

1ª EDIÇÃO



CGEMT

**GUIA SIMPLIFICADO
DE GESTÃO DE
RISCOS DE
INTEGRIDADE**



CGEMT

**GUIA SIMPLIFICADO
DE GESTÃO DE
RISCOS DE
INTEGRIDADE**

**CUIABÁ-MT
2023**

Secretário Controlador Geral do Estado

Paulo Farias Nazareth Netto

Secretária Adjunta de Ouvidoria Geral e Transparência

Karen Cristina Oldoni da Silva

Secretário Adjunto de Auditoria e Controle

Joelcio Caires da Silva Ormond

Secretário Adjunto de Corregedoria Geral

Renan Zattar Ferreira da Silva

Secretário-Adjunto Executivo e de Ações Estratégicas

José Alves Pereira Filho

Elaboração

Anderson Andrey Paes Escobar

Ariel Afonso Pinho

Fabíola Maria Belmonte Dourado

Gilmar Souza da Silva

Sérgio Antônio Ferreira Paschoal

AUDITORES DO ESTADO

Revisão

Joelcio Caires da Silva Ormond

Projeto Gráfico e Diagramação

Assessoria de Comunicação da CGE-MT





MISSÃO

“Contribuir para melhoria dos Serviços Públicos prestados pelo Poder Executivo do Estado de Mato Grosso, por meio do aperfeiçoamento dos Sistemas de Controles, da Conduta dos Servidores e dos Fornecedores, ampliando a transparência e fomentando o Controle Social”

VISÃO

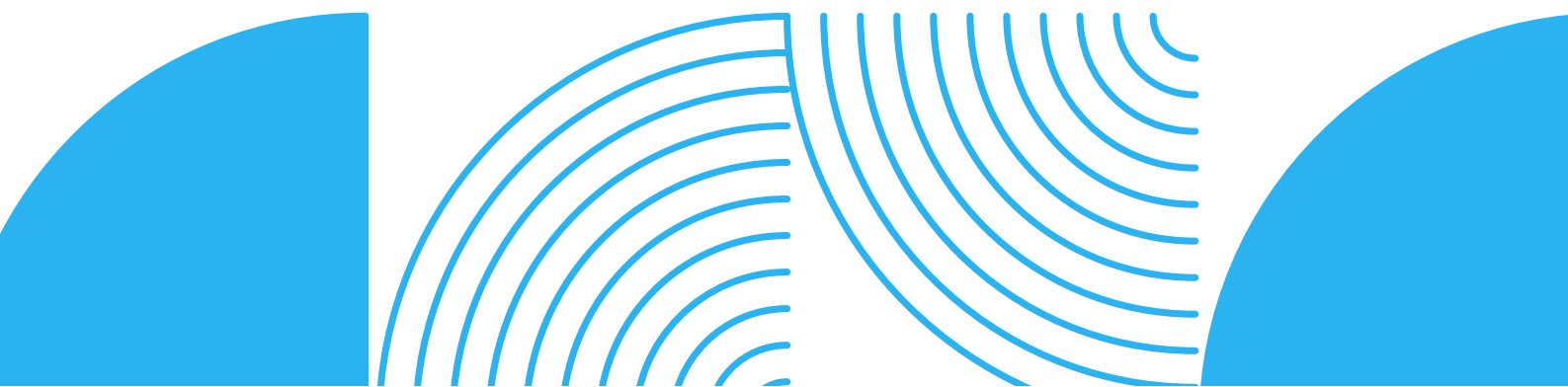
“Ser a instituição de excelência nas atividades de ouvidoria, auditoria, controle e corregedoria e reconhecimento pela sociedade como Órgão autônomo e essencial à qualidade do gasto público e ao controle social.”

VALORES

- **Legalidade:** Atuar em conformidade com a legislação e os princípios da Administração.
- **Transparência:** Comunicar de forma clara e honesta.
- **Confidencialidade:** Resguardar sigilo na medida da imposição legal.
- **Probidade:** Agir de forma reta, honesta e de acordo com a ética e a moralidade.
- **Imparcialidade:** Analisar sem privilégios.
- **Excelência:** Realizar e conduzir a prestação de serviços públicos com qualidade.

ÍNDICE

1. APRESENTAÇÃO	6
2. PROGRAMA DE INTEGRIDADE	8
2.1 PLANO DE INTEGRIDADE	10
2.2 MAPEAMENTO DE RISCOS	11
3. GESTÃO DE RISCOS DE INTEGRIDADE	12
3.1 RISCOS	13
3.2 RISCOS DE INTEGRIDADE	13
3.3 GESTÃO DE RISCOS	15
4. METODOLOGIA DE GESTÃO DE RISCOS	18
4.1 FOMENTO DA CGE/MT	19
4.2 METODOLOGIA	19
4.3 ESTABELECIMENTO DO CONTEXTO	22
4.4 MAPEAMENTO DE PROCESSOS	30
4.5 IDENTIFICAÇÃO DE RISCOS	31
4.6 ANÁLISE DOS RISCOS	36
4.7 AVALIAÇÃO DOS RISCOS	44
4.8 TRATAMENTO DOS RISCOS	45
4.9 MONITORAMENTO	46
4.10 COMUNICAÇÃO	47
5. CONSIDERAÇÕES FINAIS	48
6. REFERÊNCIAS	50
7. ANEXOS	52





1. APRESENTAÇÃO

Este Guia foi elaborado em atenção ao disposto na Lei Estadual nº 10.691, de 05 março de 2018, que instituiu o Programa de Integridade Pública do Governo do Estado de Mato Grosso para todos os órgãos e entidades da Administração Pública Direta, Autárquica e Fundacional do Poder Executivo Estadual, sendo um Programa fomentado e avaliado pela Controladoria Geral do Estado de Mato Grosso - CGE/MT.

A Controladoria possui como competência fornecer aos órgãos e entidades que aderirem ao Programa de Integridade, suporte teórico e metodológico. Compete, ainda, à CGE, a avaliação dos Planos de Integridade implantados, quanto à sua existência e efetividade.

Ao mesmo tempo que a utilização do Guia assegura uma base de coerência a toda a Administração Estadual, a natureza geral do Guia possibilita aos órgãos e entidades estaduais a adaptação das orientações e da metodologia a contextos e situações específicas das organizações.

A possibilidade de adaptar o Guia a contextos e situações específicas não deve impactar no rigor e na qualidade das informações levantadas, produzidas e registradas pelos órgãos e entidades estaduais.

O Guia Simplificado para Gestão de Riscos de Integridade faz parte de ações da CGE para o aprimoramento da governança pública, gestão de riscos de integridade e controles internos, constituindo-se um importante passo rumo a mudanças de paradigmas e da cultura organizacional da administração pública.



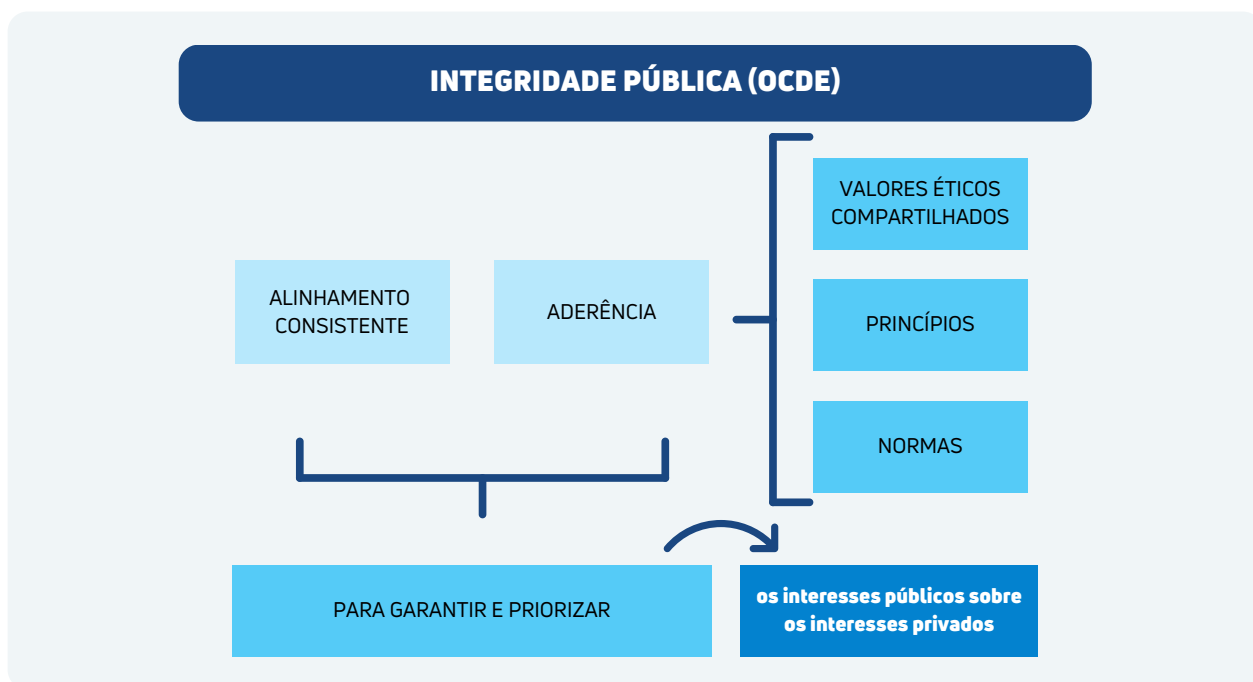
2. PROGRAMA DE INTEGRIDADE

A Lei Estadual nº 10.691/2018 instituiu o Programa de Integridade Pública do Governo do Estado de Mato Grosso para todos os órgãos e entidades da Administração Pública, Autárquica e Fundacional do Poder Executivo Estadual, Programa fomentado e avaliado pela Controladoria Geral do Estado.

A Controladoria Geral da União - CGU, definiu Integridade Pública em seu Guia de Integridade Pública (CGU, 2015), como "o conjunto de arranjos institucionais que visam a fazer com que a Administração Pública não se desvie de seu objetivo precípua: entregar os resultados esperados pela população de forma adequada, imparcial e eficiente".

No documento da Organização para a Cooperação e Desenvolvimento Econômico - OCDE, intitulado Recomendação do Conselho da OCDE sobre Integridade Pública (OCDE, 2017), conceituou-se Integridade Pública como "alinhamento consistente e a aderência a valores éticos compartilhados, princípios e normas para garantir e priorizar os interesses públicos sobre os interesses privados".

