



ORIENTAÇÃO TÉCNICA AGE Nº 01/2023 (Revisão 1)

PROGRAMA DE GESTÃO DE RISCOS

I. INTRODUÇÃO

A presente Orientação Técnica - OT substitui a OT AGE n.º 02/2020, que orienta o processo de implantação do Programa de Gestão de Riscos (PGR), no âmbito dos órgãos e entidades do Poder Executivo do Estado da Bahia.

II. OBJETIVOS

1. Estabelecer normas gerais de procedimentos e práticas para implantação do Programa de Gestão de Riscos (PGR), instituído pela Portaria SEFAZ n.º 162/2018, junto aos órgãos e entidades do Poder Executivo do Estado da Bahia;
2. Disseminar a cultura da Gestão de Riscos e sua metodologia;
3. Estabelecer um guia de implantação do Programa de Gestão de Riscos (PGR), auxiliando gestores e colaboradores a mitigar e controlar riscos.

III. BASE NORMATIVA

1. Decreto Federal n.º 9.203, de 22 de novembro de 2017;
2. Portaria SEFAZ n.º 162 de 13 de agosto de 2018;
3. ABNT ISO GUIA 73:2009;
4. Norma ABNT NBR ISO 31010:2012;
5. Norma ABNT NBR ISO 31004:2015;
6. Norma ABNT NBR ISO 31000:2018;
7. Instrução Normativa Conjunta MP/CGU n.º 01, de 10/05/2016;
8. Committee of Sponsoring Organizations of the Treadway Commission – COSO 2013 - Internal Control - Integrated Framework (ICIF);
9. Orientação Técnica AGE n.º 01/2017 - Guia Referencial dos Controles Internos da Gestão.

IV. PROGRAMA DE GESTÃO DE RISCOS - PGR

1. O Programa de Gestão de Riscos (PGR) foi instituído na Bahia em 2018, através da Portaria SEFAZ n.º 162, sob a coordenação da Auditoria Geral do Estado (AGE), e apresenta uma metodologia reconhecida como boa prática de aperfeiçoamento da gestão para atingimento dos objetivos estratégicos da Organização.
2. O PGR é instrumento de governança e liderança sendo indispensável contar com o patrocínio e o apoio do dirigente máximo da organização, a fim de assegurar que seus objetivos sejam plenamente alcançados.



3. Durante a implantação do Programa¹, eventuais trabalhos de auditoria da AGE que tenham como escopo o objeto em que está sendo aplicado o PGR ficarão suspensos.
4. A exceção se fará para os seguintes casos:
 - a) Aqueles oriundos de denúncias;
 - b) Solicitação do próprio dirigente da Secretaria/Órgão;
 - c) Indícios de inconformidades identificados em procedimentos de varredura e análises exploratórias;
 - d) Critérios específicos de seleção utilizados na programação da Auditoria Geral do Estado – AGE.
5. A metodologia adotada 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 uma ferramenta prática, de fácil aplicação e que oferece melhoria na governança da organização, permitindo maior previsibilidade e prevenindo a ocorrência de eventos negativos.
6. A adesão ao PGR deverá ser formalizada junto a Auditoria Geral do Estado (AGE) pelo dirigente máximo de cada Secretaria/Órgão, mediante ofício tramitado no sistema oficial de gestão de processos e documentos administrativos eletrônicos e digitais – SEI BAHIA.
7. No âmbito do Programa de Gestão de Riscos é disponibilizada capacitação sobre o tema, destinada aos servidores do Estado da Bahia. A capacitação, parte integrante do PGR, tem como objetivos:
 - a) Sensibilizar os participantes para a importância da Gestão de Riscos no âmbito da Administração Pública Estadual;
 - b) Capacitar os servidores para implantação do Programa de Gestão de Riscos (PGR), aperfeiçoando suas percepções sobre os riscos aos quais suas organizações estão submetidas e dotando os participantes dos instrumentos metodológicos e conceitos sobre o tema;
 - c) Nivelar conceitualmente os participantes.
8. A unidade que formalizar a adesão ao PGR junto a AGE/SEFAZ deverá constituir um Comitê de Gestão de Riscos (CGR), de caráter permanente, que se reportará diretamente ao seu dirigente máximo.

¹ Esse período se estende até a implantação das medidas previstas no Plano de Controle, não devendo ultrapassar 2 anos da data de realização da reunião de encerramento do Programa.



9. O CGR será constituído através de instrumento formal (portaria, p.ex.) expedido pelo dirigente máximo da Secretaria/Órgão, reportado à AGE via SEI, e terá a seguinte composição:
 - a) O Coordenador da Coordenação de Controle Interno (CCI) ou unidade setorial equivalente, que o coordenará;
 - b) Um representante da Assessoria de Planejamento e Gestão (APG) ou unidade equivalente;
 - c) Um representante da Assessoria do dirigente máximo do órgão.

10. O CGR possui as seguintes competências:
 - a) Definir o objeto do Programa;
 - b) Indicar os integrantes do(s) Grupo(s) de Trabalho (GTs), com perfil, conhecimento e disponibilidade para participar do desenvolvimento das atividades;
 - c) Fomentar a capacitação dos servidores em Gestão de Riscos;
 - d) Acompanhar os trabalhos dos GTs por meio de reuniões periódicas;
 - e) Validar o trabalho efetuado pelos GTs, em especial a Listagem de Riscos e o Plano de Controle elaborados;
 - f) Articular com o Dirigente máximo da unidade a indicação dos responsáveis pela implantação do Plano de Controle;
 - g) Estabelecer política de reavaliação periódica do Programa e monitorar continuamente o seu desenvolvimento;
 - h) Reportar à Auditoria Geral do Estado (AGE) todas as ações voltadas para a Gestão de Riscos;
 - i) Promover ações para disseminar internamente a cultura de Gestão de Riscos.

11. A unidade deverá constituir, ainda, Grupos de Trabalho (GTs) temporários, que atuarão diretamente nas etapas de aplicação da metodologia, dentro de cada objeto a ser analisado.

12. O GT deve ser reportado à AGE via SEI e terá a seguinte composição:
 - a) Servidores responsáveis pelo objeto analisado e que detenham conhecimento acerca dos seus aspectos técnicos e indicados pelo CGR, com perfil, conhecimento e disponibilidade para participar de reuniões e desenvolvimento dos trabalhos;
 - b) Um representante da Coordenação de Controle Interno (CCI) ou unidade setorial equivalente.

13. O GT possui as seguintes competências:
 - a) Participar das atividades e etapas do Programa de Gestão de Riscos (PGR) relacionadas ao objeto analisado;
 - b) Mapear e analisar o objeto da Gestão de Riscos;
 - c) Identificar e avaliar os riscos do objeto e propor ações mitigatórias;



d) Revisar os produtos elaborados, reunindo-se internamente com os seus membros.

14. O Programa de Gestão de Riscos (PGR) estabelece Matriz de Responsabilidades para os entes envolvidos no processo de sua implantação, conforme quadro abaixo^(alterado na rev.1):

UNIDADE RESPONSÁVEL	ATRIBUIÇÃO
AGE/GEPRE	Assessora sob demanda a aplicação do PGR
CGR	Acompanha, avalia e valida todas as etapas do PGR Valida o Plano de Controle
GT	Executa todas as etapas do PGR
CCI ou unidade equivalente	Acompanha todas as etapas do PGR Monitora o Plano de Controle
DIRIGENTE ÓRGÃO/SECRETARIA	Aprova o Plano de Controle

15. O Plano de Controle de Gestão de Riscos é o produto final do PGR e deve ser monitorado pela Coordenação de Controle Interno (CCI) ou unidade setorial equivalente, que ficará responsável pelo acompanhamento da sua execução e implantação das medidas mitigatórias.

16. A Coordenação de Controle Interno (CCI) ou unidade setorial equivalente incluirá em seu planejamento anual o acompanhamento desse Plano de Controle, reportando à AGE os resultados alcançados no Relatório Anual de Atividades (RAA).

17. A AGE manterá, junto à Coordenação de Controle Interno (CCI) ou unidade setorial equivalente monitoramento contínuo até a sua finalização, podendo solicitar, a qualquer tempo, informações sobre o andamento da sua execução.

V. DISPOSIÇÕES FINAIS

A AGE/SEFAZ publica, juntamente com esta Orientação Técnica, o **Guia de Aplicação do Programa de Gestão de Riscos – PGR**, parte integrante desse instrumento, contendo as etapas que compõem a sua metodologia, seus objetivos, conceitos e princípios que norteiam a gestão de riscos, sendo destinado aos agentes e gestores das organizações públicas do Poder Executivo do Estado da Bahia.



