MANUAL DE GESTÃO DE RISCOS CGE/PA

Controladoria de Auditoria Interna
C-AUDIN

CGE
CONTROLADORIA-GERAL
DO ESTADO DO PARÁ

GOVERNO DO
ESTADO DO PARÁ

Belém – PA Julho/2024

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

INTRODUÇÃO

A Controladoria-Geral do Estado do Pará (CGE/PA), convergente às boas práticas de governança, tem priorizado estratégias de aperfeiçoamento de suas atividades para alcançar os objetivos estratégicos de forma estruturada, transparente e eficiente.

Dessa forma, a implementação e o desenvolvimento da gestão de riscos na instituição representa um processo de aprendizagem que se inicia com a conscientização sobre sua importância e desenvolve-se com o estabelecimento de práticas e estruturas necessárias para a efetivação do gerenciamento de riscos.

Nesse sentido, foi instituída a Política de Gestão de Riscos da CGE/PA, por meio da Portaria nº 72/2024, publicada no DOE em 10 de maio de 2024, estabelecendo diretrizes e recomendações, bem como estipulando princípios, conceitos e

orientações, que deverão embasar o processo de gerenciamento de riscos, o que representa importante mecanismo de governança, devendo ser entendido como um processo contínuo e dinâmico a ser aplicado em todo o órgão.

Ademais, com vistas a propiciar o alcance das metas e objetivos estratégicos da instituição, o Processo de Gestão de Riscos surge como ferramenta que visa a coleta de evidências para avaliação e tratamento das fontes de riscos, assim como a implementação de controles contingenciais para minimizar a probabilidade de ocorrência dos eventos de risco e/ou o impacto das suas consequências.

Posto isso, o presente Manual de Gestão de Riscos da CGE/PA pretende contribuir para a implementação da gestão de riscos na CGE/PA, por meio do fornecimento de uma base teórica diversificada e simplificada às partes envolvidas em tal processo. Por consequência, o intuito é potencializar o aperfeiçoamento dos controles internos, minimização dos riscos a níveis aceitáveis e tomada de decisão fundamentada e tempestiva, estando sua base teórico-conceitual respaldada na Política de Gestão de Riscos desta CGE (Portaria nº 72/2024), bem como no Modelo *Committee of Sponsoring Organizations of the Treadway Commission – COSO (2017) – Enterprise Risk Management (ERM)*; na ABNT NBR ISO 31000:2018 - Gestão de Riscos – Diretrizes; na ABNT NBR ISO 31010:2021 - Gestão de Riscos - Técnicas para o Processo de Avaliação de Riscos; e na ABNT NBR ISO 31073:2022 – Vocabulário da Gestão de Riscos.

1. OBJETIVOS DA GESTÃO DE RISCOS NA CGE/PA

A Gestão de Riscos da CGE/PA tem como objetivos fundamentais, identificar, analisar, avaliar e tratar os riscos afetos ao órgão, aprimorando a eficiência, a eficácia, a efetividade, a integridade, a segurança e a transparência de suas atividades, seja da

sua área meio, seja da sua área fim.

Ademais, buscará minimizar e/ou usufruir dos riscos de forma a maximizar os resultados e proteger-se contra ameaças potenciais, aproveitar oportunidades, tomar decisões informadas, garantir a sobrevivência, o sucesso a longo prazo e alcançar os objetivos organizacionais. Alguns dos principais objetivos incluem:

a) Aumentar a probabilidade de alcance dos objetivos institucionais;
b) Melhorar a identificação de oportunidades e ameaças ao órgão;
c) Oferecer subsídios para a tomada de decisões com vistas ao alcance dos objetivos e missão organizacionais;
d) Fortalecer a governança institucional;
e) Fomentar a accountability;
f) Ampliar a transparência e a eficiência;
g) Promover melhorias contínuas nas atividades e processos de trabalho;
h) Fortalecer a cultura de gestão de riscos e controles internos; e
i) Alinhar a tolerância a risco à estratégia adotada.

2. GLOSSÁRIO BÁSICO

Os conceitos abaixo estão descritos com base na ABNT NBR ISO 31000:2018 e na ABNT NBR ISO 31073:2022, as quais versam sobre o vocabulário de gestão de riscos, cabendo ao tópico apenas aos conceitos entendidos como pertinentes ao conteúdo deste documento:

Risco: Efeito da incerteza. Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos e pode abordar, criar ou resultar em oportunidades e ameaças.

Objetivo: Resultado a ser alcançado. Um objetivo pode ser estratégico, tático ou operacional. Objetivos podem se relacionar a diferentes disciplinas (como finanças, saúde, segurança e metas ambientais) e podem ser aplicados em diferentes níveis (como estratégico, da organização, projeto, produto e processos). Um objetivo pode ser expresso de outras formas, por exemplo, como um resultado pretendido, um propósito, um critério operacional, como objetivo de um sistema de gestão, ou pelo uso de outras palavras com significado similar (por exemplo, finalidade, meta, alvo).

Incerteza: Estado, mesmo parcial, de deficiência de informação relacionada à compreensão ou conhecimento.

Gestão de Riscos: Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

Política de Gestão de Riscos: Declaração das intenções e diretrizes gerais de uma organização relacionada à gestão de riscos.

Processo de Gestão de Riscos: Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto e na identificação, análise, avaliação e tratamento, monitoramento e análise crítica dos riscos.

Parte Interessada (Stakeholder): Pessoa ou organização que pode afetar, ser afetada por uma decisão ou atividade.