Figura 1 – Conceito de Integridade Pública OCDE



Fonte: Elaborada pelos autores com base no conceito de integridade da OCDE, 2017

A instituição do Programa de Integridade tem o objetivo de orientar e capacitar os órgãos, autarquias e fundações do Poder Executivo Estadual a implementar seus respectivos Planos de Integridade e exprime o compromisso do Estado de Mato Grosso com os valores de integridade, da ética, da transparência pública, do controle social e do interesse público.

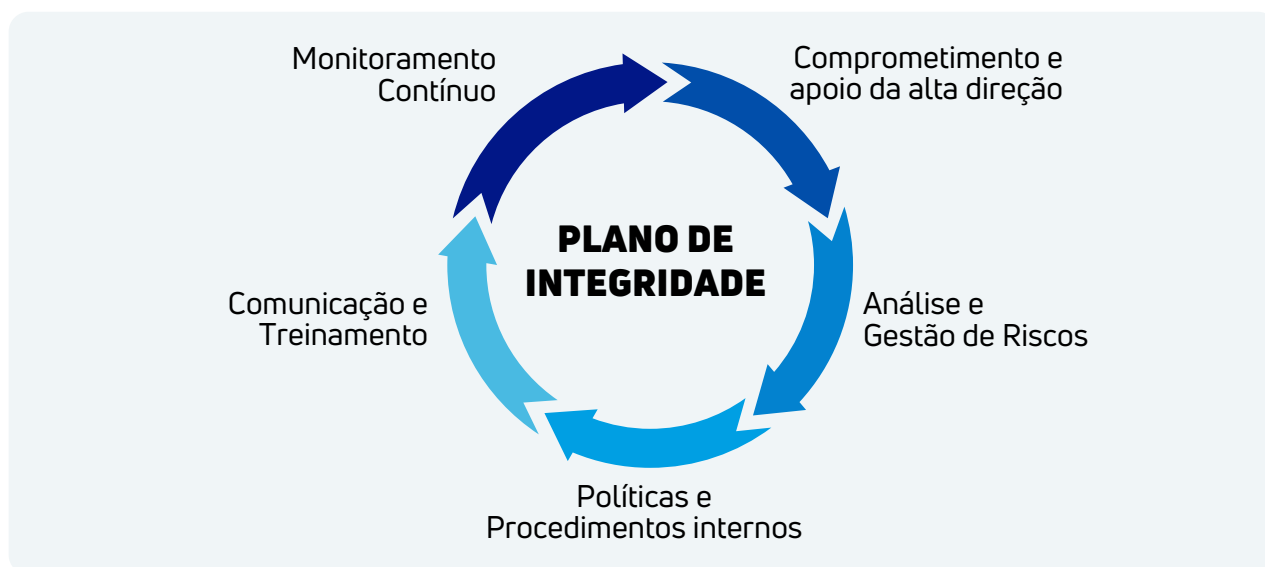
2.1 PLANO DE INTEGRIDADE

O Plano de Integridade é definido pela Lei nº 10.691/2018 como um conjunto de mecanismos e procedimentos internos de prevenção, detecção e remediação de fraudes, irregularidades e desvios de conduta, contrários ao interesse da Administração Pública.

A norma ainda definiu como um dos eixos fundamentais do Plano de Integridade a análise e gestão de riscos e, de acordo com o disposto em seu art. 3º, o Plano contemplará ações e medidas, dentre as quais, destacam-se, as ações estabelecidas no inciso IV: (...)

IV - Verificação e fiscalização, nas atividades internas e externas, de irregularidades, práticas de ilícitos ou existência de vulnerabilidades, com constante atualização da matriz de risco previamente elaborada. (Lei 10.691/2018, art. 3º, inc. IV)

Figura 2 – Eixos do Programa de Integridade do Estado de Mato Grosso



Fonte: Controladoria Geral do Estado de Mato Grosso

2.2 MAPEAMENTO DE RISCOS

A elaboração do Plano de Integridade deve ser realizada a partir do mapeamento de riscos de integridade e da avaliação das medidas existentes, com a finalidade de identificar vulnerabilidades no quadro de integridade do órgão/entidade e propor medidas para sua mitigação. (Lei nº 10.691/2018, art. 3º, §1º).

A finalidade principal do mapeamento de riscos de integridade é oferecer subsídios para a implementação de mecanismos e procedimentos de controle interno fundamentados na gestão de riscos de integridade.

Com base na avaliação dos riscos de integridade e dos controles existentes, serão elaborados planos de ação, envolvendo a implantação de controles internos e de monitoramento de riscos bem como o fortalecimento da cultura de responsabilidade por riscos e controles em toda a instituição.



3. GESTÃO DE RISCOS DE INTEGRIDADE

3.1 RISCOS

Segundo a ABNT (Associação Brasileira de Normas Técnicas) NBR ISO 31000:2018, “risco é o efeito da incerteza nos objetivos da organização”.

Os riscos podem ser considerados como eventos ou condições incertas que, caso ocorram, podem gerar impactos negativos (ameaças) ou positivos (oportunidades) para a instituição.

A definição e a realização dos objetivos de uma organização pública envolvem diferentes riscos decorrentes da natureza de suas atividades. No acompanhamento da estratégia organizacional, deve haver um processo sistemático e contínuo de detecção, avaliação e remediação de eventos que possam impedir o alcance dos resultados almejados.

3.2 RISCOS DE INTEGRIDADE

A compreensão do conceito de integridade vai além da legalidade e da conformidade das ações públicas pois a integridade pública está associada ao compromisso com a conduta ética, à conformidade dos processos e ações e ao respeito pelo serviço público.

Risco à integridade é definido pela Controladoria Geral da União como a vulnerabilidade que pode favorecer ou facilitar a ocorrência da prática de desvios éticos e/ou ilegais que possam violar a conduta de integridade pública (Portaria GM/CGU nº 57/2019).

No contexto da gestão de riscos de integridade, o favorecimento da ocorrência de fraudes e atos de corrupção não se restringe ao descumprimento de leis e normas, abrangendo outras situações de quebras de integridade, como abuso de poder/influência, conflito de interesses, nepotismo, uso indevido e vazamento de informação sigilosa, recebimento/oferta de propina e práticas antiéticas.

Os riscos, quando confirmados, podem impactar negativamente o órgão/entidade e ocasionar prejuízos ao alcance dos objetivos, atingindo a imagem e reputação da instituição, dos servidores e agentes públicos envolvidos, podendo ensejar responsabilidades nas três esferas.

Os riscos para a integridade podem ser causa, evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem.

É fundamental a compreensão por parte dos gestores públicos e dos servidores que atuam na Gestão de Riscos, de que a gestão de riscos para a integridade visa examinar, além da integridade pessoal, a integridade de funções e processos.

Figura 3 – Riscos de Integridade



Fonte: Elaborada pelos autores com base no conceito da CGU, 2019

A lista abaixo é exemplificativa e traz alguns exemplos de riscos de integridade nas organizações públicas. O Anexo II deste Guia apresenta uma lista mais abrangente, no entanto, ambas são listas não exaustivas, podendo contemplar outros riscos de integridade.

- Abuso de posição ou poder em favor de interesses privados;
- Comportamento incompatível com a função pública;
- Conflito de interesses;
- Exercer pressão externa ilegal ou antiética para influenciar agente público/privado;
- Exercer pressão interna ilegal ou antiética para influenciar agente público/privado;
- Nepotismo;
- Solicitação ou recebimento de propina/pagamento indevido;
- Utilização de verbas e fundos públicos em favor de interesses privados;
- Utilização/Vazamento de informação privilegiada/restrita.

3.3 GESTÃO DE RISCOS

De acordo com o modelo Gerenciamento de Riscos Corporativos - Integrado com Estratégia e Performance do COSO - Committee of Sponsoring Organizations:

Gestão de riscos corporativos é o processo que permeia toda a organização, colocado em prática pela alta administração da entidade, pelos gestores e demais colaboradores, aplicado no estabelecimento da estratégia e projetado para identificar possíveis eventos que possam afetar a instituição e para gerenciar riscos de modo a mantê-los dentro do seu apetite de risco, com vistas a fornecer segurança razoável quanto ao alcance dos objetivos da entidade. (COSO, 2017)

Figura 4 – Processo de Gestão de Riscos Corporativos – COSO 2017



Fonte: Elaborada pelos autores com base no COSO, 2017

Os planos de integridade devem estar alicerçados em uma política, plano ou processo de gestão de riscos que contemple ações de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos que possam comprometer o alcance dos objetivos estratégicos da instituição.

A Gestão de Riscos de Integridade possibilita o estabelecimento de um conjunto de medidas visando à prevenção de possíveis desvios e irregularidades na entrega à sociedade dos resultados esperados dos órgãos e entidades da Administração Pública Estadual, por meio do fortalecimento das decisões em respostas aos riscos.

É fundamental destacar que a equipe responsável pela gestão de riscos do órgão/entidade e a unidade de integridade (quando houver instâncias de integridade), são apenas facilitadoras do processo, sendo que cada gestor é responsável por gerir os riscos no âmbito de sua unidade de atuação, área, processos e atividades.

Considerando-se o Modelo das Três Linhas do IIA - *The Institute of Internal Auditors*, a 1ª linha refere-se aos controles internos executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio.

Figura 5 – Linhas de Defesa – IIA



Fonte: Modelo das três linhas (IIA, 2020)

Estão entre as competências da 1ª linha:

- Gestão Operacional - onde estão os riscos (proprietária do risco);
- Responsabilidade de identificar, mensurar, avaliar e mitigar os riscos;
- Manter controles internos eficientes;
- Implementar ações corretivas para resolver deficiências em processos e controles;
- Responsabilidade de prestação de contas pela gestão de riscos.



4. METODOLOGIA DE GESTÃO DE RISCOS

4.1 FOMENTO DA CGE/MT

A adesão ao Programa de Integridade do Estado de Mato Grosso é voluntária e o órgão ou entidade que aderir ao Programa desenvolverá seu Plano de Integridade, com apoio da Controladoria Geral do Estado.