Salvador, 17 de junho de 2024

Documento assinado digitalmente
gov.br VITOR RIBEIRO PINHEIRO GONCALVES
Data: 14/06/2024 16:14:54-0300
Verifique em <https://validar.iti.gov.br>

Vítor Ribeiro Pinheiro Gonçalves

Gerente de Controle Preventivo e Transparência

Documento assinado digitalmente
gov.br LUIS AUGUSTO PEIXOTO ROCHA
Data: 17/06/2024 09:51:38-0300
Verifique em <https://validar.iti.gov.br>

Luis Augusto Peixoto Rocha

Auditor Geral do Estado



SECRETARIA DA
FAZENDA

AUDITORIA GERAL
DO ESTADO

GUIA DE APLICAÇÃO DO PROGRAMA DE GESTÃO RISCOS - PGR

SECRETARIA DA FAZENDA DO ESTADO DA BAHIA (SEFAZ)

AUDITORIA GERAL DO ESTADO DA BAHIA (AGE)



SECRETARIA DA
FAZENDA

AUDITORIA GERAL
DO ESTADO

SECRETÁRIO DA FAZENDA

Manoel Vitório da Silva Filho

AUDITOR GERAL DO ESTADO

Luís Augusto Peixoto Rocha

GERENTE DE CONTROLE PREVENTIVO E TRANSPARÊNCIA

Vítor Ribeiro Pinheiro Gonçalves

EQUIPE TÉCNICA GEPRE

Ana Luiza Sodré de Aragão Vasconcellos

Cristiane Márcia Veloso de Carvalho

Rachel Valença

PROGRAMAÇÃO VISUAL E CONTEÚDO GEPRE

FICHA TÉCNICA

Guia de aplicação do Programa de Gestão de Riscos (PGR). Parte integrante da OT nº 01/2023. Estabelece normas gerais de procedimentos e práticas para implantação do Programa de Gestão de Riscos (PGR), junto aos órgãos e entidades do Poder Executivo do Estado da Bahia. Secretaria da Fazenda (SEFAZ). Auditoria Geral do Estado da Bahia (AGE).

**5ª VERSÃO
JUNHO - 2024**

HISTÓRICO DE REVISÕES

VERSÃO	DATA	DESCRIÇÃO
1	01/04/2020	Elaboração do Documento
2	23/03/2021	Revisão do documento: Incorpora informações relacionadas ao suporte tecnológico (Sistema Ágatha)
3	11/02/2022	Revisão do documento: Incorpora modificações na metodologia
4	10/02/2023	Revisão do documento: Incorpora modificações na metodologia Incorpora alterações relacionadas ao suporte tecnológico (Sistema Ágatha)
5	14/06/2024	Revisão do documento: Incorpora modificações na metodologia Incorpora planilhas automatizadas em substituição ao suporte suporte tecnológico anteriormente utilizado (Sistema Ágatha)

SUMÁRIO

1. INTRODUÇÃO	4
2. RISCOS.....	4
2.1. COMPONENTES DO RISCO	6
2.2. RISCOS ESTRATÉGICOS E OPERACIONAIS.....	6
2.3. RISCOS DE INTEGRIDADE	8
2.4. INTEGRIDADE PÚBLICA	9
3. CONTROLES INTERNOS	9
3.1. TIPOS DE CONTROLES	10
4. GESTÃO DE RISCOS	13
4.1. GOVERNANÇA E GESTÃO DE RISCOS.....	13
4.2. BENEFÍCIOS ESPERADOS	15
4.3. MITOS SOBRE A GESTÃO DE RISCOS	16
5. PROGRAMA DE GESTÃO DE RISCOS (PGR).....	17
5.1. METODOLOGIA	17
5.2. SELEÇÃO DO OBJETO.....	18
5.3. ETAPAS DO PGR.....	19
5.4. COMUNICAÇÃO E MONITORAMENTO	32
5.5. PASSO A PASSO PARA IMPLANTAÇÃO DO PGR.....	33
6. TERMOS E DEFINIÇÕES.....	33
7. CONCLUSÃO	35
8. REFERENCIAIS.....	36

1. INTRODUÇÃO

A Gestão de Riscos é uma prática de gestão voltada para aperfeiçoar o processo de planejamento das Organizações, buscando antever os possíveis riscos que possam interferir nos seus objetivos, não devendo ser encarada como um projeto complementar, nem uma tarefa de verificação da lista de afazeres. Deve estar sempre em curso e tornar-se parte da cultura global de continuidade da missão do órgão ou entidade.

Como definida no Decreto Federal n.º 9.203, de 22 de novembro de 2017, é um processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla atividades de **identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização**, destinado a fornecer segurança razoável quanto à realização de seus **objetivos** (Art. 2º, IV).

A Gestão de Riscos auxilia o gestor a antecipar, identificar e lidar com situações de risco e a se preparar para enfrentá-las, elaborando um plano de respostas, sendo um sinal de maturidade gerencial e elemento importante para a boa governança.

Também 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.

A metodologia aplicada fornece uma abordagem comum para gerenciar qualquer tipo de risco ou atividade. Embora cada órgão ou entidade possua objetivos próprios e especificidades todos tem algo em comum: os **riscos**.

2. RISCOS

As atividades de qualquer organização envolvem **riscos** que, se não gerenciados, podem se materializar e comprometer a capacidade de **gerar, preservar ou entregar valor** e, no contexto governamental, podem ter impactos de grande escala.

O conceito atual de riscos envolve a quantificação e qualificação da incerteza no que diz respeito a ganhos ou perdas, com relação ao rumo dos acontecimentos planejados pelas organizações.

Abaixo estão relacionados alguns **conceitos de Risco**:

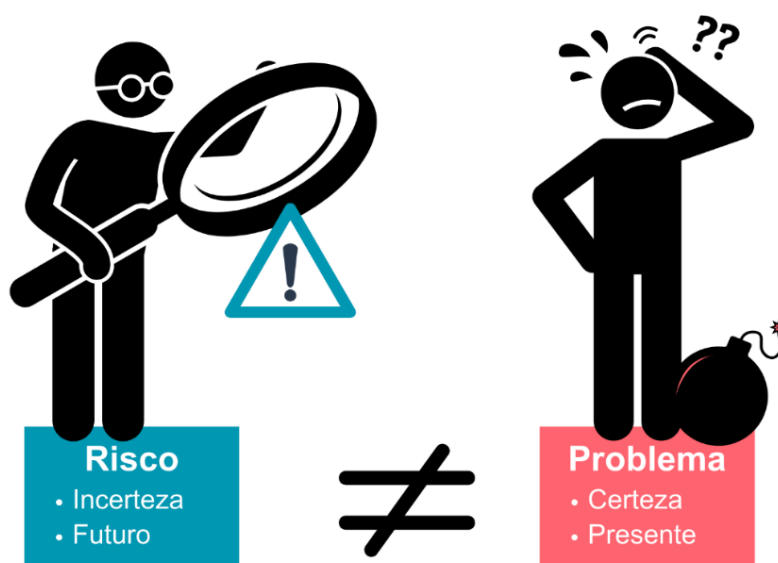
- Efeito da incerteza sobre os objetivos (ABNT NBR ISO 31000:2018).
- Evento futuro e incerto, que caso ocorra, pode impactar negativamente o alcance dos objetivos da organização (COSO II - Committee of Sponsoring Organizations).
- Possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos (Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016).
- Possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades (TCU IN 63/2010)



Notas de entrada:

- Um efeito é um desvio em relação ao esperado.
- Incerteza refere-se à deficiência, mesmo que parcial, das informações relacionadas a um evento.
- Evento é a ocorrência ou mudança em um conjunto específico de circunstâncias.

O risco, portanto, é um evento ou **condição futura e incerta** que, se ocorrer, provocará um efeito, ou seja, um impacto em um determinado objetivo. Esta afirmação deixa claro que risco é incerteza, o que significa dizer que é algo que ainda não aconteceu. Um risco, quando se concretiza, torna-se um **problema**.