Contexto Externo: Ambiente externo no qual a organização busca atingir seus objetivos.

Contexto Interno: Ambiente interno no qual a organização busca atingir seus objetivos

Critério de Risco: Termos de referência diante dos quais a significância de um risco é avaliada.

Organização: pessoa ou grupo de pessoas que possuem suas próprias funções com responsabilidades, autoridades e relações para alcançar seus objetivos.

Processo de Avaliação de Riscos: processo global de identificação de riscos, análise de riscos e avaliação de riscos.

Identificação de Riscos: processo de busca, reconhecimento e descrição de riscos.

Fonte de Risco: elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco.

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias.

Proprietário de Riscos: pessoa ou entidade com responsabilização e a autoridade para gerenciar riscos.

Vulnerabilidade: propriedades intrínsecas de algo, resultado em suscetibilidade a uma fonte de risco que pode levar a um evento como uma consequência.

Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades.

Fator de Risco: fator que tem uma grande influência no risco.

Avaliação de Riscos: processo de comparar resultados da análise de riscos com os critérios de risco para determinar se o risco é aceitável ou tolerável.

Apetite por Riscos: quantidade e tipo de riscos que uma organização está disposta a buscar ou reter.

Tolerância ao Risco: disposição da organização ou da parte interessada em suportar o risco residual a fim de atingir seus objetivos.

Aversão a Riscos: atitude de afastar-se de riscos.

Agregação de Riscos: combinação de uma série de riscos em um único risco para desenvolver uma compreensão mais completa do risco global.

Aceitação de Risco: decisão consciente de assumir um risco específico.

Tratamento de Riscos: processo para modificar os riscos.

Controle de Risco: medida que mantém e/ou modifica o risco.

Ação de evitar o risco: decisão informada de não se envolver ou retirar-se de uma

atividade, a fim de não ser exposto a um risco específico.

Compartilhamento de Riscos: forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes.

Financiamento de Riscos: forma de tratamento de riscos que envolve arranjos contingentes para a provisão de fundos, a fim de atender ou modificar consequências financeiras, caso ocorram.

Retenção de Riscos: aceitação do benefício potencial de ganho ou do ônus da perda, a partir de um risco específico.

Risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco Residual: risco remanescente após o tratamento do risco.

Monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.

Reporte de Riscos: forma de comunicação destinada a informar partes interessadas específicas, internas ou externas, fornecendo informações relativas ao estado atual do risco e à sua gestão.

Auditoria de Gestão de Riscos: processo sistemático, independente e documentado para obter evidências e avaliá-las de maneira objetiva, a fim de determinar a extensão na qual a estrutura da gestão de riscos, ou qualquer parte sua selecionada, é adequada e eficaz.

3. SISTEMA E ESTRUTURA DA GESTÃO DE RISCOS DA CGE/PA

O Sistema de Gestão de Riscos (SGR) compreende um conjunto de instrumentos

que dão suporte à implementação, ao monitoramento e à melhoria contínua da gestão de riscos na CGE/PA, composto pela Política de Gestão de Riscos, pela estrutura responsável por seu estabelecimento e organização e pelo processo de gerenciamento de riscos, que engloba estabelecimento do contexto, identificação, análise, avaliação, tratamento, monitoramento e comunicação contínua dos riscos identificados de todo o processo e do fluxo de tomada de decisões na estrutura de governança, conforme orientação da norma ABNT NBR ISO 31000:2018 – Princípios e Diretrizes da Gestão de Riscos.

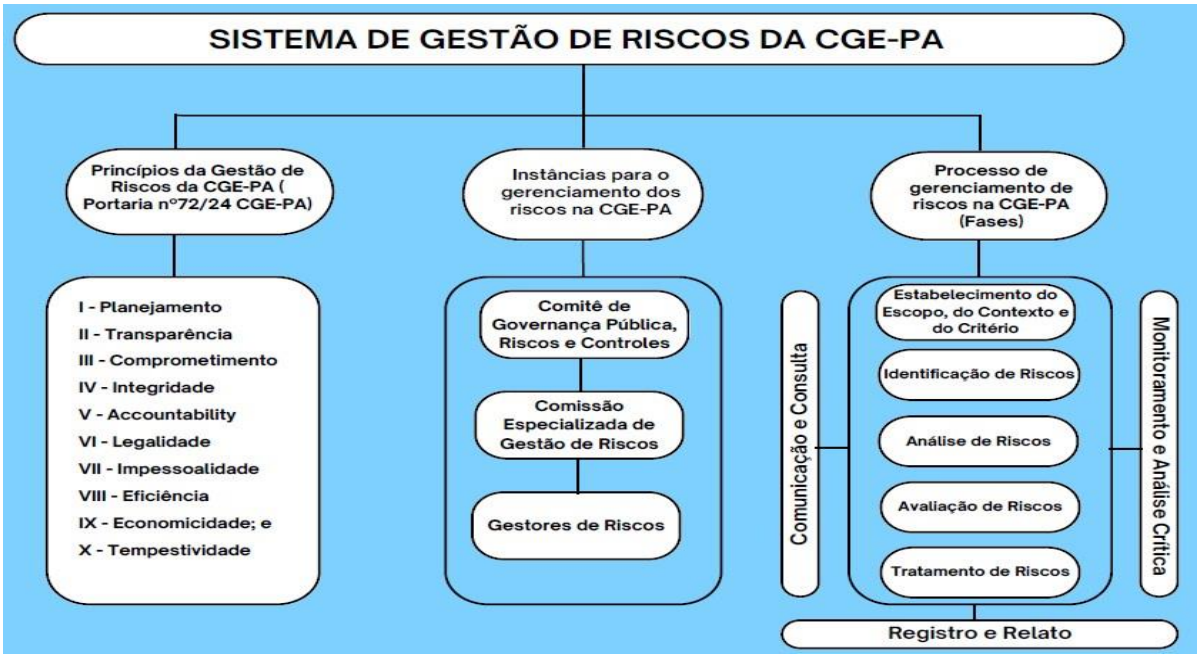
O SGR tem como objetivos o planejamento, a execução, o monitoramento e a melhoria contínua da gestão de riscos no âmbito da **Controladoria-Geral do Estado**.

