **-** para obter o **risco residual** de cada risco listado. Exemplo: risco inerente igual a 6 X avaliação do controle (FAC) igual a 0,8 (fraco) = risco residual 4,8 (6x0,8). **Atenção:** Os valores decimais devem ser aproximados para o inteiro imediatamente superior constante da **Matriz de Riscos**.
	Registrar na planilha **Mensuração dos Riscos Residuais** (Figura 10) os **riscos residuais** calculados, identificando a faixa ou nível de gravidade (crítico, alto, moderado ou pequeno), conforme Quadro 10.
	Validar o resultado das etapas anteriores em reunião específica com o CGR.

O Quadro 10 apresenta as **faixas ou níveis** de gravidade (crítico, alto, moderado ou pequeno) em que se encontram os **riscos residuais** apurados **após a avaliação dos controles existentes**.

Escala de Distribuição de Risco Residual por faixas	
Níveis/faixas de gravidade	**Pontuação (após aplicação do FAC – Quadro 9)**
RC - RISCO CRÍTICO	**13 a 25**
RA - RISCO ALTO	**7 a 12**
RM - RISCO MODERADO	**4 a 6**
RP - RISCO PEQUENO	**1 a 3**

Quadro 10 – Faixas dos Riscos Residuais

Essa distribuição poderá ter suas faixas alteradas em função do **apetite a risco** de cada organização/processo. Ou seja, a depender do apetite a risco, o **nível crítico**, por exemplo, pode ser expandido, passando da faixa de **13 a 25** para outra de **12 a 25**, o que significa que a organização considera ter um **menor** apetite a risco. Por outro lado, se o nível **crítico** for alterado de **13 a 25** para **20 a 25**, significa um **maior** apetite a risco, visto que a organização passou a considerar como **críticos** um menor número de riscos.

A mensuração dos **riscos residuais** efetuada nessa etapa, bem como a **avaliação dos controles internos existentes** para tratar cada um desses riscos, deverão ser registradas em planilha específica conforme modelo a seguir:

MENSURAÇÃO DOS RISCOS RESIDUAIS								
ÓRGÃO / ENTIDADE:								
PROCESSO:								
N.º	**RISCOS**	**RISCO INERENTE (RI)**	**CONTROLE IINTERNO EXISTENTE**	**FATOR DE AVALIAÇÃO DO CONTROLE (FAC)**	**AVALIAÇÃO CONTROLE**	**RISCO RESIDUAL (= RI X FAC)**	**NÍVEL DE RISCO**	**RESPOSTA AO RISCO**
1	xxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxx	**20**	yyyyyyyyyyyyyyyyyyyyyy yyyyyyyyyyyyyyyyyyyyyy	0,20	Forte	**4**	Moderado	
*No exemplo acima, embora o **Risco Inerente (RI)** seja alto, a avaliação do controle existente foi considerada "Forte", correspondendo a um Fator de Avaliação de Controle (FAC) de 0,2 (Quadro 9). Com isso, o **Risco Residual** apurado atingiu 4 (20x0,2), ou "Moderado", havendo uma redução de 80% em relação ao Risco Inerente, indicando que o controle existente mitiga consideravelmente o risco.*								
2								
3								
n								

Figura 10: Planilha Mensuração dos Riscos Residuais

5.6. Resposta ao risco

A estratégia de tratamento ou resposta ao risco possui diretrizes pré-definidas pelo PGR para **orientar** as medidas de tratamento correspondentes a cada nível de risco a serem adotadas pela organização (Quadro 11).