2.1. COMPONENTES DO RISCO

O risco possui 3 elementos básicos na sua composição:

CAUSA: Condição que possibilita um evento de risco acontecer e pode ter origem no ambiente interno ou externo. É uma conjunção de fontes e vulnerabilidades. A fonte do risco é um elemento que, sozinho ou combinado, pode dar origem ao risco (pessoas, processos, sistemas, infraestrutura, externalidades, etc.). Vulnerabilidades são inexistências, inadequações ou deficiências.

EVENTO: Ocorrência ou mudança em um conjunto específico de circunstâncias.

CONSEQUÊNCIA: Resultado da materialização de um evento de risco que afete os objetivos.



2.2. RISCOS ESTRATÉGICOS E OPERACIONAIS

Riscos estratégicos em organizações públicas são aqueles que afetam diretamente a missão, visão e objetivos da instituição. São riscos de longo prazo que, uma vez materializados em eventos, afetam de maneira decisiva a consecução de um ou mais objetivos estratégicos e representam a possibilidade de ocorrerem perdas pelo insucesso das estratégias adotadas.

Estes riscos podem incluir mudanças políticas, econômicas e sociais, além de fatores internos como falta de liderança adequada, ausência de planejamento estratégico, falhas de comunicação e cultura organizacional disfuncional.

São ainda denominados **riscos-chave**, em função do impacto potencial e das sérias consequências que podem trazer para a organização, comprometendo a sua eficácia e prejudicando a capacidade de fornecer serviços e soluções aos cidadãos.

Os riscos constituem insumo para o diagnóstico institucional do processo de planejamento estratégico. Ao se formular a estratégia institucional, deverão ser considerados os riscos intrínsecos àquela estratégia (COSO 2017).

Por encontram-se intrinsecamente ligados à missão e visão organizacionais, os riscos estratégicos são de responsabilidade da **alta direção**, que deverá tomar as decisões necessárias no que se refere ao seu gerenciamento. Caso o risco não seja mitigado poderá prejudicar ou comprometer a entrega dos produtos, bens e/ou serviços aos cidadãos.

O **Risco operacional** é estabelecido como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou eventos externos.

Esse tipo de risco está relacionado aos processos organizacionais executados pelos responsáveis pelas atividades cotidianas das instituições e precisam ser gerenciados de forma a criar ações de defesa quanto a possíveis ameaças.

Esses riscos precisam ser acompanhados de forma ininterrupta, objetivando a melhoria contínua dos processos do órgão ou entidade.

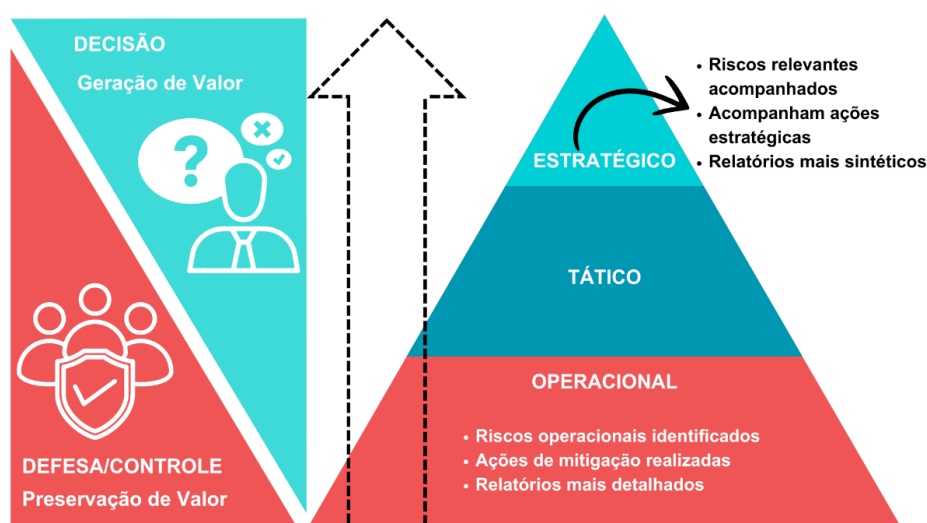


Figura: Dualidade do risco. Adaptado BACEN

2.3. RISCOS DE INTEGRIDADE

Nas organizações existem situações, processos e áreas em que há um risco maior do interesse privado sobrepor-se ao interesse público e, portanto, deve-se conhecer previamente quais são essas circunstâncias para buscar formas de evitá-las ou mitigá-las.

Neste contexto, o PGR constitui também em importante mecanismo para atenuar os Riscos de Integridade, identificando ações ou omissões que possam favorecer a 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.

De acordo com a Portaria CGU nº 1.089/2018, **Riscos de Integridade** são aqueles que configuram ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

Quando esses riscos se materializam ocorre o que usualmente é conhecido como “quebra de integridade”, expressão que engloba atos como recebimento ou oferta de propina, desvio de verbas, fraudes, abuso de poder, nepotismo, conflito de interesses, uso indevido e vazamento de informação sigilosa e todas as práticas consideradas antiéticas.

De um modo geral, atos relacionados a quebras de integridade compartilham as seguintes características:

- É um ato quase sempre doloso, ou seja, um ato intencional no qual o agente quis ou assumiu o resultado;
- É um ato humano, praticado por uma pessoa ou por um grupo de pessoas;
- Envolve uma afronta aos princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência, mas se destaca mais fortemente como uma quebra à impessoalidade e/ou moralidade;
- Envolve alguma forma de deturpação, desvio ou negação da finalidade pública ou do serviço público a ser entregue ao cidadão.

Os riscos de integridade podem ocorrer em processos em que há **manifesto interesse privado** sobre os seus produtos e serviços.

Exemplos:

- compras e contratações, em especial as de grande vulto;
- análise e julgamento de contenciosos administrativos e judiciais;
- credenciamento de prestadores de serviços;
- liberação de licenças.

Podem ocorrer também em processos relacionados a serviços públicos prestados aos cidadãos cuja **demanda seja maior que a oferta** ou, ainda, em processos relacionados com administração do **poder sancionatório, regulatório ou de polícia**.

Exemplos:

- concessão de bolsas e benefícios sociais;
- ordenamento de filas de acesso em geral;
- fiscalização, aplicação de multas e lavratura de autos de infração;
- elaboração de normas e regulamentos sobre atividades econômicas.

2.4. INTEGRIDADE PÚBLICA

Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a **Integridade pública** 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 nas instituições governamentais.

É um pilar essencial para o funcionamento eficaz e legítimo das instituições governamentais e refere-se à conduta ética e transparente de funcionários e organizações no exercício de suas funções. Isso envolve a honestidade, imparcialidade e responsabilidade na tomada de decisões, garantindo a confiança dos cidadãos nas instituições públicas.

De acordo com o Guia de Integridade Pública da CGU (2015), Integridade Pública é o conjunto de arranjos institucionais que visam fazer com que a Administração Pública não se desvie de seu objetivo principal: entregar os resultados esperados pela população de forma adequada, imparcial e eficiente.

3. CONTROLES INTERNOS

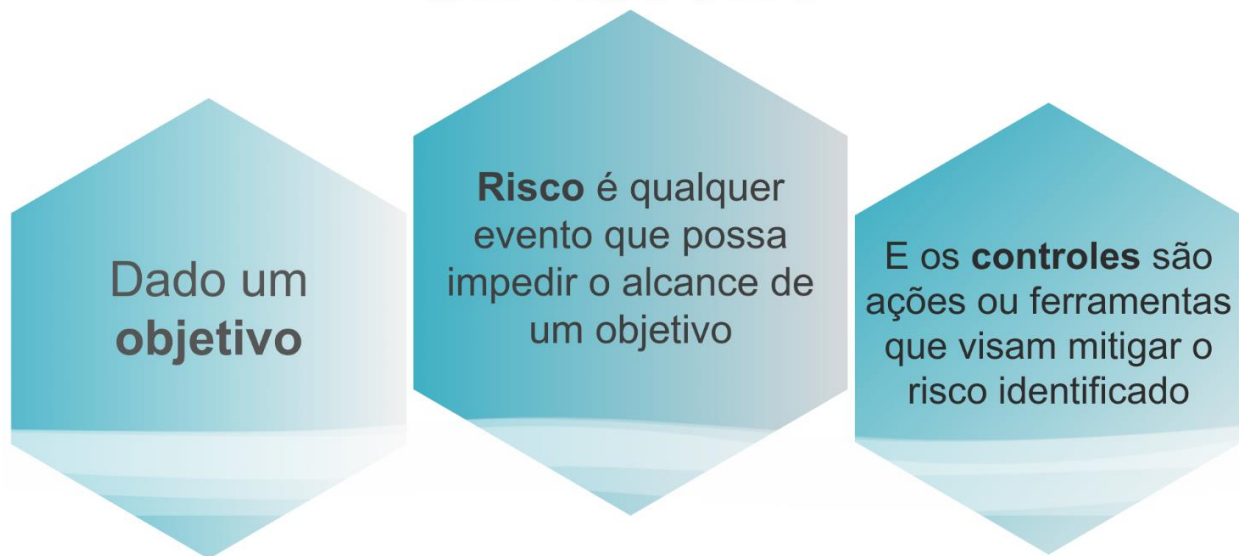
Controle interno é um processo realizado pela organização, em todos os níveis da entidade, projetado para fornecer segurança razoável quanto à consecução de objetivos nas seguintes categorias:

- Execução ordenada, ética, econômica, eficiente e eficaz;
- Em cumprimento das obrigações de *accountability*;
- Cumprimento das leis e regulamentos aplicáveis;
- Salvaguarda dos recursos para evitar perdas, mau uso e danos.