Para efeito deste Manual, entende-se como objeto de risco o conjunto de atividades realizadas no âmbito do órgão, em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos.

Nesse sentido, a estrutura instituída na CGE/PA é constituída por 3 instâncias e estão detalhadas na Política de Gestão de Riscos do órgão, sendo formada por:

- **1ª instância** = Gestores de Riscos - As chefias e respectivos âmbitos e escopos de atuação;
- **2ª instância** = Comissão Especializada de Gestão de Riscos - servidores designados por meio de portaria;
- **3ª instância** = Comitê de Governança Pública, Riscos e Controles - composto pelos responsáveis setoriais do órgão, determinado por meio de portaria.

Figura 1- Visão geral do Sistema de GR da CGE PA.



Fonte: C-AUDIN, 2024.

4. MODELO DAS TRÊS LINHAS

O Modelo das Três Linhas, conforme disciplinado pelo IIA (Instituto dos Auditores Internos), é o utilizado na estruturação do Sistema de Gestão de Riscos do órgão, o qual tem como objetivos basilares a não existência de lacunas na abordagem de riscos e controle, nem a duplicação de esforços desnecessários. Nesse sentido, suas premissas intenção visam a definição clara de atribuições para que cada grupo entenda seu papel, os aspectos pelos quais eles são responsáveis e como eles irão coordenar seus esforços uns com os outros.

Entretanto, é importante mencionar que as “linhas” não denotam elementos estruturais, mas sim uma diferenciação útil de papéis que operam simultaneamente, inclusive o órgão de governança. Abaixo, a estrutura do Modelo das Três Linhas, recomendado pelo IIA.

Figura 2- Modelo de 3 Linhas do IIA.

Fonte: IIA Brasil.

4.1 Funcionamento das Três Linhas Modelo na CGE

A responsabilidade da gestão de atingir os objetivos organizacionais compreende os papéis da 1ª e 2ª linhas. Os papéis de 1ª linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio. Os papéis de 2ª linha fornecem assistência e monitoramento no gerenciamento de riscos.

Ademais, os papéis de 1ª e 2ª linha podem ser combinados ou separados.

Alguns papéis de 2ª linha podem ser atribuídos a especialistas, para fornecer conhecimentos complementares, apoio, monitoramento e questionamento àqueles com papéis de 1ª linha. Os papéis de 2ª linha podem se concentrar em objetivos específicos do gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade. Como alternativa, os papéis de 2ª linha podem abranger uma responsabilidade mais ampla pelo gerenciamento de riscos, como o gerenciamento de riscos corporativos. Entretanto, a responsabilidade pelo gerenciamento de riscos segue fazendo parte dos papéis de 1ª linha e dentro do escopo da gestão.

Quanto ao papel da 3ª linha, a auditoria interna presta avaliação e assessorias independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Isso é feito por meio da aplicação competente de processos sistemáticos e disciplinados, expertise e conhecimentos. Ela reporta suas descobertas à gestão para promover e facilitar a melhoria contínua. Ao fazê-lo, pode considerar a avaliação de outros prestadores internos e externos. É importante destacar que as atribuições das instâncias envolvidas no SGR da CGE/PA constam na sua Política de Gestão de Riscos. Abaixo, uma adaptação do modelo adotado por esta Instituição.

Figura 3- Modelo de 3 Linhas do IIA adaptado à CGE PA.

Fonte: Adaptação, C-AUDIN, 2024.

5. ETAPAS DA GESTÃO DE RISCOS

O processo de gestão de riscos no âmbito da CGE/PA deve ser dirigido pelo Gestor de Riscos e contar com a participação de servidores e colaboradores representantes das unidades do órgão que sejam conhecedores do todo ou em parte do processo ou projeto sob análise.

O processo de gestão de riscos é contínuo e cíclico, devendo ser realizado de acordo com as seguintes etapas: estabelecimento do escopo, contexto e critério; identificação dos riscos; análise de dos riscos; avaliação (resposta aos riscos); tratamento dos riscos; comunicação e consulta com as partes interessadas; e monitoramento ao longo de todo o processo, conforme ilustrado no gráfico anteriormente (Figura 1).

É importante destacar que durante as etapas do processo de gestão de riscos deve haver comunicação informativa e consultiva entre o Gestor de Riscos e as partes

interessadas, para: auxiliar o estabelecimento do contexto apropriadamente e assegurar que as visões e percepções das partes interessadas sejam identificadas, registradas e levadas em consideração; auxiliar e assegurar que os riscos sejam identificados e analisados adequadamente, reunindo pessoas conhecedoras dos processos e áreas de diferentes especializações; bem como garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avaliem e apoiem o tratamento dos riscos.

5.1 Definição do Escopo, Contexto e Critério

O objetivo do estabelecimento do escopo, contexto e critérios é particularizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado à realidade da organização. Escopo, contexto e critérios envolvem a definição do propósito do processo e a compreensão dos contextos externo e interno. Tal etapa é finalizada com a elaboração de um documento, o qual aborde tais temas, com o intuito de materializar o ponto de partida da organização.