Nesse sentido, e em cumprimento à determinação da legislação, a CGE, por meio de seu Regimento Interno, definiu como missão da Unidade de Integridade (unidade que compõe o nível de apoio estratégico e especializado da CGE/MT), “instituir mecanismos, procedimentos e exercer a coordenação para implantação do Programa de Integridade Pública no âmbito do Poder Executivo do Estado”;

A Unidade de Integridade possui como uma de suas competências a emissão de diretrizes, elaboração de metodologia e a promoção de treinamentos sobre análise de riscos de integridade.

Por meio da Portaria CGE/MT, nº 77/2022 foi instituído Grupo de Trabalho de Gestão de Riscos para auxiliar a Unidade de Integridade tanto na Gestão de Riscos de Integridade no âmbito da CGE quanto nas atividades de consultoria aos órgãos e entidades aderentes ao Programa de Integridade.

4.2 METODOLOGIA

Inicialmente, antes de efetivamente o órgão/entidade iniciar a aplicação da metodologia de gestão de riscos de integridade, é necessária a designação formal de uma equipe para conduzir os trabalhos.

A seleção da ferramenta de riscos a ser utilizada pelos órgãos e entidades é de livre escolha, considerando os critérios de oportunidade e conveniência, mas respeitando os conceitos dos principais frameworks* de gestão de riscos.

Apesar da diversidade de métodos e instrumentos disponíveis para gestão de riscos, verifica-se bastante convergência em relação às etapas de implementação do processo.

Se o órgão/entidade já adota uma determinada metodologia de avaliação de riscos em outras áreas ou processos, pode ser uma opção aplicá-la no levantamento dos riscos de integridade e na construção de seu Plano de Integridade.

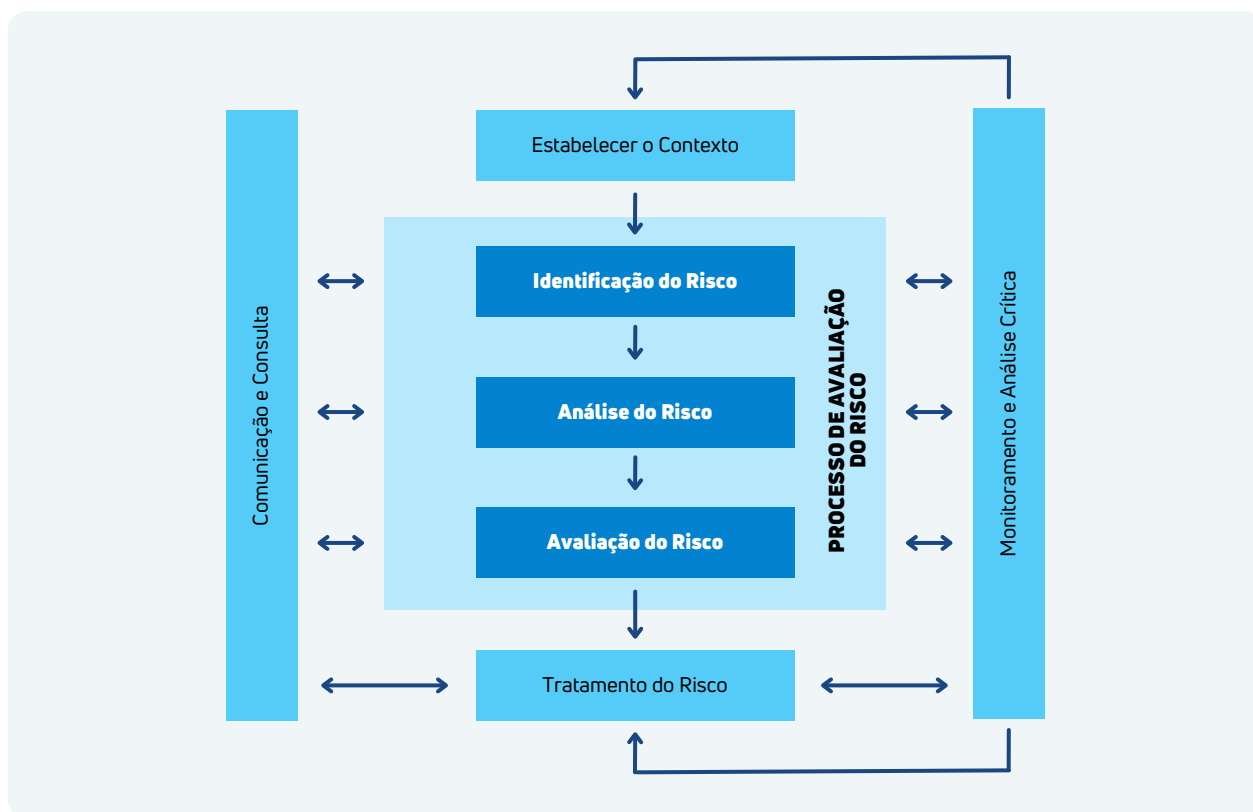
A base teórico-conceitual da Metodologia de Gestão de Riscos da CGE/MT está alinhada com os seguintes parâmetros internacionais – frameworks e normativos:

- ABNT NBR ISO 31.000: 2018, Gestão de Riscos - Princípios e Diretrizes;
- ABNT NBR ISO 31.010: 2021, Gestão de Riscos – Técnicas para o processo de avaliação de riscos;
- Modelo de Três Linhas do IIA - Instituto dos Auditores Internos;
- COSO - *Enterprise Risk Management - Integrating with Strategy and Performance*.

Neste guia, para definição da metodologia do Processo de Gestão de Riscos foram utilizados os conceitos da ABNT NBR ISO 31000:2018 como referência. Segundo esta norma, o processo de gestão de riscos deve ser parte integrante do órgão/entidade e, ainda, adaptado aos seus processos. A seguinte sequência de atividades é sugerida:

- I – realizar o estabelecimento do contexto;
- II - identificar os riscos de integridade;
- III - analisar os riscos;
- IV - avaliar os riscos;
- V - estabelecer medidas de tratamento; e
- VI - monitorar os riscos mapeados.

Figura 6 – Processo de Gestão de Riscos



Fonte: ABNT – ISO 31000:2018

As etapas do processo de avaliação de riscos podem ser realizadas tanto em nível organizacional quanto departamental, e, ainda, para projetos, atividades individuais ou riscos específicos e, de acordo com o disposto na ABNT NBR ISO 31010:2021, o processo de avaliação de riscos tenta responder às seguintes questões fundamentais:

- o que pode acontecer e por quê? (pela identificação de riscos)
- quais são as consequências?
- qual é a probabilidade de sua ocorrência futura?
- existem fatores que mitigam a consequência do risco ou que reduzam a probabilidade do risco?
- o nível de risco é tolerável ou aceitável e requer tratamento adicional?

* *framework*: termo em inglês que significa estrutura e que, em administração, pode ser considerada a estrutura conceitual básica que permite a realização de entregas padronizadas para diferentes objetos de negócio.

4.3 ESTABELECIMENTO DO CONTEXTO

O diagnóstico realizado nessa etapa possibilita compreender o cenário em que o órgão está inserido além de permitir identificar as práticas de integridade que já existem na instituição.

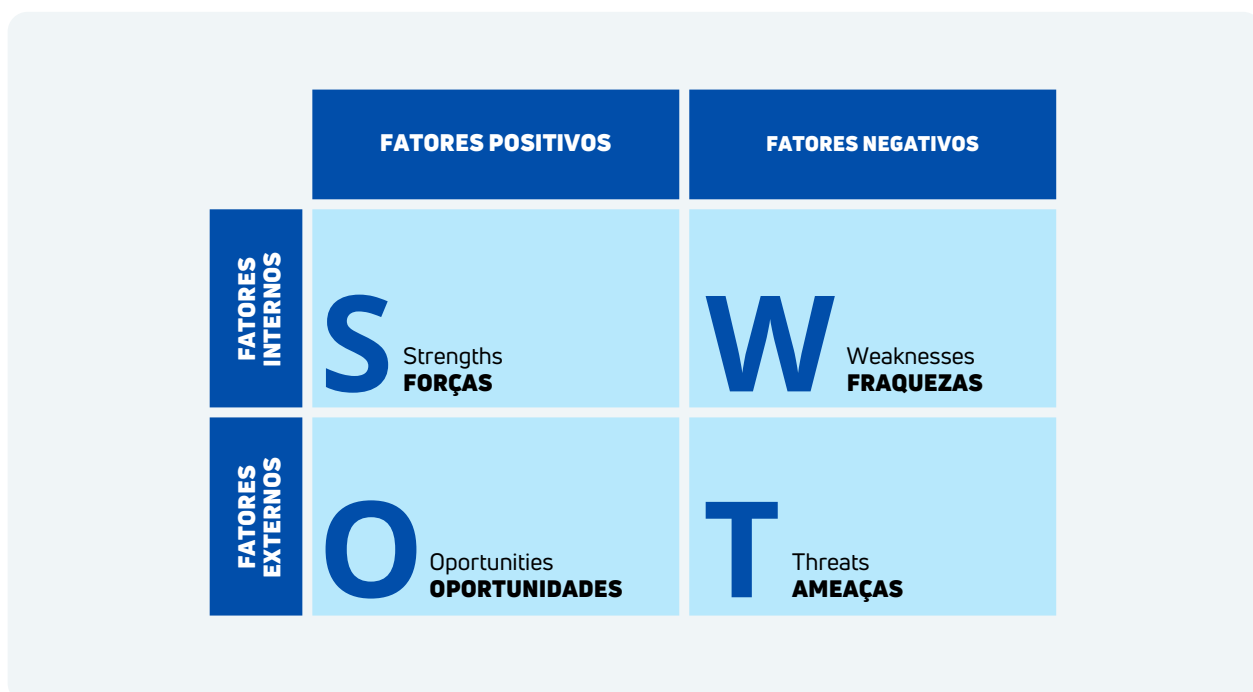
Estabelecer o contexto consiste em compreender o ambiente interno e externo no qual o objeto de gestão de riscos encontra-se inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

Nessa etapa, podem ser consultados documentos como o planejamento estratégico, relatórios de gestão, orçamentos, análises e qualquer outra documentação pertinente à organização e suas finalidades.

Técnica utilizada para estabelecimento do contexto

Sugere-se a utilização da matriz *SWOT* (*Strengths, Weaknesses, Opportunities and Threats*) ou FOFA (Forças, Oportunidades, Fraquezas e Ameaças), que é um instrumento para identificação de cenários, internos e externos, com potencial de impactar positiva ou negativamente a organização.