Refere-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).

Portanto, os controles são instrumentos para **mitigação de riscos** e representam uma **rede de proteção** contra danos, perdas, desvios, etc.

EM RESUMO



3.1. TIPOS DE CONTROLE

Os controles objetivam melhorar o controle existente ou adotar um controle novo e são de dois tipos:

- a) **Preventivo**: tem como objetivo prevenir a materialização do evento de risco. Visa evitar a ocorrência de desvios ou não conformidades. Via de regra atua sobre a causa do evento de risco.

Ex. *Checklist*

b) **Corretivo:** tem como objetivo mitigar evento que já ocorreu. Acionado após a identificação de desvios para corrigir a situação e evitar repetições. Atua sobre a consequência do evento e atenua seu efeito, caso se materialize.

Ex. Plano de contingência

Segue abaixo uma lista (não exaustiva) contendo exemplos de controles:

- **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.
- **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).
- **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).
- **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).
- **Plano 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.
- **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.
- **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:** 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.
- **Visitas ou vistorias *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).

4. GESTÃO DE RISCOS

De acordo com a NBR ISO 31000:2018 a Gestão de Riscos corresponde às atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

Trata-se de um processo sistemático desenvolvido para:

- a) **Identificação de riscos:** encontrar, reconhecer e descrever riscos que possam impedir que uma organização alcance seus objetivos.
- b) **Análise de Riscos:** compreender a natureza dos riscos e suas características.
- c) **Tratamento dos riscos:** selecionar e implementar opções para abordar riscos.

Para o TCU, a gestão de riscos consiste em um “conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. É o processo que visa conferir razoável segurança quanto ao alcance dos objetivos” (TCU, 2018, apud VIEIRA e BARRETO, 2019, p. 100).

Para a CGU – Controladoria-Geral da União, a Gestão de Riscos consiste na arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente. Trata-se de um sistema institucional de natureza permanente, estruturado, monitorado e direcionado às atividades de identificar, analisar e avaliar riscos, decidir sobre estratégias de resposta e ações para tratamento desses riscos, além de monitorar e comunicar sobre o processo de gerenciamento desses riscos, com vistas a apoiar a tomada de decisão, em todos os níveis, e ao efetivo alcance dos objetivos da Organização (Metodologia de Gestão de Riscos, 2018).

4.1. GOVERNANÇA E GESTÃO DE RISCOS

De acordo com o Referencial básico de Governança do TCU (3ª ed.2020) governança pública compreende essencialmente os 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.

A integração da gestão de riscos à governança corporativa aparece em diversos modelos de melhores práticas, incluindo o modelo das três linhas. Este modelo é uma forma simples de mostrar o papel da gerência operacional e do controle interno como a primeira linha, da gestão de riscos como a segunda linha e da auditoria interna como a terceira linha. Cada uma dessas linhas desempenha um papel distinto dentro do processo de

governança corporativa. O modelo mostra, também, o papel dos órgãos de governança e da alta administração como supervisores da atuação das linhas de defesa.


A gestão de riscos é uma das principais ferramentas na governança corporativa. A governança fornece os requisitos de estrutura e direção necessários para que uma organização consiga atingir seus objetivos e gerenciar apropriadamente suas operações, ao passo que a gestão de riscos fornece as políticas e procedimentos necessários para que a organização opere com efetividade em um ambiente mutável e incerto.

O Modelo das Três Linhas do The Institute of Internal Auditors (IIA) é uma estrutura conceitual projetada para ajudar as organizações a entender e aprimorar seus processos de gerenciamento de riscos, controle e governança. Ele fornece uma estrutura para entender como diferentes partes interessadas dentro de uma organização desempenham papéis distintos na gestão eficaz de riscos e controles.

O Modelo das Três Linhas do The IIA



Figura – Modelo das Três Linhas do The Institute of Internal Auditors (IIA)

- 
- a) **Primeira Linha (Unidade de Negócios):** A primeira linha é composta pelas atividades operacionais e pela gestão dos riscos diários dentro da organização. Isso inclui a atuação de gerentes de negócio, equipes operacionais e todos aqueles que têm responsabilidade direta pela realização das operações e pela gestão dos riscos associados a essas atividades. A primeira linha é responsável por identificar, avaliar e gerenciar proativamente os riscos em suas operações diárias.
- b) **Segunda Linha (Gerenciamento de Riscos e Compliance):** A segunda linha é composta por funções de gerenciamento de riscos, conformidade e controle interno. Essas funções fornecem orientação, supervisão e suporte à primeira linha na identificação, avaliação e mitigação de riscos. Elas garantem que os controles sejam eficazes e que a organização esteja em conformidade com as leis, regulamentos e políticas internas aplicáveis. A segunda linha também é responsável por monitorar continuamente o ambiente de riscos e garantir que os processos de gerenciamento de riscos estejam alinhados com os objetivos estratégicos da organização.
- c) **Terceira Linha (Auditoria Interna):** A terceira linha é representada pela função de auditoria interna. A auditoria interna fornece uma avaliação independente e objetiva dos processos de gerenciamento de riscos, controle e governança da organização. Ela avalia a eficácia dos controles internos, identifica áreas de melhoria e fornece recomendações para fortalecer os processos de gestão de riscos e controles. A auditoria interna também desempenha um papel importante na prestação de contas aos órgãos de governança e na comunicação de questões importantes às partes interessadas.

4.2. BENEFÍCIOS ESPERADOS

- Aumenta probabilidade de atingir objetivos;
- Auxilia no processo de tomada de decisão;
- Estimula gestão proativa (em vez de reativa);
- Melhora a governança, o controle interno da gestão e a qualidade do gasto público;
- Melhora a prevenção de perdas, fraudes e a gestão de incidentes;
- Preza pelas conformidades legal e normativa dos processos organizacionais.

4.3. MITOS SOBRE A GESTÃO DE RISCOS

Alguns mitos sobre a gestão de riscos devem ser abordados, pois eles distorcem a percepção da implantação desta prática administrativa.

- **Mais uma tarefa, vai aumentar o meu volume de trabalho:** A gestão de riscos é relativamente simples, prática e deve ser incorporada aos processos de trabalho e não ser algo mais a ser feito.
- **A gestão de riscos é um desperdício de tempo:** Investe-se uma quantidade de tempo, porém o tempo economizado depois é muito maior. A gestão de riscos aumenta a capacidade realizadora das organizações.
- **O que não conhecemos não vai nos machucar:** Esse mito sugere que ignorar riscos desconhecidos é seguro. Na realidade, os riscos podem impactar negativamente uma organização, mesmo que não estejamos cientes deles. Não conhecer o risco pode custar muito caro.
- **Os riscos podem ser totalmente evitados:** Não existe risco zero, pois o risco não pode ser eliminado. A única forma de evitar um risco é suspender a atividade que gera o risco, descontinuando o processo.
- **Se formos cuidar dos riscos, não faremos mais nada na organização, pois em tudo há riscos:** Na realidade, somente são geridos os riscos mais significativos. O que proporciona que as atividades mais complexas sejam realizadas com mais segurança é conhecer os riscos envolvidos e adotar providências para mitigá-los.

5. PROGRAMA DE GESTÃO DE RISCOS (PGR)

O PROGRAMA DE GESTÃO DE RISCOS foi criado pela Auditoria Geral do Estado (AGE) por meio da Portaria SEFAZ n.º 162/2018 e tem como objetivo disseminar a GESTÃO DE RISCOS e sua metodologia, orientando a identificação e avaliação dos riscos e a adoção de medidas de controle.