Trata-se do momento inicial da gestão de riscos, o qual consiste no entendimento da organização, delimitação do escopo do trabalho, percepção dos ambientes os quais o órgão ou entidade estão inseridos, identificando os critérios a serem considerados, de modo a detectar fatores que tenham o poder de influenciar no alcance dos resultados planejados.

Basicamente, aqui há a definição da estratégia da gestão de riscos, a qual se materializa com a definição de elementos como:

- Unidade responsável pelo processo organizacional;
- Definição de parâmetros internos e externos;

- Metodologias e normas relacionados ao processo em análise;
- Ferramentas, relatórios, recursos e formulários a serem utilizados.

Uma das técnicas utilizadas para a realização da análise do ambiente é a matriz SWOT, cuja sigla provém do inglês e busca identificar forças, fraquezas, oportunidades e ameaças da instituição ou das unidades.

Ademais, cabe salientar que é nesta fase em que a instituição definirá o seu **Apetite a Riscos**, que consiste na quantidade de risco que a organização deseja assumir para conseguir atingir seus objetivos. Tal evento está diretamente relacionado à estratégia da organização e é levado em conta na ocasião de sua definição, haja vista que as estratégias expõem a organização a diferentes riscos.

Nesse sentido, é importante que o apetite a risco seja estabelecido no início do processo de gerenciamento de riscos, tendo em vista que é esse posicionamento da instituição que irá direcionar as atenções para determinados riscos, os que sejam considerados relevantes, em detrimento de outros, que não afetam de maneira significativa os objetivos estratégicos.

5.2 Identificação dos Riscos

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos (ABNT NBR ISO 31000:2018 – Princípios e Diretrizes da Gestão de Riscos).

A etapa de identificação de riscos pode ser caracterizada como o processo de levantamento, identificação e descrição dos riscos, tendo por base as informações obtidas durante as etapas anteriores, e contando com a comunicação e consulta contínua das equipes envolvidas e outras partes interessadas. O principal objetivo é

elaborar um registro abrangente de riscos, isto é, uma relação detalhada dos eventos que caso ocorram, podem influenciar na realização dos objetivos institucionais.

Tais riscos PODEM ser identificados a partir de perguntas, como:

- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?

Para facilitar a compreensão entre riscos, causa e consequência, a sintaxe a seguir poderá auxiliar no desenvolvimento da identificação de riscos: Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DO RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIAS>, impactando no/na < OBJETIVO DO PROCESSO ORGANIZACIONAL >.

Nesse sentido, para o desenvolvimento do levantamento de riscos, as equipes podem utilizar dados históricos, análises teóricas, opiniões de especialistas, assim como as seguintes técnicas de coleta de informação:

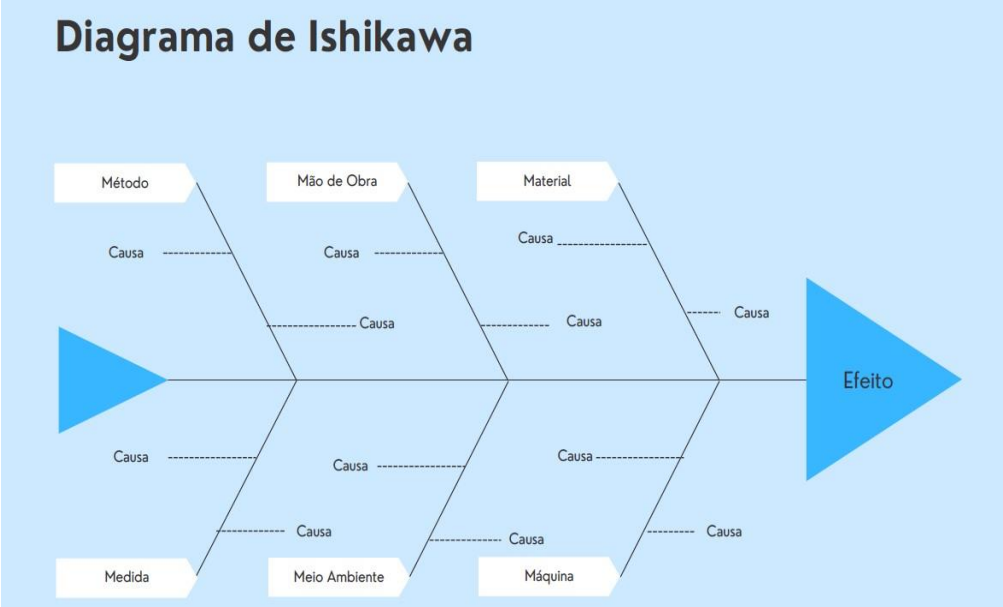
Análise SWOT *(strengths, weaknesses, opportunities and threats analysis)*: Com base na análise SWOT elaborada na fase do Estabelecimento de Contexto, os responsáveis devem identificar possíveis eventos, tanto internos quanto externos, que poderiam resultar em problemas financeiros, legais, operacionais, de imagem, entre outros, para a organização ou entidade.

Entrevistas: Tal técnica baseia-se na formulação prévia de um conjunto de

perguntas que são apresentadas nas entrevistas feitas com os agentes mais envolvidos nos processos e especialistas no assunto. Ela tem como finalidade garantir que todos os entrevistados abordem os mesmos assuntos na identificação de riscos e evitar a influência da opinião de outros participantes do grupo nas respostas.