Figura 7 – Matriz Swot



Fonte: Elaborada pelos autores com base na Matriz SWOT

Os elementos forças e fraquezas são internos à organização e potencialmente podem ser controlados por ela.

As forças são os recursos, habilidades, posição da unidade, capital humano, além de outras competências distintas - que distinguem a organização das demais.

As fraquezas, por sua vez, podem levar as organizações a um fraco desempenho, sendo exemplos importantes o método de trabalho obsoleto, carência de recursos tecnológicos, políticas de incentivos inadequada, entre outros fatores.

Os fatores do ambiente externo - oportunidades e ameaças, não podem ser controlados pelas organizações, as quais devem atuar sobre suas forças e fraquezas para que possam explorar as oportunidades do ambiente e se proteger das ameaças.

Identificação dos atributos do órgão/entidade

A análise realizada nessa etapa de estabelecimento do contexto pode ser feita em um nível estratégico e não necessariamente por área ou atividade e contribui para a identificação de macroprocessos e processos críticos da organização.

- Ambiente Interno

Para a identificação dos pontos fortes e fracos do ambiente interno devem ser levados em consideração tanto aspectos tangíveis - como pessoas, equipamentos e materiais, quanto aspectos intangíveis - como cultura, processos, valores e conhecimento.

Os pontos fortes referem-se aos aspectos que devem ser conservados, já os pontos fracos são aqueles que devem ser eliminados ou reduzidos.

- Forças: características internas que representam uma facilidade para o alcance dos objetivos;
- Fraquezas: Fatores internos que oferecem risco à execução do processo.

A lista abaixo é uma relação exemplificativa e não exaustiva de pontos fortes e fracos que podem ser identificados no ambiente interno:

PONTO	CONSIDERAÇÕES
Infraestrutura física	<p>Pode ser vista como um ponto fraco ou forte, dependendo da avaliação dada pelos servidores que estão na localidade.</p> <p>É um importante indicativo, pois retrata um ponto objetivo, e é um importante indicador que influencia diretamente no coeso desenvolvimento dos trabalhos setoriais.</p>
Infraestrutura tecnológica	<p>Da mesma forma que a infraestrutura física, este pode representar um ponto forte ou não, a depender do nível de satisfação dos envolvidos.</p>
Qualificação dos servidores	<p>Grande parte dos serviços públicos, tem sua forma de atuação alterada por instrumentos legais que, quando não inovam, modificam a legislação, sendo, portanto, essencial que servidores se qualifiquem para a melhor aplicação da legislação vigente. Nesse cenário, qualificar o corpo técnico é fundamental e pode representar tanto um ponto forte quanto fraco, estando vinculado ao nível de qualificação aplicado neste setor.</p>
Clima organizacional	<p>É fundamental o mapeamento do clima organizacional dos setores. Muitos ajustes podem ser realizados após o mapeamento do clima organizacional, a partir do qual é possível identificar servidores insatisfeitos com sua lotação atual e que podem ser realocados em outros setores que necessitam de habilidades e qualificação que estes já possuem.</p>

PONTO	CONSIDERAÇÕES
Estruturação da carreira	Pode representar tanto um ponto forte quanto um ponto fraco do ambiente interno. Está diretamente vinculada ao fator de “estímulo de crescimento” dos servidores.
Integração entre as áreas	Um dos principais fatores a ser analisado e mensurado. Muitos dos riscos detectados têm como fonte de origem os ruídos de informações entre as áreas.
Comunicação interna	Está diretamente ligada à alta gestão e a forma como ela atua em divulgar as ações para conhecimento dos servidores. Sua assessoria é responsável por promover a comunicação de atividades setorizadas, para conhecimento de todos. Quando os servidores têm conhecimentos das ações desenvolvidas e em atuação, tendem inclusive a ajudar e promover melhorias em processos que tem mais afinidade.
Comunicação externa	Fator que deve ser levado em consideração sobretudo por retratar a comunicação das unidades com os interessados.
Planejamento elaboração execução integração	Pode representar tanto um ponto forte quanto um ponto fraco, dependendo do seu nível de implementação, aceitação. Planejamentos realizados “pro-forma”, tendem a causar mais um impacto negativo internamente (pois são rapidamente internalizados como fictícios) sendo por vezes, muito mais trabalhoso o processo de alteração desta imagem, entre os servidores.

PONTO	CONSIDERAÇÕES
Quantitativo de pessoal	<p>Pode representar tanto um ponto forte quanto um ponto fraco do ambiente interno. Esse indicativo deve ser avaliado em conjunto com outros, como: o clima organizacional e a qualificação dos servidores. Isso porque, rearranjos de servidores entre as unidades, podem eventualmente suprir quantitativos deficitários em determinados setores.</p>
Governança de dados	<p>É essencial que a governança de dados seja disciplinada na unidade, não apenas para atendimento da Lei de Acesso à informação e Lei Geral de Proteção de Dados, mas também para facilitar o acesso de informações dos servidores do próprio órgão, para desempenhar seus trabalhos.</p>
Plano de capacitação	<p>Diretamente ligado ao ponto qualificação dos servidores, serve para que a unidade determine metas de capacitação a serem atingidas para que os setores não fiquem “a descoberto”, de servidores com conhecimento específico em determinadas funções. Reforça-se ainda o fato de as novas avaliações de desempenho dos servidores, levarem o item capacitações realizadas, em consideração e a implementação de um plano de capacitação estimula que os servidores façam àquelas direcionadas ao interesse da instituição.</p>
Alocação de pessoal	<p>Outro fator que depende de outros pontos, sobretudo, clima, qualificação dos servidores, quantitativo etc.</p>

PONTO	CONSIDERAÇÕES
Gestão do conhecimento	Deve ser avaliado sobretudo em conjunto com a pesquisa do "Clima Organizacional", pois sua eficácia depende do real efeito sobre os servidores para ser considerada como satisfatória. Reforça-se o fato de não ser suficiente dispor de um legado de conhecimentos, mas é fundamental que a unidade preveja mecanismos de acessos, para que os servidores tenham acesso às bases de conhecimento da unidade.
Sistemas de Tecnologia de Informação	A avaliação se os sistemas existentes atendem às necessidades dos setores, sobretudo evitando retrabalho.
Legislação	As legislações podem tanto ser um ponto forte quanto fraco, pois mudanças no sistema legislativo podem sanear eventuais problemas existentes, mas trazem a necessidade de os servidores se capacitarem sobre os novos instrumentos legais vigentes.
Recursos orçamentários e financeiros	Aliados juntamente com um coeso planejamento, tendem a ser um excelente ponto forte. Entretanto, quando afetos a contingenciamentos, podem representar um ponto fraco.
Gestão por competências	Diretamente ligado aos quesitos: qualificação dos servidores, gestão do conhecimento e plano de capacitação, este item permite que a unidade possa gerir melhor as alocações de servidores, aproveitando o potencial de cada um. Notadamente quando um dos quesitos citados for falho, tem-se que este ponto tende a ser um ponto fraco.

PONTO	CONSIDERAÇÕES
Descontinuidade administrativa	A descontinuidade pode gerar desmotivação entre os servidores e descontinuidade de ações relevantes, devendo ser analisada caso a caso.
Estrutura de Governança	A depender do nível de maturidade e organização da unidade, pode representar tanto um ponto forte quanto um fraco.
Políticas de gestão de riscos	Sua implementação, ainda que em fase inicial demonstra ser um ponto forte da unidade pois representa, acima de tudo, compromisso e transparência em realizar melhorias em determinados processos.
Estrutura de integridade	Alinhado aos pontos de governança e gestão de riscos, representa um forte instrumento de mitigação aos riscos e governança da unidade.
Código de ética próprio	Essencial que cada unidade adote um código de ética, aderente à sua realidade.
Políticas de formação e aperfeiçoamento gerencial	Permite que novos servidores com perfil gerencial possam assumir funções na unidade. Fundamental para a promoção de novos talentos.

Especificamente sobre Planejamento do órgão/entidade, verificar se foram fixados objetivos em todos os níveis da unidade, se esses objetivos estão alinhados à missão e à visão da organização e se foram comunicados a todos os envolvidos.

- Ambiente Externo

Para a identificação das oportunidades e ameaças do ambiente externo devem ser levados em consideração aspectos como: relacionamentos, leis, tecnologia, aspectos sociais e econômicos, entre outros.

As oportunidades referem-se a aspectos a serem conquistados, enquanto as ameaças são aspectos que devem ser evitados ou terem os impactos minimizados.

- Oportunidades: situações positivas do ambiente externo que permitem o cumprimento da missão da unidade;
- Ameaças: situações externas, sobre as quais se tem pouco controle ou não há controle, que representam ou podem representar dificuldades para o cumprimento da missão da unidade.

A lista abaixo é uma relação exemplificativa e não exaustiva de oportunidades e ameaças que podem ser identificadas no ambiente externo:

- Restrições orçamentárias
- Interferência política sobre as ações técnicas
- Aumento da demanda dos serviços
- Inovações tecnológicas
- Desenvolvimento de Parcerias
- Benchmarking
- Networking em eventos
- Instabilidade política
- Capacidade de atração de investimentos
- Percepção da sociedade
- Legislação

Antes de seguir para a próxima etapa, sugere-se que o grupo de trabalho se reúna com a Alta Administração, para que sejam apresentadas as informações dessa etapa de diagnóstico e de alinhamento dos objetivos pretendidos com as estratégias de atuação da instituição.

Participantes desta etapa:

Equipe responsável pela Gestão de Riscos
Unidade de integridade (se houver)
NGER - Núcleo de Gestão Estratégica para Resultados
Alta gestão - validação da Matriz SWOT

Insumos: regimento interno; planejamento estratégico; relatórios de gestão; projetos; orçamentos; relatórios dos órgãos de fiscalização e controle; análises e qualquer outra documentação pertinente à organização e suas finalidades.

Produtos: Atas de reuniões; Matriz SWOT.

4.4 MAPEAMENTO DE PROCESSOS

O levantamento e desenho dos fluxos aprofundam o conhecimento em relação aos processos e atividades que serão objeto da avaliação de riscos.

A situação ideal é que a Cadeia de Valor e os Processos de Trabalho da unidade estejam mapeados.

- Cadeia de Valor é a representação de modelo que permite a visão lógica dos processos organizacionais.
- Processos de Trabalho representam detalhadamente as atividades, o processamento, as entradas e saídas de cada processo.