O processo da gestão de riscos compreende os seguintes componentes que serão descritos em detalhe.



Figura: Processo de Gestão de Riscos do PGR (autoria própria)

5.1. METODOLOGIA

A metodologia da Gestão de Riscos utilizada no PGR pode ser aplicada em qualquer organização e atividade e o ponto de partida é a escolha ou seleção do objeto a ser trabalhado.

A metodologia utiliza como referência normas técnicas relacionadas à gestão de riscos, conforme figura abaixo:

METODOLOGIA



5.2. SELEÇÃO DO OBJETO

A Gestão de Riscos identifica, avalia e trata riscos, podendo ser utilizada em diferentes objetos dentre os quais:

- Atividade
- Contrato específico
- Determinada área organizacional
- Obra de infraestrutura
- Organização como um todo
- Processo organizacional
- Projeto

Para dar início às atividades de gestão de riscos, é importante que sejam selecionados os objetos prioritários que serão objeto da identificação dos riscos. Não é razoável imaginar que a gestão de riscos possa ser incorporada de forma automática e abrangente em tudo o que uma determinada organização faz.

Essa priorização de “objetos” para aplicação da gestão de riscos pode ser feita em função de critérios como:

- a) **materialidade:** objetos que envolvem um volume significativo de recursos orçamentários em sua execução;

- b) **criticidade:** objetos para os quais há registro de recorrentes irregularidades ou impropriedades apontadas pelos órgãos de controle ou pelas próprias verificações internas do órgão ou entidade;
- c) **relevância:** objetos que estejam relacionados diretamente aos principais macroprocessos da cadeia de valor ou aos objetivos estratégicos do órgão ou entidade.

Na seleção do objeto deverão ser considerados, ainda, o **tipo da organização** administrativa (direta ou indireta), a **complexidade da estrutura organizacional** e a **suscetibilidade à ocorrência de fraudes ou atos de corrupção**.

5.3. ETAPAS DA GESTÃO DE RISCOS

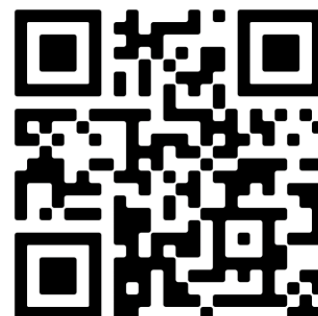
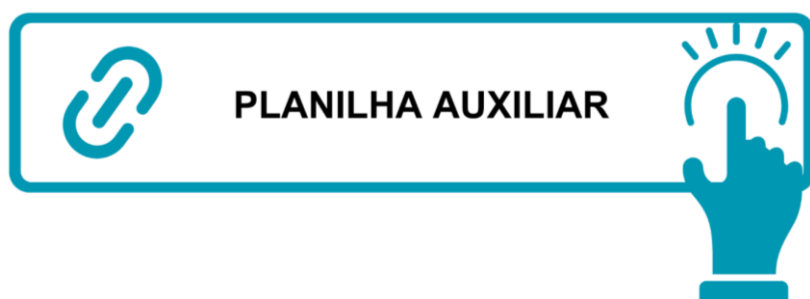
A metodologia de Gestão de Riscos compreende **6 etapas** principais que, embora demonstradas sequencialmente, na prática são aplicadas de forma iterativa. Isso significa que as etapas vão progredindo através de refinamentos sucessivos. Assim, o trabalho realizado pode sempre ser melhorado nas etapas subsequentes.



Figura: Etapas da GR (autoria própria)

Foi elaborada planilha que estrutura e materializa o gerenciamento de risco, isto é, o instrumento por meio do qual se identifica os riscos e busca mitigá-los por meio da implementação de novos controles ou melhoria de controles existentes.

A planilha com suas devidas instruções de preenchimento encontra-se no link abaixo:



ETAPA 1 - ANÁLISE DE CONTEXTO E DEFINIÇÃO DO OBJETIVO

Nesta etapa se estabelece o contexto em que o objeto está inserido dentro da organização.

O estabelecimento do contexto é um precursor essencial para etapa de identificação de riscos. Nesta fase é definido o objetivo e quais fatores externos e internos podem impedir ou comprometer o sucesso da organização em alcançá-lo.

Primeiramente, é feita a coleta de informações sobre o ambiente interno, a exemplo de missão, visão, política de recursos humanos, existência de código de ética ou normas de conduta etc.

Em seguida, o objeto selecionado é detalhado, o que envolve, no que couber, a sua delimitação, alcance, finalidade, fluxo de atividades, estrutura organizacional, legislação vinculada etc, descrevendo de forma expressa, clara e concisa o seu objetivo.

O **objetivo** constitui o propósito ou resultado esperado do objeto analisado e a sua clara compreensão e definição é fundamental para que a organização possa realizar a gestão de riscos.

Ao fim desta etapa é estruturada a matriz SWOT.

MATRIZ SWOT

A análise SWOT ou matriz SWOT ou análise FOFA, em português, se constitui em uma ferramenta usualmente empregada para fazer avaliação de cenário e análise de contexto. É utilizada para identificar, no ambiente interno, as forças e fraquezas e, no ambiente externo, ameaças e oportunidades. Estas informações vão contribuir para o levantamento dos RISCOS.

O termo SWOT é uma sigla oriunda do idioma inglês e é um acrônimo de Forças (Strengths), Fraquezas (Weaknesses), Oportunidades (Opportunities) e Ameaças (Threats).

O **ambiente interno** considera todos os aspectos que a organização tem controle, ou seja, tem como agir e tomar decisões. Como o próprio nome sugere, é tudo que “está dentro” da organização. Especificamente neste domínio estão localizadas as forças e fraquezas.

O **ambiente externo** leva em conta o que está fora do controle da organização. São aspectos para os quais não se tem poder de ação ou decisão e é onde as oportunidades e ameaças se encontram. Geralmente se referem a fatores políticos, econômicos, sociais, tecnológicos, ambientais e legais.



Figura: Análise SWOT

Exemplos de FATORES POSITIVOS:

- Forças: Tecnologia avançada, equipe capacitada.
- Oportunidades: Crescimento macroeconômico, avanços tecnológicos.

Exemplos de FATORES NEGATIVOS:

- Fraquezas: Sistema informatizado ultrapassado, equipe técnica insuficiente.
- Ameaças: Alterações climáticas, crise fiscal, pandemias, restrições orçamentárias.

ETAPA 2 - IDENTIFICAÇÃO DOS RISCOS

O objetivo dessa etapa é encontrar, reconhecer e descrever os eventos que possam impedir que a organização alcance seus **objetivos**.

A etapa de identificação dos riscos que podem vir a impactar negativamente os processos organizacionais do órgão ou entidade é subjetiva, por isso ela requer a participação das equipes envolvidas no objeto que será analisado.

O risco é expresso em termos de: **causa** (fontes de risco e vulnerabilidades), **evento** - que é a ocorrência ou mudança em um conjunto específico de circunstâncias, e **consequência** (impacto no objetivo ou perda).

Para cada evento de risco identificado, deve-se especificar, explorar e ressaltar suas prováveis causas e possíveis consequências.

A partir dos fatores negativos, ou seja, fraquezas e ameaças da análise SWOT, deverão ser identificados **os possíveis riscos associados** e também suas causas e consequências.

Nesta identificação as fraqueza e ameaças poderão ser os próprios riscos ou mesmo suas causas e consequências.

As **causas** são condições que possibilitam um evento acontecer e podem ter origem no ambiente interno ou externo. As **consequências** são o resultado da materialização de um risco.

O risco identificado deve ser descrito de forma clara e precisa, atentando-se para não o descrever simplesmente como o “não alcance” do objetivo.

As fraquezas e ameaças identificadas na matriz SWOT poderão vir a ser consideradas também como causa ou mesmo consequência do risco. O adequado enquadramento como um desses elementos deverá ser confirmado durante a realização da análise Bow tie, a seguir detalhada.

BOW TIE

A análise Bow tie ou gravata borboleta é uma maneira esquemática e simples de descrever e analisar os caminhos de um risco, desde as causas até as consequências, bem como a consistência da relação de causa e efeito.