Diagrama Causa e Efeito (espinha de peixe ou diagrama de ishikawa): Ferramenta gráfica, com o formato de espinha de peixe, que tem como finalidade ajudar as equipes a identificar as causas dos riscos e definir alguns potenciais impactos.

Figura 4 - Diagrama de Ishikawa

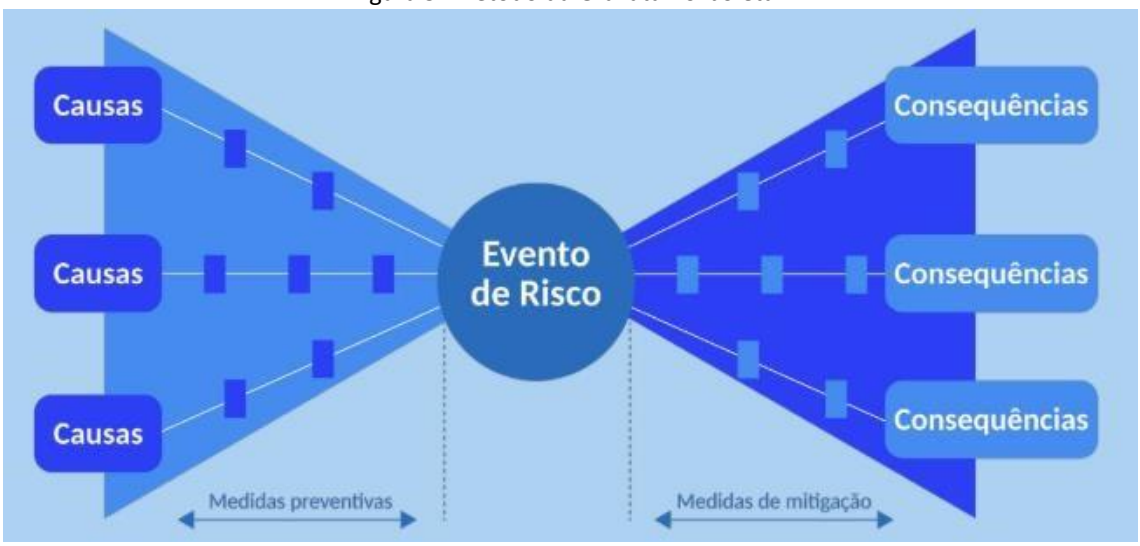


Fonte: Adaptação, C-AUDIN, 2024.

Método *bow-tie* ou gravata borboleta: Ferramenta que visa descrever, de maneira simples, os riscos, suas causas e as consequências do evento analisado. Tratase de uma análise para demonstrar que o risco possui uma série de possíveis

causas e consequências, conforme a figura abaixo.

Figura 5- Método da Gravata Borboleta



Fonte: Manual de Gestão de Riscos, TCE-CE.

Medidas Preventivas: Reduzem as chances de ocorrência do evento.
Medidas de Mitigação: Atenuam a severidade dos impactos derivados do evento.

5.3 Análise dos Riscos

Quanto à análise de riscos, trata-se do processo de compreender a natureza do risco e de determinar o nível de risco, mediante o produto entre a probabilidade de sua ocorrência e o impacto possível. Assim, analisar os riscos inclui multiplicar a **probabilidade** de ocorrência futura do evento e o **impacto** caso este se concretize.

A análise de riscos pode ser realizada com vários graus de detalhamento e complexidade, dependendo do propósito da análise, da disponibilidade e confiabilidade da informação, e dos recursos disponíveis. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos. (ABNT, 2018). A partir da combinação entre probabilidade e impacto em uma matriz, é possível estabelecer o nível de risco.

NÍVEL DE RISCO = PROBABILIDADE X IMPACTO

Para o cálculo do nível de risco serão utilizadas escalas numéricas previamente convencionadas para mensurar a probabilidade e o impacto.

Escala de Probabilidade (A probabilidade corresponde a chance que o risco tem de acontecer)

Quadro 1- Escala de probabilidade.

Probabilidade	Descrição da Probabilidade, sem os controles	Peso
Muito baixa	Rara. Evento extraordinário, ocorrendo em situação excepcional. Ou seja, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade (sem histórico de ocorrência).	1
Baixa	Pouco provável. Evento inesperado ou casual, com baixo histórico de ocorrência (baixa frequência).	2
Média	Possível. Evento esperado, com frequência razoável. O histórico de ocorrência é conhecido pela maioria dos gestores e operadores do processo.	3
Alta	Provável. Evento com elevada frequência, com histórico de ocorrência amplamente conhecido.	4
Muito alta	Praticamente certa. Evento constante e conhecido. As circunstâncias apontam evidências de novas ocorrências.	5

Fonte: C-AUDIN, 2024.

Escala de Impacto (O impacto corresponde ao efeito resultante da ocorrência do evento de risco sobre os objetivos analisados)

Quadro 2 - Escala de impacto.

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso

Muito baixo	Impacto nulo ou insignificante nos objetivos (estratégicos, operacionais, de informação/comunicação, de conformidade).	1
Baixo	Impacto mínimo nos objetivos.	2
Médio	Impacto mediano nos objetivos, porém recuperável em caso de consequências negativas.	3
Alto	Impacto significativo nos objetivos, de difícil recuperação em caso de consequências negativas.	4
Muito alto	Impacto máximo nos objetivos, sem possibilidade de recuperação em caso de consequências negativas.	5

Fonte: C-AUDIN, 2024.