Ambos são importantes, mas não essenciais, para que a aplicação da metodologia de gestão de riscos de integridade tenha maior efetividade. Ao mapear os processos, mesmo que informalmente, é possível identificar pontos sensíveis para a identificação de potenciais riscos.

Para aplicação da metodologia, faz-se necessário que os macroprocessos/processos das unidades estejam claramente definidos e priorizados e desenhados - ainda que informalmente.

Recomendam-se as seguintes ações antes de iniciar a etapa de identificação dos riscos:

- Definição de um escopo que contemple os objetivos do processo/unidade/organização (objeto da gestão de riscos de integridade);
- Abranger todas as áreas, tecnologias, processos e pessoas envolvidas;
- Documentar o escopo definido;
- Aprovar o escopo com as partes interessadas;
- Comunicar todas as áreas envolvidas no processo.
- Mapeamento (ainda que informal) da Cadeia de Valor e dos Processos de Trabalho.

4.5 IDENTIFICAÇÃO DE RISCOS

Após a definição do processo a ser trabalhado e com os pontos críticos levantados no estabelecimento do contexto, é possível passar à identificação dos componentes do risco, compreendidos como causa (fonte), evento e consequência. A identificação dos riscos é o processo da busca, reconhecimento e descrição dos riscos (ISO 31000:2018).

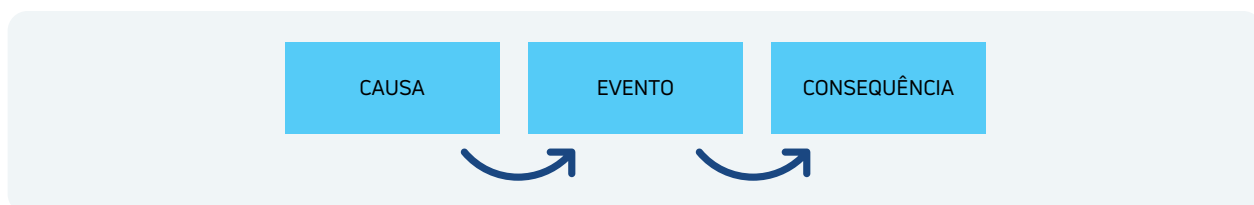
É importante que as pessoas envolvidas nesse processo tenham um conhecimento adequado sobre o objeto de gestão em avaliação, bem como sejam incentivadas a não se restringirem a conhecimentos do passado.

É fundamental estimular a participação dos gestores e dos servidores da linha da frente, pois eles são diretamente responsáveis pelas operações e serviços em toda a organização e podem contribuir para a identificação de riscos, oferecendo diferentes perspectivas e validando os resultados de mapeamento de riscos.

Riscos Inerentes

Inicialmente, os eventos de riscos identificados são aqueles chamados de riscos inerentes - riscos a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto (CGU, 2016).

Figura 8 – Trinômio do Risco



Fonte: Elaborada pelos autores com base na ABNT, 2021

Objetivos, eventos, causas e consequências

Sugere-se partir do objetivo da unidade/processo/atividade (objeto de gestão) para a identificação dos eventos de riscos de integridade relacionados a esse objetivo. Os eventos, causas (fontes) e consequências foram assim definidos pela norma ISO 31000:2018 (ABNT, 2018):

- O evento refere-se à ocorrência ou mudança em um conjunto específico de circunstâncias;
- A consequência é o resultado do evento que afeta os objetivos;
- A causa (fonte de risco) é o elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco.

Técnicas para identificação dos riscos:

- *Brainstorming em equipe (Tempestade de ideias)*

Consiste em permitir que os participantes contribuam com o máximo de ideias que conseguirem sem críticas ou censuras.

É fundamental que o brainstorming envolva um número elevado de participantes pois essa pluralidade de ideias é o pilar da técnica. Para que seja efetivo, o processo deve focar em quantidade e não em qualidade. Assim, é importante que a técnica seja completamente livre de críticas. Mesmo ideias que parecem ineficientes devem ser levadas em consideração, afinal, elas podem ser o ponto de partida para a construção de pensamentos mais aprofundados.

Para cada objetivo apresentado no estudo do processo, deve-se questionar quais os riscos para a integridade percebidos que podem comprometer o alcance desse objetivo, não se restringindo a eventos que já aconteceram no passado, mas ampliando a perspectiva para o que pode ocorrer, trazendo, assim, o elemento de incerteza do conceito do risco.

Nesta etapa, ocorre o preenchimento dos seguintes campos da Matriz de Risco: processo, objetivo, eventos de riscos.

- *Check-list:*

Também conhecida como folha de verificação, é um instrumento de coleta de dados referentes a uma situação específica.

Essa ferramenta de controle é baseada em uma lista com diversas condutas, nomes, tarefas e/ou atividades que devem ser seguidas para que determinado resultado seja alcançado de forma sistemática.

No final da etapa de identificação de riscos, ocorre o preenchimento dos seguintes campos da Matriz de Riscos: processo, objetivo e eventos de riscos.

Técnicas para identificação das causas:

- *Brainstorming em equipe (descrito nas técnicas de identificação):*

Após a identificação dos eventos de risco de integridade, investigar as causas (fontes) que podem favorecer a ocorrência desses eventos, descrevendo, além das causas, as consequências para o objetivo caso os eventos de risco ocorram.

- *5 por quês:*

Os 5 por quês é um método que consiste em, após definido exatamente o problema, questionar o por quê por até cinco vezes, até que se encontre a verdadeira causa. Pode-se ir até quantos por quês forem necessários, uma vez que um problema está acontecendo, sempre relacionado à causa anterior, e, dessa forma, será determinada a causa raiz do problema ao invés da fonte de problemas.

- *Entrevistas;*

As entrevistas podem ser utilizadas para obter informações detalhadas e opiniões. Elas podem ser estruturadas ou semiestruturadas - no primeiro tipo, há um conjunto de perguntas preparadas. Já na entrevista semiestruturada, há liberdade para explorar questões que não foram previamente preparadas.

- *Formulários.*

Normalmente, uma pesquisa envolve a aplicação de questionários/formulários, seja em papel ou por meio eletrônico. É importante que sejam respondidos por uma amostra representativa para ser suficiente para fornecer validade estatística. Também podem ser utilizadas perguntas livres, no entanto, é recomendável que não seja um número elevado de perguntas desse tipo, devido às dificuldades de análise.

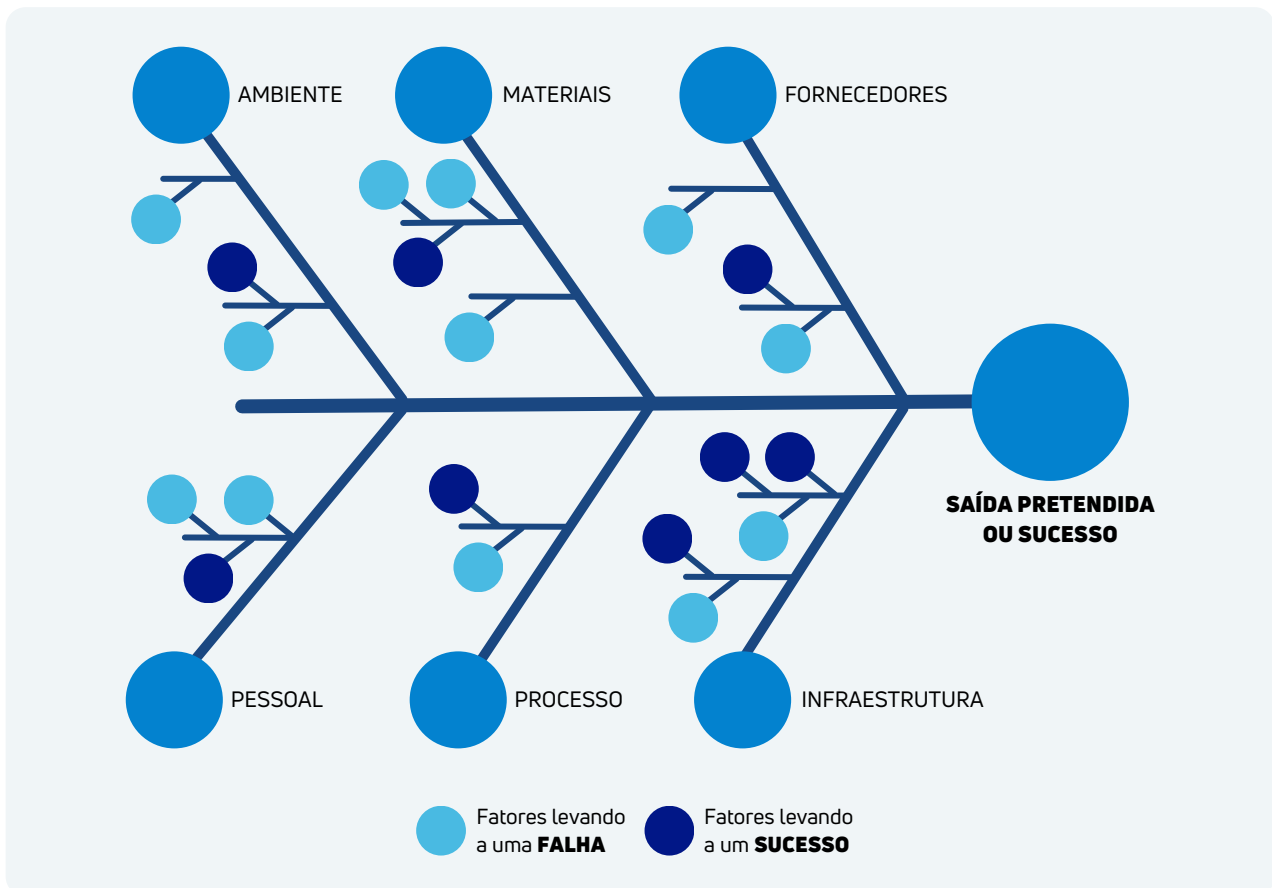
- *Diagrama de Ishikawa*

O diagrama de Ishikawa, que também é conhecido como espinha de peixe ou diagrama de causa e efeito, é uma ferramenta que possibilita entender melhor um processo ou um problema. e pode ajudar a equipe a chegar nas causas reais de problemas que acometem os processos organizacionais.