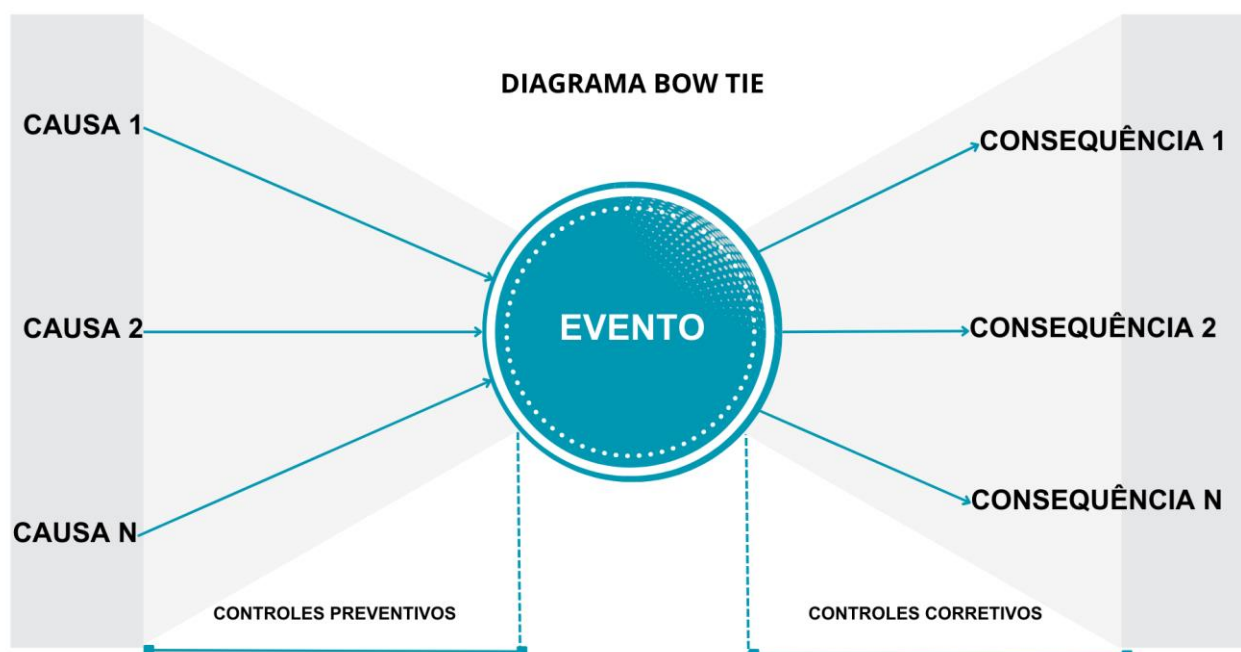


Figura: Diagrama Bowtie (autoria própria)

O ramo esquerdo do diagrama corresponde ao mapeamento das CAUSAS, enquanto o ramo direito corresponde às CONSEQUÊNCIAS. No centro é registrado o EVENTO DE RISCO.

A seguinte sintaxe é aplicada para avaliação da relação de consistência entre causa e efeito:

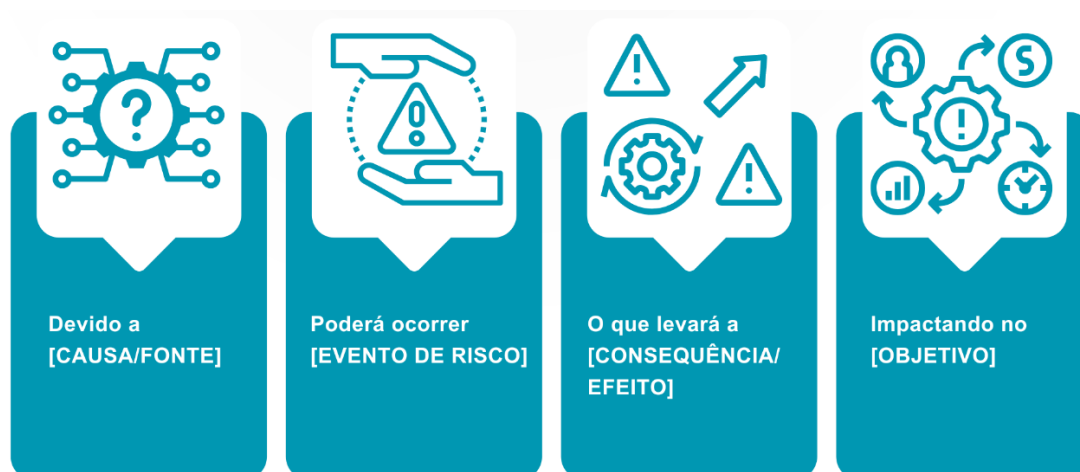


Figura: Avaliação de consistência entre causa e efeito (autoria própria)

Para melhor compreensão da ferramenta, é apresentado **como exemplo** um processo de licitação para aquisição de produtos ou prestação de serviços. A análise BOW TIE, para essa situação, possui a seguinte configuração:

CAUSAS/FONTES	EVENTOS DE RISCOS	CONSEQUÊNCIAS/EFEITOS
Apresentação de recursos pelos concorrentes	Impugnação do Edital	Atraso ou suspensão do processo licitatório
Requisitos indevidamente restritivos		Atraso no recebimento do produto ou na prestação de serviços
Inobservância de requisitos legais do Edital		Prejuízos ao Erário e desperdício de recursos
Cláusulas desnecessárias ou inadequadas	Licitação deserta ou fracassada	Atraso ou suspensão do processo licitatório
Valores referenciais incompatíveis com os praticados no mercado		Prejuízos ao Erário e desperdício de recursos
Valores referenciais incompatíveis com os praticados no mercado	Sobrepreço	Contratação desvantajosa para a Administração
Quantitativo de produtos ou serviços aquém ou além do necessário		
Conluio		Prejuízos ao Erário e desperdício de recursos

Quadro: Exemplo de identificação de risco

Se um risco não se enquadrar de forma coerente nessa sintaxe, deverá ser revisto e reformulado.

A qualquer tempo, durante a execução da Gestão de Riscos, os eventos de risco, causas e consequências podem ser reavaliados (alterados, excluídos ou adicionados).

ETAPA 3 – ANÁLISE DOS CONTROLES EXISTENTES

Nesta etapa deve-se identificar, registrar e avaliar os controles existentes na organização que respondam aos eventos de riscos levantados, seguindo a escala constante na tabela adotada.

Os controles internos da gestão, denominados neste documento de **controles existentes na organização**, 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).

Deficiências nos controles internos indicam que existem falhas na sua formulação, na implementação e ainda, cumulativamente ou não, na eficácia operacional de uma atividade de controle.

Os controles existentes para cada um dos riscos identificados devem ser relacionados e descritos sendo que um mesmo controle pode ser utilizado para tratar mais de um risco.

AVALIAÇÃO DE CONTROLES		
ITEM		DESCRIÇÃO
1	INEXISTENTE	Controle inexistente ou não funcional
2	FRACO	Controle concebido e/ou aplicado caso a caso, sendo a responsabilidade individual e com elevado grau de confiança no conhecimento e experiência das pessoas
3	MEDIANO	Controle mitiga alguns aspectos do risco, mas não contempla todos devido a deficiências na sua concepção e/ou nas ferramentas utilizadas para sua execução
4	SATISFATÓRIO	Controle implementado e sustentado por ferramentas adequadas, que mitigam o risco satisfatoriamente, podendo ser aperfeiçoado
5	FORTE	Controle implementado pode ser considerado a melhor prática e mitiga todos os aspectos relevantes do risco

Figura: Avaliação qualitativa dos controles

Os controles existentes não são computados em termos matemáticos, e sim considerados qualitativamente na avaliação da probabilidade e do impacto do risco. Sendo assim, quanto maior o valor do controle existente, menor será o nível do risco.

ETAPA 4 – MENSURAÇÃO DOS RISCOS

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

Após realizar a avaliação dos controles existentes na organização, atribui-se, para cada risco identificado, uma classificação tanto para a **probabilidade** como para o **impacto** do evento, cuja combinação determinará o nível do risco.

O risco é uma função tanto da probabilidade como do impacto. Portanto, o nível do risco é expresso pela combinação da **probabilidade de ocorrência do evento** e de suas consequências, em termos da **magnitude do impacto** nos objetivos.

A **probabilidade** representa a possibilidade de que um determinado evento ocorra, enquanto o **impacto** representa o seu efeito.