NÍVEL DE RISCO	DESCRIÇÃO	DIRETRIZ PARA RESPOSTA AO RISCO
CRÍTICO	Indica um nível de risco absolutamente inaceitável, muito além do apetite a risco da organização.	Qualquer risco encontrado nessa área deve ter uma resposta imediata do gestor maior da unidade.
ALTO	Indica um nível de risco inaceitável, além do apetite a risco da organização.	Qualquer risco encontrado nessa área deve ter uma resposta num intervalo de tempo definido pelo gestor maior da unidade. Admite-se postergar o tratamento somente mediante manifestação do gestor maior da unidade.
MODERADO	Indica um nível de risco aceitável, dentro do apetite a risco da organização.	Não se faz necessário adotar medidas especiais de tratamento, exceto manter os controles já existentes.
PEQUENO	Indica um nível de risco muito baixo, de baixa ocorrência e impacto reduzido.	Apenas acompanhar para verificar eventual mudança de probabilidade e impacto, sem adotar medidas de controle adicionais.

Quadro 11 - Diretrizes de resposta aos riscos

O gestor do processo pode alterar a diretriz de resposta ao risco, desde que sejam apresentadas justificativas devidamente validadas por instância superior. A organização deverá avaliar o seu **apetite a risco,** que é o **nível de tolerância ao risco que está disposta a assumir** e que deve ser definido antes de deliberar sobre a necessidade de implementar ou não ações de controle, ou seja, as respostas que serão dadas aos riscos (Quadro 12).

A escolha da estratégia de tratamento ou resposta ao risco dependerá do nível de exposição previamente estabelecido em confronto com a avaliação que se fez do risco residual (Faixas dos Riscos Residuais – Quadro 10).

Um mesmo controle ou tratamento pode servir para atuar sobre uma ou várias causas do risco.

RESPOSTA AO RISCO	
TIPO	**EXEMPLO**
MITIGAR	Reduzir a probabilidade, o impacto, ou ambos, através de controles específicos. **É a resposta que deverá ser a mais comum.**
TRANSFERIR	Terceirização; garantia contratual; matriz de riscos contratual; seguro.
EVITAR	Encerrar uma atividade em determinada localidade; não iniciar uma obra por não ter garantia de orçamento; descontinuar a forma de transferência de recursos.
ACEITAR	Evitar instaurar procedimentos de penalização a partir de determinado nível de dano

Quadro 12 – Resposta ao risco

5.7. Elaboração do Plano de Ação

Após definidas pela UA as respostas/tratamentos para cada risco será elaborado **Plano de Ação (PA)**, que se constitui em um conjunto de controles a serem implementados ou revistos para tratar os riscos identificados.

Nesta etapa são concebidas as ações necessárias para tratar os riscos identificados, priorizando-se aquelas voltadas para os riscos/eventos situados nos níveis "**crítico**" e "**alto**", ou seja, na faixa em que o **risco residual** esteja **entre 7 e 25** (Quadro 10).

As "**ações de controle**" correspondem ao que será feito para tratar cada risco, ou seja, no **Plano de Ação** devem ser especificadas as **soluções finais** que serão implementadas ou aperfeiçoadas.

O **Plano de Ação** deverá ser elaborado pelo GT, seguindo os passos abaixo:

<table>
<tr><td rowspan="4">PASSO A PASSO</td><td>Definir e registrar para cada risco:
• Tipo de resposta ao risco;
• Ações de controle interno que serão implementadas ou aperfeiçoadas;
• Prazo;
• Responsável.</td></tr>
<tr><td>Atenção: Devem ser evitadas como “solução final” expressões do tipo “solicitar contratação”, “fazer gestão para adquirir sistema” ou “planejar capacitação”. Usar “contratar”, “adquirir e implantar sistema” ou “capacitar”, que constituem as soluções efetivas propostas em termos de controle interno para tratamento do risco.
Atenção: As ações previstas no Plano de Ação correspondem a macroações que deverão ser desdobradas em planos detalhados pelos seus respectivos responsáveis.</td></tr>
<tr><td>Validar o Plano de Ação em reunião específica com o CGR e encaminhá-lo para aprovação do Dirigente máximo do órgão/entidade.</td></tr>
<tr><td>Efetuar reunião de finalização do respectivo ciclo do PGR, com apresentação dos resultados para os dirigentes e donos do processo.</td></tr>
</table>