O propósito do Diagrama é descobrir os fatores que resultam em uma situação indesejada na organização, sendo uma forma sequencial e ordenada para descrever ou separar todas as fases e partes de um problema.

Parte-se dos efeitos dos problemas para a identificação das causas que o provocam, colocando-as em grau de importância da esquerda para a direita. Toda a equipe deve participar na identificação das causas, como forma de garantir que todas as causas potenciais sejam consideradas.

Figura 9 – Diagrama de Ishikawa



Fonte: Elaborado pelos autores com base no Modelo do Diagrama de Ishikawa

Após esta etapa, é possível o preenchimento da coluna causas (fontes) da Matriz de Riscos.

Lista de eventos de riscos de integridade

Sugere-se a utilização da lista de eventos de riscos de integridade, anexo II desse Guia para auxiliar na compreensão de eventos de riscos de integridade. A lista não é exaustiva, podendo completar outros riscos não considerados inicialmente.

Participantes desta etapa:

- Equipe responsável pela gestão de riscos;
- Servidores que trabalham diretamente no processo organizacional;
- Unidade de Integridade (se houver).

Para fins de levantamento das informações desta etapa e documentação dos trabalhos, poderão ser utilizados os seguintes insumos:

- Entrevistas
- Formulários
- Normativos;
- Fluxos processuais.

Produtos desta etapa:

Esperam-se como produtos desta etapa atas de reuniões e uma lista abrangente de eventos de riscos de integridade.

4.6 ANÁLISE DOS RISCOS

Refere-se ao desenvolvimento da compreensão sobre o risco e à determinação do nível de risco. O resultado da análise gera a Matriz de Probabilidade x Impacto ou Matriz de Calor.

A análise de risco permite o entendimento do risco e fornece uma entrada para a etapa de avaliação de riscos e, conseqüentemente, para a tomada de decisões sobre o tratamento dos riscos.

Nessa etapa, determina-se a probabilidade de o risco acontecer e o impacto de sua ocorrência sobre um objetivo definido e atribuem-se valores padronizados de frequência de ocorrência (probabilidade) e consequência da ocorrência (impacto).

- Avaliação do Impacto do risco sobre o objetivo/resultado: o impacto mede o potencial comprometimento do objetivo/resultado.
- Avaliação da Probabilidade de ocorrência do risco é a chance de o evento ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado.

Escalas de Probabilidade e Impacto

Sugere-se a utilização de escalas semiquantitativas para determinação das variáveis Probabilidade e Impacto. As escalas possuem classificação numérica e o produto dessas variáveis resulta no nível de risco.

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

Quadro 1 - Escala de Probabilidade

RARO	1	Acontece apenas em situações excepcionais, mas não há nada nas circunstâncias que indica essa possibilidade.
POUCO PROVÁVEL	2	O histórico conhecido aponta para baixa frequência de ocorrência o prazo associado ao objetivo. As circunstâncias pouco indicam essa possibilidade.
PROVÁVEL	3	As circunstâncias indicam moderadamente a possibilidade de ocorrência do evento. O evento repete-se com frequência razoável ou há indícios que possa ocorrer no prazo associado ao objetivo.
MUITO PROVÁVEL	4	As circunstâncias indicam fortemente a possibilidade de ocorrência do evento. O evento repete-se com frequência elevada ou há muitos indícios de que ocorrerá no prazo associado ao objetivo.
PRATICAMENTE CERTO	5	As circunstâncias indicam claramente a possibilidade de ocorrência do evento. O evento ocorrerá de forma quase garantida no prazo associado ao objetivo.

Fonte: Tribunal de Contas da União, 2020

Quadro 2 – Escala de Impacto

MUITO BAIXO	1	Compromete minimamente o atingimento do objetivo; não altera o alcance do objetivo/resultado. Mínimo impacto nos objetivos.
BAIXO	2	Compromete em alguma medida o atingimento do objetivo, mas não impede o alcance da maior parte do objetivo/resultado. Pequeno impacto nos objetivos.
MÉDIO	3	Compromete razoavelmente o alcance do resultado/objetivo. Moderado impacto nos objetivos.
ALTO	4	Compromete a maior parte do atingimento do objetivo/resultado. Significativo impacto nos objetivos.
MUITO ALTO	5	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado. Total impacto nos objetivos.

Fonte: Tribunal de Contas da União, 2020

Riscos residuais

Nessa fase, é realizada uma série de questionamentos e reunidos elementos comprobatórios em relação à adoção de normas, padrões e procedimentos que visem identificar, prevenir e/ou coibir a prática de condutas violadoras de integridade pública.

A seguir, são levantados e avaliados os controles já estabelecidos em relação aos riscos com a finalidade de se obter os riscos residuais. O risco residual é "o risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco" (CGU, 2016).

São exemplos de controles:

- Controles preventivos: requisitos/checklists definidos para o processo; capacitação dos servidores.
- Controles de atenuação e recuperação: plano de contingência, tomada de contas especiais; procedimento apuratório.

É necessário realizar uma análise da eficácia geral dos controles existentes e, segundo a Norma da ABNT NBR ISO 31010:2021, convém que os seguintes aspectos dos controles sejam considerados:

- o mecanismo pelo qual os controles se destinam a modificar o risco;
- se os controles existentes são capazes de operar como planejado e se estão alcançando os resultados esperados;
- se existem deficiências no projeto dos controles ou na forma como eles são aplicados;
- se existem lacunas nos controles;
- se os controles funcionam independentemente ou se precisam funcionar coletivamente para serem eficazes;
- se existem fatores, condições, vulnerabilidades ou circunstâncias que podem reduzir ou eliminar a eficácia do controle, incluindo falhas de causa comuns;
- se os próprios controles introduzem riscos adicionais

Escala de Análise de Controles

Para avaliação dos controles existentes sugere-se a utilização de escalas de avaliação. A seguir, são apresentadas escalas de avaliação de controles em relação ao desenho do controle e quanto à sua operação:

Quadro 3 – Escalas de Avaliação de controles

DESENHO	
1	Não há sistema de controle.
2	Há procedimentos de controle para algumas atividades, porém informais.
3	Controles não foram planejados formalmente, mas são executados de acordo com a experiência dos servidores.
4	É desenhado um sistema de controle integrado adequadamente planejado, discutido e documentado. O sistema de controle vigente é eficaz.
5	O sistema de controle é eficaz na gestão de riscos (adequadamente planejado, discutido, testado e documentado com correções ou aperfeiçoamento planejados de forma tempestiva.
OPERAÇÃO	
1	Controle não executado.
2	Controle parcialmente executado e com deficiências.
3	Controle parcialmente executado.
4	Controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade.
5	Controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.

Matriz de Probabilidade x Impacto

A Matriz de Probabilidade x Impacto ou Matriz de Calor fornece uma apresentação visual da do nível de risco.

No quadrante verde, ficam os riscos de baixa severidade; nos amarelados, aqueles de média severidade; e, no vermelho, os riscos mais graves, de alta severidade.

Figura 10 – Matriz de Probabilidade x Impacto

IMPACTO	MUITO ALTO 5	5 RM	10 RM	15 RA	20 RE	25 RE
	ALTO 4	4 RB	8 RM	12 RA	16 RA	20 RE
	MÉDIO 3	3 RB	6 RM	9 RM	12 RA	15 RA
	BAIXO 2	2 RB	4 RB	6 RM	8 RM	10 RM
	MUITO BAIXO 1	1 RB	2 RB	3 RB	4 RB	5 RM
		RARO 1	POUCO PROVÁVEL 2	PROVÁVEL 3	MUITO PROVÁVEL 4	PRATICAMENTE CERTO 5
		PROBABILIDADE				

CLASSIFICAÇÃO		FAIXA
RB	Risco Baixo	0-4,99
RM	Risco Médio	5-11,99
RA	Risco Alto	12-19,99
RE	Risco Extremo	20-25

Essa Matriz orienta a seleção dos riscos (priorização) que demandam acompanhamento e colabora para a avaliação de medidas de tratamento aos riscos.

Técnicas para análise dos riscos:

- *Brainstorming em equipe (Tempestade de ideias)*

Descrição no tópico de técnicas para identificação dos riscos

Sugestão de aplicação:

- 1 - Iniciar a avaliação de riscos utilizando a relação de eventos de riscos identificados na etapa anterior;
- 2 - Antes de considerar a probabilidade e o impacto de cada evento, ressaltar a todos os participantes dessa etapa, que os eventos devem ser considerados como se não houvesse a adoção de quaisquer controles de gestão.
- 3 - Para cada evento de risco, utilizando-se as escalas de probabilidade e impacto, debater com todos os participantes qual a percepção em relação a esses dois fatores.
- 4 - Após o consenso, atribuir os valores na planilha. Se não houver consenso, é prudente que o maior valor percebido pelo(s) participante(s) seja atribuído.
- 5 - Atribuídos os valores de probabilidade e impacto para todos os eventos de risco, realizar o cálculo do Nível do Risco, multiplicando-se os valores atribuídos de Probabilidade e Impacto de cada risco. Esse nível de risco refere-se ao risco inerente.

6 - A seguir, verificar a existência de eventual atividade de controle que previna ou mitigue o risco de integridade identificado;

7 - Com base na existência ou não do controle bem como de seu desenho e funcionamento, avaliar os controles existentes, destacando-se todos os seus atributos. Essa avaliação dos controles será utilizada para se chegar ao risco residual. É sobre o risco residual que deverá ser avaliada a necessidade de aplicar novas medidas de tratamento.

Apresenta-se, a seguir, sugestão de participantes para a etapa de Análise de Riscos:

Participantes:

- Grupo de Trabalho de Gestão de Riscos;
- Instância de Integridade - se houver;
- Servidores com experiência no processo organizacional.

Para análise dos riscos identificados, sugere-se a utilização dos seguintes insumos:

Insumos:

- Lista de eventos de riscos, causas e consequências - levantada na etapa anterior;
- Levantamento dos controles de gestão existentes em relação aos riscos identificados;
- Entrevistas;
- Formulários.

Espera-se que os trabalhos desta etapa estejam consolidados nos seguintes produtos:

Produtos

- Matriz de Riscos (colunas: probabilidade, impacto e controles existentes);
- Matriz Probabilidade x Impacto;
- Atas de reuniões;

4.7 AVALIAÇÃO DOS RISCOS

A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável. O apetite a risco é o nível de que uma organização está disposta a aceitar.