Risco = função (Probabilidade X Impacto)

a) RISCO INERENTE E RESIDUAL

Risco Inerente é aquele obtido da combinação entre probabilidade e impacto **sem considerar os controles internos existentes na organização**. Equivale ao risco bruto, e sua mensuração se dá, usualmente, na fase de criação e implantação de novos processos ou projetos.

Risco Residual é o risco remanescente depois que são identificados e avaliados os controles existentes sobre os riscos inerentes.

b) CÁLCULO DA PROBABILIDADE

Para o cálculo da probabilidade, o PGR utiliza tabela referencial de probabilidade que é aferida em termos da frequência observada/esperada e/ou chance de ocorrência do evento de risco.

O cálculo da probabilidade utiliza a escala de pesos de 1 a 5, variando de 1, "muito baixa", a 5, "muito alta", conforme tabela a seguir:

PROBABILIDADE					
ASPECTOS AVALIATIVOS	Evento pode ocorrer apenas em <u>circunstâncias excepcionais</u>	Evento <u>pode</u> ocorrer em algum momento	Evento <u>deve</u> ocorrer em algum momento	Evento <u>provavelmente</u> ocorra na <u>maioria</u> das circunstâncias	Evento <u>esperado</u> que ocorra na <u>maioria das</u> 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: Tabela de Probabilidade

Para cada risco identificado deve ser atribuída um peso que representa a probabilidade de ocorrência do evento de risco, conforme a tabela acima.

No cálculo da probabilidade são considerados **os controles existentes** na organização avaliados na etapa anterior. Isto porque a probabilidade sofre influência direta da existência e suficiência de controles internos.

c) CÁLCULO DO IMPACTO

Para o cálculo do impacto utiliza-se tabela referencial que apresenta os aspectos a serem considerados para orientar a análise do impacto do evento de acordo com seus efeitos.

IMPACTO					
ASPECTOS AVALIATIVOS	Nenhum impacto no alcance da meta	Prejudica minimamente o alcance da meta	Prejudica razoavelmente o alcance da meta	Prejudica gravemente o alcance da meta	Impede o alcance da meta
DESCRITOR	Insignificante	Pequeno	Moderado	Grande	Catastrófico
PESO	1	2	3	4	5

Figura: Tabela de Impacto

Neste cálculo são considerados os controles existentes na organização avaliados na etapa anterior. Isto porque, assim como a probabilidade, o impacto também sofre influência direta da existência e suficiência de controles internos.

MATRIZ DE RISCOS

A matriz de riscos se constitui em ferramenta gráfica que permite visualizar o nível de risco dos eventos que irão afetar a organização, possibilitando a tomada de decisões sobre aqueles que devem ter seu tratamento priorizado.

É definida pela combinação de dois fatores: probabilidade e impacto. Ao cruzar essas duas informações, encontra-se o quadrante específico para cada risco, sendo possível definir quais são os mais relevantes.

Cada nível ou faixa de risco está representado por uma área de cor específica. Os níveis identificados em “vermelho” (nível crítico) e “laranja” (nível alto) devem receber maior atenção do que aqueles enquadrados nas cores “amarela” (nível moderado) e “verde” (nível pequeno).

A metodologia utilizada adota a seguinte **matriz de risco**:

IMPACTO		MATRIZ DE RISCOS				
Catastrófico	5	5	10	15	20	25
Grande	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Pequeno	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
		1	2	3	4	5
		Muito baixa	Baixa	Média	Alta	Muito alta
PROBABILIDADE						

Figura: Matriz de Riscos (autoria própria)

NÍVEL DE RISCO

O nível de risco expressa a magnitude de determinado evento, em termos de combinação de seu **impacto** e **probabilidade**.

Do cruzamento entre os pesos atribuídos a **probabilidade** e **impacto** resulta uma tabela de níveis de gravidade dos riscos com pontuações de 1 a 25 distribuídas em faixas com cores específicas, que variam de “pequeno” a “crítico”, conforme a tabela abaixo:

Escala de Nível de Risco	
Nível	Pontuação
RC - Risco Crítico	16 a 25
RA - Risco Alto	8 a 15
RM - Risco Moderado	4 a 6
RP - Risco Pequeno	1 a 3

Figura: Escala de nível de risco

O risco de nível CRÍTICO deve ser notificado formalmente ao dirigente máximo e ao proprietário do risco, para que sejam adotadas medidas imediatas de tratamento.

ETAPA 5 – SELEÇÃO DE RESPOSTAS AOS RISCOS

A resposta aos riscos é a etapa em que, a cada risco identificado e avaliado, poderá ser elaborada e proposta uma ou mais medidas (respostas ao risco) para sua mitigação, na forma de um Plano de Tratamento dos Riscos, que pode variar entre MITIGAR, EVITAR, TRANSFERIR ou ACEITAR. Essa resposta será definida por cada órgão ou entidade, levando-se em consideração o nível de risco identificado e a complexidade do objeto.

A figura abaixo traz as medidas de resposta ao risco:



Figura: Resposta ao risco (autoria própria)

MITIGAR: desenvolver ações para reduzir o risco, ou seja, remover suas fontes ou reduzir a probabilidade e/ou impacto do risco. É a resposta mais comum objetivando a reduzir o risco a um nível tolerável.

EVITAR: Como o risco não pode ser eliminado, não existe risco com nível zero. A única forma de evitá-lo é eliminar a atividade a qual está associado, descontinuando o processo ou suspendendo as atividades que geram o risco.

TRANSFERIR: compartilhar ou transferir parte dos riscos a terceiros.

ACEITAR: manter as práticas existentes, aceitando a exposição ao risco. Neste caso convém que a situação seja devidamente registrada e o risco mantido sob análise contínua.

ETAPA 6 – ELABORAÇÃO DO PLANO DE TRATAMENTO DE RISCOS

O Plano de Tratamento de Riscos é um conjunto de ações necessárias propostas pela organização para adequar os níveis de riscos, seja por meio da adoção de novos controles ou otimização dos controles existentes.

O propósito do plano de tratamento de riscos é especificar como as medidas serão implementadas, de maneira que as ações sejam compreendidas pelos envolvidos e o progresso do plano monitorado.

Nesta etapa são concebidas ações necessárias para o tratamento dos riscos residuais identificados, priorizando-se aqueles situados nos níveis “**crítico**” e “**alto**”, ou seja, na faixa em que o risco esteja **entre 8 e 25**, conforme Escala de Nível de Risco.

Para tratamento dos riscos deve ser identificada a opção mais adequada de resposta (controle), equilibrando, de um lado, os custos e os esforços de implementação e, de outro, os benefícios decorrentes.

Independentemente do tipo de controle a ser implementado, é importante que ele seja proporcional ao risco.

É recomendável na elaboração do Plano de Tratamento de Riscos que a organização:

- Descreva sucintamente os controles propostos para cada evento de risco. Nesse momento, deve ser colocado **o controle** propriamente dito, e não como o controle será implementado. Exemplo: usar “Checklist” em vez de “Elaborar Checklist”; “Instrução Normativa” em vez de “Publicar Instrução Normativa”; e “Sistema informatizado” e não “Implantar sistema informatizado”.
- Especifique e detalhe as ações de controle utilizando metodologia já adotada pela organização, de forma a listar as macroatividades necessárias para sua execução, estabelecendo prazos e apontando seus responsáveis.
- No detalhamento das ações, evite expressões do tipo “solicitar contratação”, “fazer gestão para adquirir sistema” ou “planejar capacitação”. Deve-se usar “contratar”, “adquirir e implantar sistema” ou “capacitar”, que constituem as soluções efetivas em termos de controle interno para tratamento do risco.

Na proposição de ações, é importante considerar, dentre outras:

- Controles automatizados em substituição aos manuais, quando possível;
- Utilização de indicadores de desempenho: estabelecimento de indicadores (índice de rotação de pessoal, cumprimento de prazos legais, entre outros);
- Segregação de funções: atribuição de obrigações entre pessoas com a finalidade de reduzir risco, erro ou fraude;

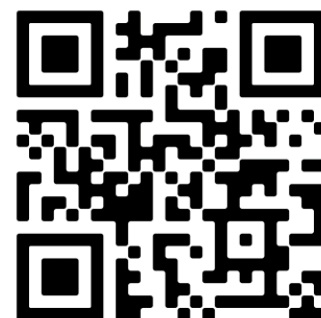
- Limites para transações;
- Combinação de controles manuais e informatizados (automatizados).