Exemplo Prático

Ex.: A C-AUDIN tem como meta a execução de certo número de auditorias em um período de tempo. Foram identificados os seguintes eventos de risco que poderiam afetar o cumprimento dessa meta:

RISCO 1 – absenteísmo (falta de pontualidade e assiduidade) dos servidores acima do esperado;

RISCO 2 – perda da base de dados do sistema, sem possibilidade de recuperação.

Análise do RISCO 1: Absenteísmo

Impacto: alto = 4

Probabilidade: baixa = 2

Nível de risco: 4 x 2 = 8

Análise do RISCO 2: Perda da base de dados

Impacto: muito alto = 5

Probabilidade: muito baixa = 1

Nível de risco: 5 x 1 = 5

Para o gerenciamento dos riscos é importante estabelecer categorias para classificar os níveis de riscos resultantes da análise da probabilidade e do impacto. A CGE/PA estabeleceu a seguinte escala de classificação dos níveis de riscos:

Escala para classificação de níveis de risco

Risco baixo: 0 a 4	Risco médio: 5 a 10	Risco alto: 11 a 16	Risco extremo: 17 a 25

Os resultados das combinações de probabilidade e impacto, classificados de acordo com a escala de níveis de risco, podem ser expressos em uma matriz de nível de risco ou, comumente chamada, MATRIZ DE RISCO.

Quadro 3- Escala para classificação de níveis de risco

Impacto					
Muito alto	RM 5	RM 10	RA 15	RE 20	RE 25
Alto	RB 4	RM 8	RA 12	RA 16	RE 20
Médio	RB 3	RM 6	RM 9	RA 12	RA 15
Baixo	RB 2	RB 4	RM 6	RM 8	RM 10
Muito baixo	RB 1	RB 2	RB 3	RB 4	RM 5
	Muito Baixa	Baixa	Média	Alta	Muito Alta

Probabilidade

Fonte: C-AUDIN, 2024.

Retomando o exemplo dado acima dos riscos 1 (absenteísmo) e 2 (perda da base de dados), tem-se na matriz de risco o seguinte:

Quadro 4- Escala da classificação de níveis de risco (exemplos apresentados).

Impacto					
Muito alto	RM 5 **RISCO 2**	RM 10	RA 15	RE 20	RE 25
Alto	RB 4	RM 8 **RISCO 1**	RA 12	RA 16	RE 20
Médio	RB 3	RM 6	RM 9	RA 12	RA 15
Baixo	RB 2	RB 4	RM 6	RM 8	RM 10
Muito baixo	RB 1	RB 2	RB 3	RB 4	RM 5
	Muito Baixa	Baixa	Média	Alta	Muito Alta

Probabilidade

Fonte: C-AUDIN, 2024.

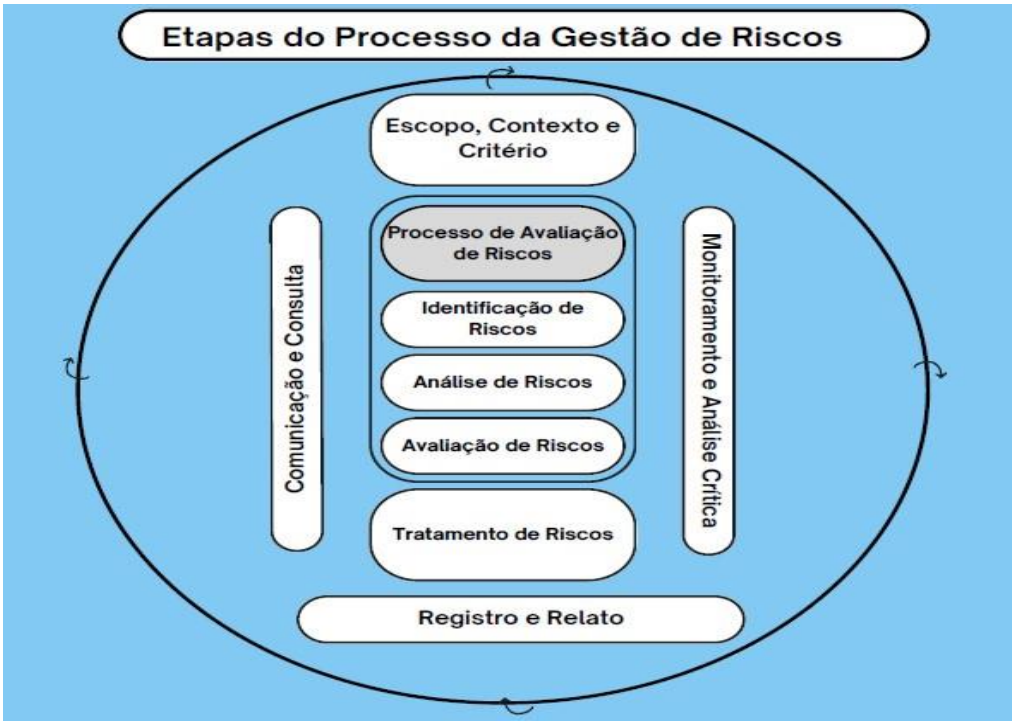
É importante mencionar a necessidade de um cuidado na análise da matriz, para não se ater apenas ao valor do nível de risco encontrado. No exemplo dado acima, o RISCO 1 possui um valor maior que o RISCO 2. Contudo, caso o risco 2 venha se concretizar, o seu impacto terá consequências com alto impacto (perda total da base de dados). O RISCO 2 é o risco – chave e deve ser gerenciado como um risco crítico.