Conforme disposto na ABNT NBR ISO 31010:2021:

“Uma avaliação da significância de um risco em comparação com outros riscos frequentemente é baseada em uma estimativa da magnitude do risco em comparação com critérios diretamente relacionados aos limites estabelecidos em torno dos objetivos da organização. A comparação com estes critérios pode informar uma organização sobre quais riscos convém focar no tratamento, com base em seu potencial de direcionar resultados fora dos limites estabelecidos em torno dos objetivos.”

A comparação dos resultados da análise de riscos com os critérios definidos para probabilidade e impacto e, posteriormente, a avaliação dos controles internos em funcionamento sobre os riscos atuais identificados, permitem determinar se o nível de risco é aceitável ou tolerável, auxiliando na decisão sobre quais riscos necessitam de tratamento e a prioridade para implementação do tratamento.

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Cabe à gestão, diante da lista de riscos ordenados por nível de risco, decidir quais terão ações mitigadoras.

Apresenta-se abaixo sugestão de participantes para a etapa de Avaliação de Riscos:

Participantes

- Instância de Integridade - se houver
- Servidores com experiência no processo organizacional
- Servidores com poder de decisão

Para análise dos riscos identificados, sugere-se a utilização dos seguintes insumos:

Insumos

- Matriz de Riscos
- Mapa de Calor
- Apetite a risco do órgão/entidade

Espera-se que os trabalhos desta etapa estejam consolidados nos seguintes produtos:

Produtos

- Atas de reuniões
- Relação dos riscos de integridade avaliados

4.8 TRATAMENTO DOS RISCOS

Compreende o planejamento e a realização de ações para modificar o nível do risco. O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco.

O tratamento dos riscos de integridade identificados e avaliados visa o estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, devendo ser observada a relação custo-benefício.

Ações que podem ser realizadas quanto ao risco:

- a) evitar o risco, ao eliminar a causa raiz do risco, implementando ações para eliminar a probabilidade de ocorrência do evento de riscos;
- b) mitigar o risco, quando busca reduzir a probabilidade de ocorrência ou o impacto de um risco a um nível aceitável;
- c) transferir o risco, ao conferir à outra parte a responsabilidade pela gestão ou do impacto gerado pelo evento de risco; ou
- d) aceitar o risco, adotado nos casos em que a probabilidade de ocorrência e o impacto dos eventos de riscos são baixos, de forma que se considera aceitar o risco.

As medidas de respostas aos riscos devem considerar, inicialmente, as fontes e causas dos riscos e, adicionalmente, podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize.

Plano de Ação

O Plano de ação é documento que prevê perspectivas de implementação a curta, médio e longo prazos, para o cumprimento das metas.

Fica a critério dos gestores dos órgãos/entidades a escolha do Plano de Ação a ser elaborado, sendo recomendável que seja o mais simples possível, com o objetivo de facilitar a sua operação e acompanhamento.

Sugere-se a utilização do modelo 5W2H para o controle das informações do Plano de Ação:

- O que fazer
- Por que fazer
- Quem faz
- Onde
- Quando
- Como
- Quanto custa

Produtos desta etapa

- Atas de reuniões
- Plano de Ação

4.9 MONITORAMENTO

Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

É recomendável que seja designada uma instância ou comitê - ainda que não seja permanente, que fique responsável pelo acompanhamento, monitoramento e controle das ações e medidas de integridade que serão implementadas.

Sempre que for identificada uma necessidade de ajuste de ações, metas, prazos, resultados e responsáveis, é fundamental que ocorra uma revisão do que foi planejado com a finalidade de fazer uma adequação à realidade dos órgãos e entidades.

4.10 COMUNICAÇÃO

A comunicação trata-se de uma ferramenta estratégica e deve ser periódica, sistemática e alcançar toda a organização. É importante divulgar o andamento das ações periodicamente, de maneira a fomentar o envolvimento de todos.



5. CONSIDERAÇÕES FINAIS

A implementação da Gestão de Riscos de integridade nos órgãos e entidades do Poder Executivo do Estado de Mato Grosso subordina-se ao interesse público e deve ser realizada de forma sistemática, estruturada, oportuna e documentada.

A Gestão de Riscos deve integrar-se ao processo de planejamento estratégico do órgão/entidade e aos seus desdobramentos - às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização.

A gestão de riscos, elemento fundamental da governança pública, não elimina o risco, seu objetivo é garantir que a organização conheça os seus riscos e possa lidar com eles de maneira apropriada. A adoção de controles apropriados busca mitigar os efeitos dos riscos e fornecer maior garantia de que os objetivos da organização serão alcançados.

Os resultados da Gestão de Riscos devem ser utilizados para apoiar o órgão na melhoria contínua do desempenho e dos processos de gerenciamento de riscos, controle e governança e permitir à administração a oportuna utilização das informações sobre os riscos no processo de tomada de decisão.



6. REFERÊNCIAS

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. Gestão de Riscos: Diretrizes.

BRASIL. Tribunal de Contas da União. Manual de Gestão de Riscos do TCU, Brasília, DF, 2020.

Norma Brasileira ABNT NBR ISO 31000:2018 Segunda Edição, 2018.

COSO ERM. Gerenciamento de Riscos Corporativos - Integrado com Estratégia e Performance, 2017.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP. Curso Fundamentos da Integridade Pública: Prevenindo a Corrupção.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO CGU. Guia Prático de Implementação de Programa de Integridade Pública: Orientações para a Administração Pública Direta, Autárquica e Fundacional. Abril, 2018.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO CGU. Guia Prático de Gestão de Riscos: Orientações para a Administração Pública Direta, Autárquica e Fundacional. Setembro, 2018.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO CGU. Instrução Normativa Conjunta MP/CGU nº 01/2016, Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, Brasília, mai. 2016.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO CGU. Manual para Implementação de Programas de Integridade: orientações para o setor público. Brasília, DF, jul. 2017.

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO CGU. Portaria nº 57, de 04 de janeiro de 2019, que "Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências".

ORGANIZAÇÃO PARA COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO OCDE. Recomendação do Conselho da OCDE sobre Integridade Pública. Paris, 2017. Disponível em: <http://www.oecd.org/gov/ethics/integrity-recommendation-brazilian-portuguese.pdf>.



7. ANEXOS

ANEXO I - LISTA DE RISCOS DE INTEGRIDADE

Nº	RISCOS PARA A INTEGRIDADE	Nº	FATORES DE RISCO
1	Abuso de posição ou poder em favor de interesses privados	1.1	Concessão de cargos ou vantagens em troca de apoio ou auxílio
		1.2	Esquivar-se do cumprimento de obrigações
		1.3	Falsificação de informação para interesses privados
		1.4	Concessão de patrocínios e/ou incentivos a entidades privadas.
		1.5	Outras formas de favorecimento – a outros ou a si mesmo
2	Nepotismo	2.1	Contratação de familiares para cargos em comissão e função de confiança
		2.2	Contratação de familiares para vagas de estágio e de atendimento a necessidade temporária de excepcional interesse público
		2.3	Contratação de pessoa jurídica de familiar por agente público responsável por licitação
		2.4	Nepotismo cruzado, quando autoridades de um órgão nomearem familiares de autoridades de outro órgão, compensando-se reciprocamente.
		2.5	Contratação de familiares para prestação de serviços terceirizados.
		2.6	Outras nomeações, contratações não previstas expressamente anteriormente, com indícios de influência

Nº	RISCOS PARA A INTEGRIDADE	Nº	FATORES DE RISCO
3	Conflito de interesses	3.1	Prestar serviço a pessoa física ou jurídica com a qual tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego;
		3.2	Aceitar cargo de administrador ou conselheiro ou estabelecer vínculo profissional com pessoa física ou jurídica que atue em atividade relacionada à área de competência do cargo ou emprego ocupado;
		3.3	Celebrar contratos de serviço, consultoria, assessoramento ou atividades similares com órgãos ou entidades do Poder Executivo vinculados ao órgão ou entidade em que tenha ocupado o cargo ou emprego; ou
		3.4	Intervir em favor de interesse privado, direta ou indiretamente, perante órgão ou entidade em que haja ocupado cargo ou emprego ou com o qual tenha estabelecido relacionamento relevante em razão do exercício desse mesmo cargo.
		3.5	Exercer, direta ou indiretamente, atividade que em razão da sua natureza seja incompatível com as atribuições do cargo ou emprego, considerando-se como tal, inclusive, a atividade desenvolvida em áreas ou matérias correlatas.
		3.6	Praticar ato em benefício de interesse de pessoa jurídica de que participe o agente público, seu cônjuge, companheiro ou parentes, consanguíneos ou afins, em linha reta ou colateral, até o terceiro grau, e que possa ser por ele beneficiada ou influir em seus atos de gestão.

Nº	RISCOS PARA A INTEGRIDADE	Nº	FATORES DE RISCO
4	Pressão interna ou externa ilegal ou antiética para influenciar agente público a atuar de maneira parcial ou sem autonomia técnica.	4.1	Pressões implícitas ou explícitas de natureza hierárquica
		4.2	Pressões implícitas ou explícitas de colegas
		4.3	Pressões implícitas ou explícitas de natureza política ou social
5	Solicitação ou recebimento de vantagem indevida	5.1	Adiantar ou atrasar intencionalmente a tramitação de processos.
		5.2	Deixar de aplicar penalidades em situações comprovadamente irregulares.
		5.3	Criar dificuldades e/ou embaraço com a finalidade de auferir vantagem.
		5.4	Perda de prazo em processos administrativos.
		5.5	Receber presente de quem tenha interesse em decisão do agente público ou de colegiado do qual este participe fora dos limites e condições estabelecidos em regulamento.
6	Utilização de recursos públicos em favor de interesses privados.	6.1	Apropriação indevida
		6.2	Irregularidades em contratações públicas.
		6.3	Concessão de patrocínios e/ou incentivos a entidades privadas.