Após finalização, o plano de tratamento de riscos deve ser encaminhado para aprovação do dirigente máximo da organização e posteriormente comunicado às partes interessadas, que são as pessoas ou organizações que podem afetar, ser afetadas ou peceber-se afetadas por uma decisão ou atividade.

Ao responsável por cada ação indicada no Plano de Tratamento de Riscos caberá:

- Desdobrar as macroatividades previstas em tarefas, isto é, em atividades mais detalhadas.
- Coordenar e acompanhar a sua implementação e o contínuo monitoramento para verificar a necessidade de revisão.
- 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.

Para melhor entendimento da metodologia, seguem-se as etapas a serem cumpridas, tendo como exemplo um processo de licitação para aquisição de de serviços de Tecnologia da Informação e Comunicação (TIC) conforme link abaixo:



5.4. COMUNICAÇÃO E MONITORAMENTO

A comunicação visa promover a conscientização e o entendimento do riscos de forma oportuna, pertinente, precisa e compreensível levando em consideração a confidencialidade e integridade da informação, bem como os direitos de proteção de dados e privacidade dos indivíduos.

O monitoramento das ações de tratamento de riscos envolve a verificação contínua e periódica do funcionamento da implementação e dos seus resultados.

Deve considerar o tempo necessário para que as medidas mitigadoras produzam seus efeitos e ser conduzido pela coordenação setorial de controle interno ou unidade equivalente que ficará responsável pelo acompanhamento do Plano de Tratamento de Riscos, visando avaliar se as ações de tratamento dos riscos são eficazes e estão sendo implementadas nos prazos previstos.

A eficácia das ações do Plano de Tratamento de Riscos pode ser aferida realizando-se nova mensuração do nível de riscos, preferencialmente àqueles categorizados como crítico e alto, de forma frequente e de modo a verificar se os controles implementados atuaram, ou não, na mitigação dos riscos.

5.5. PASSO A PASSO - IMPLANTAÇÃO DO PGR

PASSO	DESCRIÇÃO	REFERÊNCIA	RESPONSÁVEL
1	Formalizar adesão ao PGR	OT 01/2023	Dirigente máximo
2	Constituir Comitê de Gestão de Riscos (CGR)	OT 01/2023	Dirigente máximo
3	Definir Objeto alvo do PGR	PAG. 18	Dirigente máximo e CGR
4	Constituir Grupo de Trabalho (GT) temporário	OT 01/2023	CGR
5	Analisar o Objeto selecionado para entendimento do escopo e seu contexto	PAG. 20	GT
6	Realizar Análise SWOT a fim de identificar cenários internos e externos com potencial de impactar nos objetivos estratégicos do objeto selecionado	PAG. 21	GT
7	Identificar os riscos , a partir dos fatores negativos da análise SWOT (fraquezas e ameaças)	PAG. 22	GT
8	Apurar e registrar as causas dos riscos identificados, ou seja, as condições que dão origem à possibilidade de um evento ocorrer (fatores de risco)	PAG. 22	GT
9	Apurar e registrar as consequências dos riscos identificados, ou seja, os resultados ou os efeitos de um evento de risco sobre os objetivos do objeto selecionado	PAG. 22	GT
10	Testar a coerência dos riscos identificados, aplicando a sintaxe constante no diagrama Bow tie	PAG. 23	GT
11	Relacionar e avaliar os controles existentes	PAG. 24	GT
12	Calcular Probabilidade dos riscos	PAG. 26	GT
13	Calcular Impacto dos riscos	PAG. 27	GT
14	Determinar o nível dos riscos	PAG. 28	GT
15	Definir resposta aos riscos	PAG. 29	GT
16	Elaborar Plano de Tratamento de Riscos (PTR)	PAG. 29	GT
17	Autorizar a implantação das ações previstas no PTR	OT 01/2023	Dirigente máximo
18	Comunicar as ações de controle	PAG. 31	Dirigente máximo e CGR
19	Monitorar implantação das ações de controle	PAG. 31	CGR

6. TERMOS E DEFINIÇÕES

- a) **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.
- b) **Análise de riscos:** 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.
- c) **Bow tie:** 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”**). A origem do diagrama “Bowtie” (gravata borboleta) é desconhecida, tendo esses registros sido perdidos ao longo do tempo. Acredita-se que seja uma evolução dos diagramas de causa-consequência dos anos 70 e dos diagramas de barreiras dos anos 80. A primeira referência a esta metodologia apareceu na Universidade de Queensland, Austrália em 1979. Posteriormente a metodologia amadureceu na década de 90 após o desastre de “Piper Alpha” que ocorreu numa plataforma de petróleo no mar do Norte. O Grupo Royal Dutch/Shell aplicou essa técnica no estudo do desastre, evento este que pode ser considerado como um divisor de águas para a difusão e amadurecimento dessa metodologia.
- d) **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.
- e) **Dirigente máximo:** pessoa que dirige e controla a organização no mais alto nível.
- f) **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 ou 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.).

- g) **Fraude:** qualquer ato ilegal caracterizado por desonestidade, dissimulação ou quebra de confiança.
- h) **Integridade pública:** 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 nas instituições governamentais.
- i) **Mensuração de risco:** significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência.
- j) **Objeto do PGR:** elemento em que será aplicada a metodologia do PGR, podendo ser uma organização como um todo; uma determinada área da organização (ex; Setor de Licitação); um projeto ou um determinado contrato. A condição essencial para a delimitação do objeto é que se identifique seu objetivo e se delimite com precisão seu foco.
- k) **Organização:** órgão/entidade que aderir ao Programa de Gestão de Riscos, nos termos da Portaria SEFAZ nº 162/2018.
- l) **Processo:** conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.
- m) **Proprietário do risco:** indivíduo que possua responsabilização e tenha autoridade para gerenciar riscos.
- n) **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.
- o) **Risco residual:** risco a que uma organização está exposta após a implementação de ações gerenciais (controles) para o tratamento do risco.
- p) **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.
- q) **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.).

7. CONCLUSÃO

A gestão de riscos não é uma atividade única, mas um processo contínuo que requer monitoramento regular e ajustes conforme necessário. Com o compromisso e a participação de todos, o Programa de Gestão de Riscos – PGR pode contribuir significativamente para o sucesso e a resiliência das unidades que integram o Estado.

Através de uma abordagem sistemática e estruturada, o PGR ajuda a minimizar a incerteza e a maximizar as oportunidades. Ele promove uma cultura de gestão de riscos que permeia todos os níveis da administração estadual, incentivando a tomada de decisões informada e a responsabilidade compartilhada.

No entanto, a eficácia do programa depende de sua aplicação consistente e de sua revisão e atualização contínuas. É essencial que todos os envolvidos compreendam seus papéis e responsabilidades e estejam comprometidos com a gestão de riscos.

Finalmente, embora o programa forneça uma estrutura robusta para a gestão de riscos, ele deve ser adaptado às necessidades e circunstâncias específicas de cada órgão ou entidade.

Vale destacar que o conteúdo deste documento não exaure o tema. Novos estudos, modelos e atualizações poderão ser oportunamente editados e publicados no site da SEFAZ-BA, ficando a AGE disponível para dirimir quaisquer dúvidas através do e-mail **gepre@sefaz.ba.gov.br**.

8. REFERENCIAIS

- MANUAL DE GESTÃO DE RISCOS DO TCU. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão. (Seplan), 2020.
- METODOLOGIA DE GESTÃO DE RISCOS. Brasil. Ministério da Transparência e Controladoria-Geral da União (CGU), 2018-04.
- GUIA PRÁTICO DE GESTÃO DE RISCOS PARA A INTEGRIDADE. Ministério da Transparência e Controladoria Geral da União. 2018.
- IMPLEMENTANDO A GESTÃO DE RISCOS NO SETOR PÚBLICO. Fundação Escola Nacional de Administração Pública. Módulo 3 - Ciclo de Gerenciamento de Riscos Corporativos. 2018.
- Declaração de Posicionamento do IIA: AS TRÊS LINHAS DE DEFESA NO GERENCIAMENTO EFICAZ DE RISCOS E CONTROLES. Janeiro 2013. The Institute of Internal Auditors.
- INSTRUÇÃO NORMATIVA CONJUNTA MP/CGU n. 01, de 2016.
- NBR ISO 31000/2018. Gestão de Riscos – Diretrizes
- NBR ISO 31010/2009. Gestão de Riscos – Técnicas para o processo de avaliação de riscos.
- NBR ISO GUIA 73/2009. Gestão de Riscos – Vocabulário