O **Plano de Ação** deve ser registrado em planilha específica, conforme modelo a seguir:

<table>
<tr><th colspan="9">PLANO DE AÇÃO (GESTÃO DE RISCOS)</th></tr>
<tr><td colspan="9">ÓRGÃO / ENTIDADE:</td></tr>
<tr><td colspan="9">PROCESSO:</td></tr>
<tr><th>N.º</th><th>RISCOS</th><th>CAUSAS</th><th>RISCO RESIDUAL</th><th>NÍVEL DO RISCO RESIDUAL</th><th>RESPOSTA AO RISCO</th><th>AÇÃO DE CONTROLE (o que será feito)</th><th>PRAZO (quando será feito)</th><th>RESPONSÁVEL (quem fará)</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx xxxxxx</td><td>aaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaa aaaaaa</td><td rowspan="2">4</td><td rowspan="2">Moderado</td><td rowspan="2">Mitigar</td><td>zzzzzzzzzzzzzzzzzzzz zzzzzzzzzzzzzzzzzzzz zzzzzzzzzzzzzzzzzzzz zzzzzzzzzzzzzzzzzzzz</td><td>Até mm/aa</td><td>Juarez Silva</td></tr>
<tr><td>bbbbbbbbbbbbbbbbb bbbbbbbbbbbbbbbbb bbbb</td><td>yyyyyyyyyyyyyyyyyyyyyy yyyyyyyyyyyyyyyyyyyyyy yyyyyyyyyyyy</td><td>Até mm/aa</td><td>José Souza</td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">n</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figura 11: Planilha do Plano de Ação

5.7.1. Implementação e monitoramento do Plano de Ação (PA)

Ao “**dono do processo**” caberá, coordenar a efetiva implementação do Plano de Ação e o contínuo monitoramento do processo para verificar a necessidade de revisão e identificar eventuais novos riscos decorrentes de mudanças de

legislação e normas, alterações nos fluxos dos processos ou nos sistemas de tecnologia de informações, ou qualquer outra condição que altere o nível de exposição a riscos.

O monitoramento do Plano de Ação deve ser conduzido pela **Coordenação de Controle Interno (CCI)** ou unidade equivalente, que ficará responsável pelo acompanhamento de sua execução, visando aferir se as ações planejadas de tratamento dos riscos estão sendo implementadas nos prazos previstos e estão sendo eficazes.

A Coordenação de Controle Interno (CCI) ou unidade equivalente deverá incluir em seu planejamento anual o acompanhamento do **Plano de Ação da Gestão de Riscos** e reportar à AGE, no Relatório Anual de Atividades (RAA), avaliação do andamento do Programa de Gestão de Riscos como um todo, inclusive apontando os resultados alcançados em termos de tratamento dos riscos, em função das medidas e controles internos implantados.

A AGE manterá, junto à Coordenação de Controle Interno (CCI) ou unidade equivalente, monitoramento contínuo a partir do início da implantação do Plano de Ação, podendo solicitar, a qualquer tempo, informações sobre o andamento da sua execução.

O **fluxo básico** das etapas da metodologia da gestão de riscos está resumido na Figura 12:

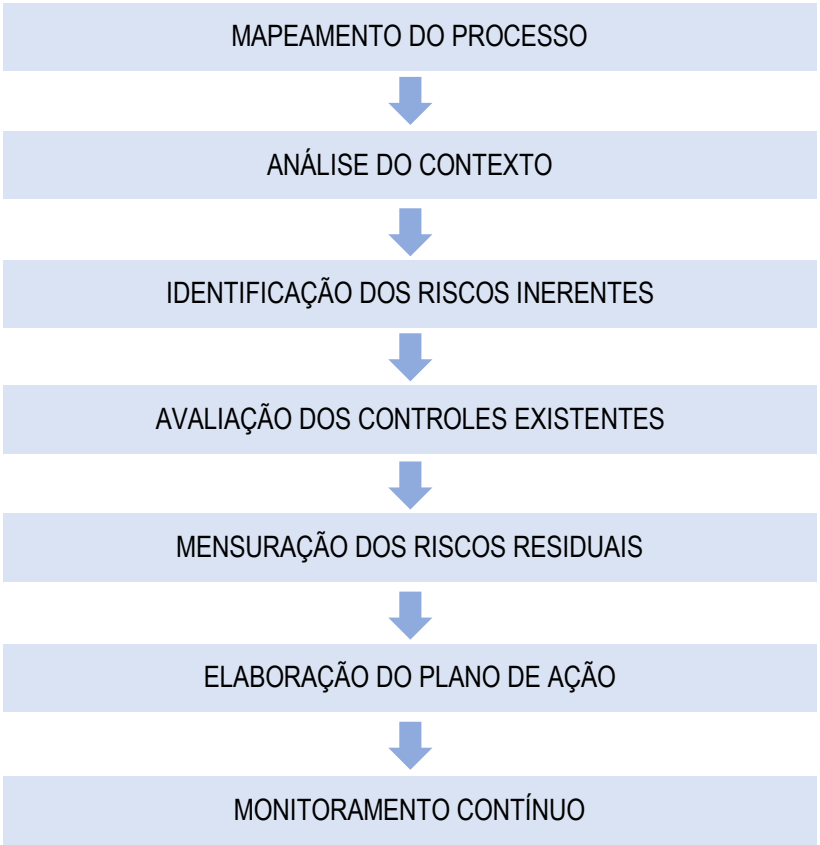


Figura 12: Fluxo básico das etapas da metodologia da Gestão de Riscos

5.8. Matriz de Responsabilidades

O Programa de Gestão de Riscos (PGR) estabelece uma **Matriz de Responsabilidades** para os entes envolvidos no processo de sua implantação, de acordo com o nível de maturidade da organização estabelecido no Quadro 2.

MATRIZ DE RESPONSABILIDADES							
Responsável	**Nível de Maturidade**	**Análise de contexto**	**Identificação dos riscos**	**Mensuração dos riscos inerentes**	**Identificação/ avaliação dos controles internos**	**Mensuração dos riscos residuais**	**Plano de Ação**
AGE/GEPRE	N1 (Inicial)	Assessora	Assessora	Assessora	Assessora	Assessora	Assessora e Monitora
	N2 (Intermediário)	-	Avalia	-	-	Avalia	Avalia e Monitora
	N3 (Avançado)	-	-	-	-	Ciência	Ciência
CGR	N1 (Inicial)	Valida	Valida	Valida	Valida	Valida	Valida
	N2 (Intermediário)	-	-	-	-	Valida	Valida
	N3 (Avançado)	-	-	-	-	-	Valida
GT	N1, N2 e N3	Executa	Executa	Executa	Executa	Executa	Propõe
CCI	N1, N2 e N3	Acompanha	Acompanha	Acompanha	Acompanha	Acompanha	Acompanha e Monitora
Dono do processo	N1, N2 e N3	-	-	-	-	Valida	Valida
Dirigente da UA	N1, N2 e N3	-	-	-	-	-	Aprova