Nº	RISCOS PARA A INTEGRIDADE	Nº	FATORES DE RISCO
7	Conduta profissional inadequada	7.1	Deixar de realizar as atribuições conferidas com profissionalismo, honestidade, imparcialidade, responsabilidade, seriedade, eficiência, qualidade e/ou urbanidade.
8	Uso indevido de autoridade contra o exercício profissional	8.1	Atentar contra os direitos e garantias legais assegurados ao exercício profissional com abuso ou desvio do poder hierárquico ou sem competência legal para atender interesse próprio ou de terceiros
		8.2	Ato movido por capricho, maldade, perseguição, vingança ou outra motivação que não se enquadre no princípio da moralidade dos atos da administração pública.
		8.3	Realizar transferência ou dispensa arbitrária de algum trabalho relevante, pressionar servidor a omitir-se, por estar exercendo suas funções em órgãos/entidades do próprio Estado, exigindo o cumprimento da lei.
		8.4	Proceder a qualquer tentativa de obrigar o servidor a executar o que evidentemente não está no âmbito das suas atribuições ou a deixar de executar o que está previsto.
9	Uso indevido de autoridade contra a honra e o patrimônio	9.1	Atentar contra a honra ou o patrimônio de pessoa natural (no caso, servidor público) ou jurídica com abuso ou desvio de poder ou sem competência legal para atender interesse próprio ou de terceiros.

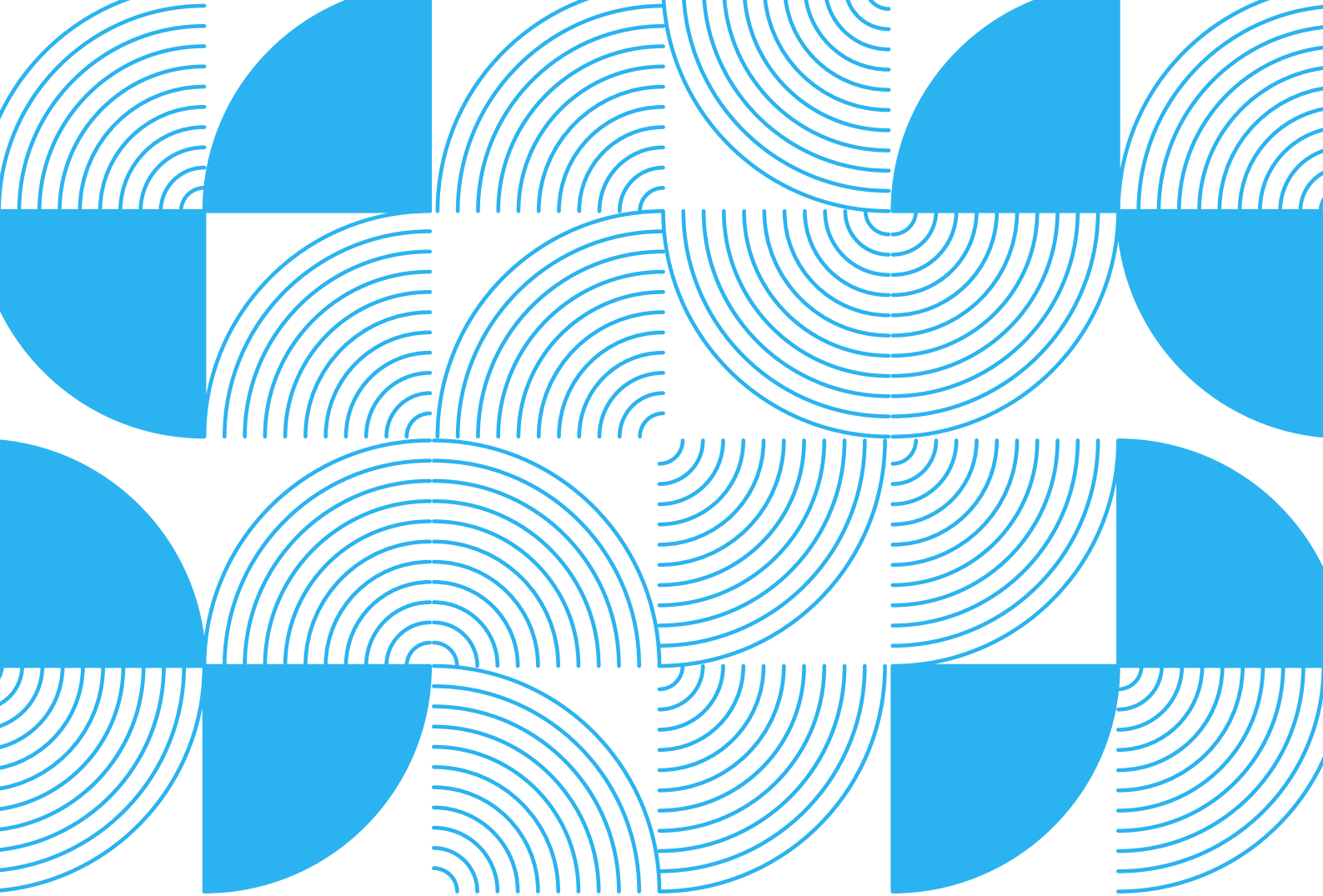
Nº	RISCOS PARA A INTEGRIDADE	Nº	FATORES DE RISCO
10	Uso indevido e/ou manipulação de dados e informações	10.1	Divulgar ou fazer uso de informação privilegiada, em proveito próprio ou de terceiros, obtida em razão das atividades exercidas, bem como permitir o acesso de pessoas não autorizadas a sistemas de informações da Administração Pública.
		10.2	Fornecer ou divulgar dados ou informações intencionalmente de forma incorreta, incompleta ou imprecisa, bem como inserir ou facilitar a inserção de dados falsos em sistemas informatizados para atender interesse próprio ou de terceiros.
		10.3	Restringir ou retardar a publicidade ou acesso a dados ou informações, ressalvados os protegidos por sigilo, bem como extraviar ou inutilizar dados e informações para atender interesse próprio ou de terceiros.
11	Desvio de pessoal e/ou recursos materiais	11.1	Desviar ou utilizar, em obra ou serviço particular, veículos, máquinas, equipamentos ou material de qualquer natureza, de propriedade ou à disposição de entidades públicas, bem como o trabalho de servidores públicos, empregados ou terceiros contratados por essas entidades para fins particulares ou para desempenho de atribuição que seja de sua responsabilidade ou de seu subordinado.

Nº	RISCOS PARA A INTEGRIDADE	Nº	FATORES DE RISCO
12	Interferências externas e/ou políticas e/ou alterações no cenário político	12.1	As nomeações para os cargos da alta administração não observarem critérios técnicos e de competência diretamente relacionados com as atribuições da secretaria
		12.2	Relacionados com mudanças de governo e/ou de políticas de governo que possam implicar em supressão de atribuições, esvaziamento do órgão e/ou desaparelhamento por falta de recursos.
		12.3	Descontinuidade da gestão com mudanças no alto escalão do governo e do órgão podem influenciar a continuidade de programas e projetos.
		12.4	As mudanças legislativas que possam implicar no modelo de subordinação e reporte, com comprometimento da independência ou alterações e/ou supressões de atribuições fundamentais ao exercício da atividade.
		12.5	Interferência de órgãos diversos na atuação da CGE, como PGE, TCE, MP; com demandas fora das nossas obrigações legais, comprometendo a atuação nas áreas/escopos definidos, por faltar estrutura para atender todas as demandas e ainda manter a realização dos trabalhos identificados por meio de análise de risco.
		12.6	Mudanças de governo e/ou de políticas de governo que possam implicar em supressão de atribuições, esvaziamento do órgão e/ou desaparelhamento por falta de recursos.

ANEXO II - MODELO PARA MATRIZ DE RISCOS

MATRIZ DE RISCOS												
ATIVIDADE	OBJETIVO	FATORES DE RISCO	5 por quês?	Categoria	Risco Inerente				Risco Residual			Tratamento
1.	1.	1. 2. 3.	1.		P	I	P x I	Controles existentes	P	I	P x I	
			2.									
			3.									
			4.									
			5.									
OBJETIVO	FATORES DE RISCO	5 por quês?	Categoria	Risco Inerente				Risco Residual			Tratamento	
2.	1. 2. 3.	1. 2. 3. 4. 5.	1.		P	I	P x I	Controles existentes	P	I	P x I	
			2.									
			3.									
			4.									
			5.									
ATIVIDADE	OBJETIVO	FATORES DE RISCO	5 por quês?	Categoria	Risco Inerente				Risco Residual			Tratamento
2.	1.	1. 2. 3.	1.		P	I	P x I	Controles existentes	P	I	P x I	
			2.									
			3.									
			4.									
			5.									

Roteiro resumido para preenchimento	Campo a ser preenchido
Após a definição da área a ser trabalhada e mapeamento, ainda que informal, das atividades desenvolvidas e dos fluxos processuais: listar todas as atividades que são de competência daquela área/setor.	Atividade
Para cada atividade que é competência daquela área/setor, listar o objetivo principal dessa atividade.	Objetivo
Utilizar a aba Riscos e fatores de riscos para identificar quais são os riscos de integridade relacionadas à atividade que podem comprometer o alcance do objetivo.	Riscos
Utilizar a aba Riscos e fatores de riscos para identificar quais são os fatores de riscos de integridade relacionadas à atividade que podem comprometer o alcance do objetivo.	Fatores de risco (eventos de risco)
Realizar a identificação das causas que podem levar à ocorrência dos riscos. Causa é o elemento que, individualmente ou combinado, tem o potencial de dar origem ao risco.	5 por quês? (CAUSAS: fontes de riscos)
Identificar a categoria do risco. Exemplos de categorias: Integridade / Operacional / Estratégico. O risco pode fazer parte de mais de uma categoria. As categorias de riscos estão nas legendas abaixo dessa matriz.	Categoria
Realizar análise de probabilidade e impacto dos riscos inerentes. Risco inerente é o risco a que se está exposto sem considerar quaisquer ações gerenciais/controles. Probabilidade é a chance de o evento de risco ocorrer dentro do prazo previsto para se alcançar o objetivo/resultados. O impacto mede o potencial comprometimento do objetivo/resultados. O impacto mede o potencial comprometimento do objetivo/resultados.	Riscos inerentes - Probabilidade e Impacto
Realizar análise de probabilidade e impacto dos riscos residuais. Risco residual é o risco a que se está exposto após a implementação de ações gerenciais / controles para o tratamento do risco.	Riscos residuais: Probabilidade e Impacto
Descrever as medidas que serão adotadas para o tratamento do risco. Compreende o planejamento e a realização de ações para modificar o nível do risco. Leva-se em consideração o apetite a risco da organização, da área/setor e a relação custo-benefício.	Tratamento



CGEMT