Ademais, é fundamental a ciência de que a análise dos riscos envolve diversas variáveis, internas e externas à organização, e que tais fatores interagem com o todo o processo da gestão de riscos. Por isso, tal gerenciamento tem como atributo ser um processo contínuo pelas mudanças de cenário que a instituição pode enfrentar.

No âmbito das tomadas de decisões, o gestor deve considerar o nível de risco

que vai agregar valor ao órgão, para que os devidos esforços sejam direcionados, de forma mais assertiva e interessante para a instituição. **O Anexo 1 deste documento consta um modelo de planilha de gestão de riscos**.

Figura 6- Etapas do Processo da GR utilizadas na CGE PA.



Fonte: ISO 31000:2018

5.4 Avaliação dos Riscos

Tal etapa consiste na comparação dos resultados obtidos na etapa de análise com o apetite a risco, a fim de decidir quais riscos serão tratados. A avaliação de riscos auxilia na decisão sobre o tratamento de riscos. Nela há a seleção da resposta mais adequada dentro do contexto da CGE/PA. Nesse sentido, a matriz de riscos permitirá uma melhor visão dos riscos organizacionais e da eficácia dos controles a eles aplicados. A tomada de decisão para cada risco mapeado é feita com base na matriz de

risco, somada ao apetite a risco e as soluções disponíveis para o risco em análise.

Dessa forma, uma vez publicado o apetite a risco do órgão, entende-se que a instituição está disposta a assumir certos níveis de riscos. Cabe ao gestor do risco, juntamente com a equipe, analisar cada caso, considerando o apetite institucional declarado.

Todavia, deve-se ter em mente que os níveis de riscos assumidos no apetite e a tolerância utilizada em caso específico não podem prejudicar a organização no alcance de seus objetivos ou, ainda, trazer consequências negativas a um processo/projeto específico.

Assim, a avaliação dos riscos deve seguir da seguinte forma:

1. **EVENTOS DE RISCOS** cujos níveis estão **ACIMA** do APETITE AO RISCO – Identificar os riscos, listar as causas e consequências para cada um, e os controles já implementados, para que assim seja tomada uma resposta de tratamento;
2. **EVENTOS DE RISCOS** cujos níveis estão **ABAIXO** do APETITE AO RISCO – Deve-se avaliar a necessidade de tratamento e/ou monitoramento desses riscos, a depender da resposta ao risco tomada.

Como resposta de tratamento aos riscos, segue que:

Quadro 5- Respostas aos riscos.

RESPOSTAS AOS RISCOS	
RESPOSTAS	**PARÂMETROS**
Mitigar	Significa tomar medidas que venham diminuir o nível de risco avaliado. Alguns exemplos são: adotar novos controles, redesenhar processos, realocar pessoas, realizar capacitação, desenvolver ou aperfeiçoar soluções de TI e adequar estrutura organizacional.

Compartilhar	Um risco normalmente é compartilhado quando se torna vantajoso para a instituição. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Evitar o risco significa excluí-lo. Um risco normalmente é excluído quando a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou quando não há entidades dispostas a compartilhar o risco. A depender do caso, o processo de trabalho poderá ser interrompido. Antes da decisão de exclusão do risco, o gestor deve comunicar a Comissão Especializada de Gestão de Riscos.
Aceitar	Um risco normalmente é aceito quando seu nível está abaixo da faixa do apetite a risco declarado. Nessa situação, nenhuma medida será adotada. Porém, é importante que o risco aceito seja monitorado.

Fonte: C-AUDIN, 2024.

5.5 Tratamento dos Riscos

Nesta etapa, compreende-se que deve traçar um plano de ação para modificar o nível dos riscos identificados como prioritários para seu tratamento. Um risco pode precisar de um ou vários controles a fim de reduzir sua probabilidade e/ou seus **O tratamento dos riscos deve seguir os seguintes passos:**

Passo 1 – Listar cada ação adotada como medida de tratamento. Ressalta-se que para um mesmo evento de risco, pode existir inúmeras ações;

Passo 2 – Determinar o responsável para cada ação;

Passo 3 – Traçar uma data de início e de término para a ação, de acordo com os atores envolvidos, bem como o status de conclusão da ação (em percentual);

Passo 4 – Identificar quem deve ser comunicado quanto a ação em tratamento e a frequência dessa comunicação.

O plano de tratamento deve seguir a base do ciclo PDCA, no qual é feito o planejamento, a execução do planejado, o monitoramento e atuação para ajustar aquilo não alcançado, conforme planejamento.

O processo de tratamento de riscos, como reforça a norma ABNT NBR ISO 31000:2018 – Princípios e Diretrizes da Gestão de Riscos, é iterativo, envolvendo não só a descrição de um plano de ação, mas também a avaliação da eficácia do tratamento, de forma a verificar a aceitabilidade do risco residual e a necessidade (ou não) de definição e implementação de tratamento adicional para as situações em que o risco remanescente extrapole o apetite e a tolerância a riscos.

No caso de o processo organizacional passar por vários setores do órgão, o plano de tratamento de riscos será definido em conjunto com um representante de cada unidade.

5.6 Comunicação e Consulta

A comunicação e a consulta têm como escopo possibilitar a troca de informações buscando garantir a integração, a colaboração e o alinhamento entre todas as instâncias e as partes interessadas, levando-se em consideração os aspectos da confidencialidade, integridade, confiabilidade e tempestividade.