Quadro 13 – Matriz de Responsabilidades

6. Glossário de termos técnicos sobre Gestão de Riscos

1. ***Accountability***: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações.
2. **Apetite a risco**: nível de risco que uma organização está disposta a tolerar. Está relacionado à predisposição da organização em assumir determinados níveis de exposição a riscos.
3. **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 de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:
   - Cumprimento das leis e regulamentos aplicáveis;
   - Cumprimento das obrigações de *accountability*;
   - Execução ordenada, ética, econômica, eficiente e eficaz das operações.
4. **Diagrama Bowtie**: ferramenta utilizada para apresentar graficamente a sintaxe do risco. É uma maneira esquemática simples para descrever e analisar o risco, desde as suas causas até suas consequências, servindo para testar a coerência do risco (**devido à causa "x", poderá ocorrer o risco "y", que poderá levar ao efeito "z"**). Se um risco não se enquadrar de forma coerente nessa sintaxe, deverá ser revisto e reformulado.
5. **Dono do Processo:** gestor regimentalmente responsável pelo gerenciamento das atividades relacionadas ao processo objeto da Gestão de Riscos.
6. **Fatores de riscos:** são condições que dão origem à possibilidade de um evento acontecer. São também chamados de **fontes de risco**, que associadas às **vulnerabilidades,** dão origem às **causas** dos riscos (**causa = fonte de risco + vulnerabilidades**). Podem estar representados por ***pessoas*** (sem capacitação; com perfis inadequados; desmotivadas; sem idoneidade p.ex), ***processos*** (mal concebidos; sem procedimentos formalizados; sem segregação de funções etc), ***sistemas*** (obsoletos; sem integração; sem funcionalidades de controle de acesso e rastreabilidade etc), ***infraestrutura organizacional*** (centralização/descentralização excessiva; falta de matriz de responsabilidades; delegações exorbitantes; descoordenação; falta de indicadores de desempenho etc) ou ***infraestrutura física*** (localização inadequada; instalações e leiaute inadequados; inexistência de controle de acesso etc)
7. **Fraude**: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança.
8. **Mensuração de risco**: significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência.
9. **Processo**: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.

10. **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.
11. **Risco estratégico**: é aquele que tem a capacidade de impactar diretamente os objetivos estratégicos da organização, podendo a chegar a ameaçar sua sobrevivência (ex: mudanças no rumo da economia; alterações na legislação; rupturas tecnológicas; mudança de hábito dos consumidores etc).
12. **Risco de imagem**: é aquele relacionado a eventos que possam afetar a credibilidade e a reputação da organização (ex: descoberta de fraudes e atos de corrupção; contaminação de produtos; defeitos de fabricação de produtos que possam levar a acidentes; publicação extraordinária de decisão condenatória; falsificação ou não divulgação de informações relevantes etc).
13. **Risco de regulação**: relacionado a eventos que podem propiciar ações sancionatórias contra a organização por parte de órgãos e instâncias reguladoras (ex: multas por descumprimento de normas; suspensão de funcionamento; proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas; proibição de contratação etc).
14. **Risco operacional**: é aquele que tem a capacidade de impactar diretamente os objetivos dos processos operacionais da organização (ex: panes de sistemas; quebra de equipamentos; suspensão de fornecimento de matérias primas e insumos; superfaturamento de contratos etc).
15. **Risco financeiro**: é aquele que tem a capacidade de impactar diretamente as finanças da organização (ex: perda de arrecadação; fraudes; fluxo de caixa negativo; perda de ativos etc).
16. **Risco inerente**: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais (controles) que possam reduzir a probabilidade de sua ocorrência ou seu impacto.
17. **Risco residual**: risco a que uma organização está exposta após a implementação de ações gerenciais (controles) para o tratamento do risco.
18. **Riscos de integridade**: são aqueles relacionados a ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção (ex: recebimento/oferta de propina, desvio de verbas, abuso de poder, nepotismo, conflito de interesses, uso indevido e vazamento de informação sigilosa e outras práticas antiéticas). Essas situações tendem a ser observadas nos processos/áreas em que há manifesto interesse privado sobre os seus produtos (compras vultosas, multas, fiscalizações, licenciamentos, cobrança de taxas, aprovação de crédito, manipulação de dados e informações privilegiadas, etc).
19. **Unidade Aderente (UA)**: órgão/entidade que aderir ao Programa de Gestão de Riscos, nos termos da Portaria Sefaz nº 162/2018.