Ressalta-se que não são etapas isoladas, sendo importante que aconteçam de forma contínua durante todas as fases do gerenciamento de riscos, visando auxiliar as partes interessadas na compreensão do risco, para as tomadas de decisão e definição das ações necessárias.

5.7 Monitoramento e Análise Crítica

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.

O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Convém que o monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas.

Assim, essa etapa consiste em:

- Verificar a ocorrência de mudanças nos contextos externo e interno do órgão, que podem vir a modificar os critérios identificados para os riscos ou o próprio risco, podendo exigir uma revisão no tratamento dos riscos e respectivas prioridades;
- Registrar as lições aprendidas com o tratamento dos riscos, para aperfeiçoamentos futuros;
- Identificar o surgimento de possíveis riscos, que podem emergir após o processo de análise crítica, sendo uma entrada para um novo ciclo de processo de gestão de riscos.

Como os riscos aos processos organizacionais são dinâmicos e o processo de gestão de riscos deve ser continuamente melhorado, a metodologia de gestão de riscos não se encerra com a implementação do respectivo plano de tratamento. É importante que os eventos de risco sejam monitorados, pois os contextos externo e interno de uma instituição podem mudar e riscos podem emergir, mudar ou até desaparecer. O monitoramento pode, ainda, revelar que os controles adotados no respectivo plano de

ação não são suficientemente eficazes.

Na metodologia de gestão de riscos da CGE/PA, o Gestor de Riscos será responsável pelo monitoramento contínuo (ou, ao menos, frequente) dos riscos sobre sua responsabilidade, atualizando as informações pertinentes e comunicando os participantes envolvidos.

5.8 Registro e Relato

Diante da necessidade da documentação e relato do processo de gestão de riscos e seus resultados, por meio de mecanismos apropriados, o Registro e o Relato visam: comunicar atividades e resultados de gestão de riscos em toda a organização; fornecer informações para a tomada de decisão; melhorar as atividades de gestão de riscos; auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

Convém que as decisões relativas à criação, retenção e manuseio de informação documentada levem em consideração, mas não se limitem a, o seu uso, a sensibilidade da informação e os contextos externo e interno.

O relato é parte integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a Alta Direção e os órgãos de supervisão a cumprirem suas responsabilidades. Os fatores a considerar para o relato incluem, mas não estão limitados a: diferentes partes interessadas e suas necessidades específicas de informação e requisitos; custo, frequência e pontualidade do relato; método de relato; pertinência da informação para os objetivos organizacionais e para a tomada de decisão.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ABNT. NBR ISO 31000: Gestão de Riscos: Diretrizes. Rio de Janeiro, 2018. Disponível em: https://dintegcgcin.saude.gov.br/attachments/download/23/2018%20-%20Diretrizes%20-%20Gest%C3%A3o%20de%20Riscos_ABNT%20NBR%20ISO%2031000.pdf. Acesso em: 15 jul.2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR ISO 31073: Gestão de Riscos: Vocabulário. Rio de Janeiro, 2022.

BRASIL. Portaria nº 910/ 2018-CGU - Aprova a Metodologia de Gestão de Riscos da Controladoria Geral da União. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/34537/8/Boletim_Interno_Extra_04_de_abril_2018.pdf. Acesso em: 15 jul. 2024.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL (IIA Brasil). Modelo das 3 linhas do IIA 2020, IIA Brasil. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-theditorHTML-00000013-20082020141130.pdf . Acesso em: 04 jun.2024.

Manual de Gestão de Riscos da Controladoria Geral do Município de São Paulo, 2023. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/Manual_Gestao_Riscos_versao01_2023_publicacao_03_01_2024.pdf. Acesso em: 04 jun.2024.

Manual de Gestão de Riscos do Tribunal de Contas do Estado do Ceará, 2022. Disponível em: https://www.tce.ce.gov.br/downloads/manual_gestao_riscos_2022.pdf. Acesso em: 04 jun.2024.

Manual de Gestão de Riscos do Tribunal de Justiça Estado do Pará, 2024. Disponível em: https://www.tjpa.jus.br/CMSPortal/VisualizarArquivo?idArquivo=1523629. Acesso em: 04 jun.2024.

PARÁ. Portaria nº 72/2024-CGE PA, de 10 de maio de 2024. Institui a Política de Gestão

de Riscos na Controladoria Geral do Estado do Pará. DOE Nº 35.814. Disponível em: https://www.ioepa.com.br/pages/2024/2024.05.10.DOE.pdf.
Acesso em: 15 jul. 2024.

ANEXO - **MODELO DE PLANILHA DE APOIO AO PROCESSO DE GERENCIAMENTO DOS RISCOS**

Identificação e Análise dos Riscos						
Objetivo Estratégico (1)	**Processo/Etapa (2)**	**Objetivo (3)**	**Evento do Risco (4)**	**Categoria (5)**	**Causa (6)**	**Consequência (7)**
		Avaliação dos Riscos				
Controles						
Preventivo (8)	**Mitigatórios (9)**	**Probabilidade (10)**	**Impacto (11)**	**Risco Inerente (12)**	**Avaliação e Controle (13)**	**Risco Residual (14)**

Priorização dos Riscos			Respostas aos Riscos			
Calssificação (15)	**Priorizado (16)**	**Justificativa (17)**	**Tipos de Tratamento (18)**	**Medidas de Tratamento (19)**	**Iniciativa (20)**	**Evento de Risco/Medida de Tratamento (21)**

Unidade Responsável	Responsável pela implmentação	Como será implementado?	Custo Previsto	Avaliação e Controle	Data Prevista para o início da implementação	Data prevista para o término da implementação

Situação