POLÍTICA DE GERENCIAMENTO DE RISCOS - PGR

PREFEITURA RIO | Controladoria Geral do Município

Sumário

ÍNDICE DE FIGURAS E QUADROS

Controladoria Geral do Município ● Subcontroladoria de Auditoria e Controle ● Coordenadoria Técnica de Controles Internos
Rua Afonso Cavalcanti 455, 14º andar – sala 1445 ●controlesenormas.cgm@prefeitura.rio● Tel.: 2976-3277
Anexo único à Resolução CGM-RIO nº 1.794/2022

V.3 - FECHAMENTO DESTA EDIÇÃO: 06/11/2025

Fotografia: Michelle Guimarães
Disponível em https://www.pexels.com/pt-br/foto/cidade-perto-de-corpo-d-agua-sob-ceu-nublado-3648269/
(LICENÇA: ✓ Disponível para uso gratuito. ✓ Não é necessário citar os créditos.)

ACESSE O CÓDIGO DE INTEGRIDADE DO AGENTE PÚBLICO MUNICIPAL

Glossário

Apetite ao risco: nível de exposição ao risco que o órgão está disposto a aceitar, a partir de análise do ambiente, do custo de oportunidade e do custo/benefício de tratamento de riscos de menor impacto projetado;

Causa: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo. São considerados os "porquês" da ocorrência do evento. A ação a ser desenvolvida pela equipe no tratamento do risco deve, necessariamente, combater/mitigar, uma ou mais causas. Em geral, somente com a exclusão das causas ou a descontinuidade do processo geram a extinção do risco;

Consequência: possíveis efeitos resultantes da ocorrência de um evento sobre os objetivos do processo de trabalho ou da organização. A necessidade de tratamento das consequências dará azo aos planos de contingenciamento/estancamento dos efeitos do evento;

Controles Internos: conjunto de regras, procedimentos, diretrizes, entre outros, operacionalizados de forma integrada pela direção e pelos servidores do órgão, destinados a enfrentar as causas dos riscos, de modo a fornecer segurança razoável de que a ocorrência de determinado evento terá menor impacto na consecução da missão da entidade, quando comparado a risco não tratado (controlado);

Dimensões do risco: classificação dos tipos de riscos que podem afetar o alcance dos objetivos estratégicos da CGM-Rio, observadas as características de sua área de atuação e as particularidades do setor público.

Fraude: ato ilegal caracterizado por desonestidade, dissimulação ou quebra de confiança, com o propósito de obter vantagem indevida, manipular informações ou omitir fatos relevantes. Pode ocorrer sem uso de ameaça ou violência ou de força física;

Gerenciamento de riscos: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar, positiva ou negativamente, os objetivos, processos de trabalho e projetos da CGM-Rio, nos níveis estratégico, tático e operacional;

Gestão de riscos: o conjunto de ações direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da CGM-Rio;

Impacto: o grau ou importância dos efeitos da ocorrência de um risco, estabelecido a partir de uma escala predefinida de consequências possíveis;

Incerteza: é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade;

Mapa de riscos: registro formal através do qual o gestor insere os riscos identificados, assim como as ações mínimas referentes ao gerenciamento;

Nível de risco: o nível de criticidade do risco, assim compreendido o quanto um risco pode afetar os objetivos, processos de trabalho e projetos da CGM-Rio, a partir de escala predefinida de criticidades possíveis;

Probabilidade: é a chance de o risco acontecer, estabelecida a partir de uma escala predefinida de probabilidades possíveis;

Processos de trabalho: conjunto de atividades inter-relacionadas ou interativas que representam os métodos de execução de um trabalho necessário para alcançar um objetivo;

Processos-chave: são os processos relevantes para a CGM-Rio relacionados à sua atividade-fim e/ou aos objetivos estratégicos definidos no Planejamento Estratégico - PE;

Resiliência organizacional: capacidade da CGM-Rio de antecipar, resistir e se recuperar de eventos adversos sem comprometer suas funções essenciais, mantendo a continuidade dos serviços;

Risco inerente: é o nível de risco ao qual uma organização está exposta antes de considerar qualquer controle preexistente;

Risco residual:é o nível de risco ao qual uma organização está exposta depois de considerar os controles preexistentes que possam reduzir sua frequência ou o seu impacto; e

Risco: a possibilidade de que um evento ocorra e afete, positivamente (risco positivo) ou negativamente (risco negativo), os objetivos estratégicos do órgão, por meio dos seus processos de trabalho ou projetos desenvolvidos;

Introdução à Política de Gestão de Riscos

A Política de Gerenciamento de Riscos – PGR da CGM-Rio chega a sua segunda revisão com o intuito de aprimorar a metodologia com a adição de mais um enfoque, o da gestão de riscos de integridade, fraude e corrupção, com base da ISO 37001. Assim, passam a embasar a política a ISO 31000 (Gestão de Riscos), ISO 37001 (Sistema de Gestão Antissuborno), a ISO 22301 (Continuidade de Negócios) e o COSO ERM 2017 (Gerenciamento de Riscos Corporativos), além das boas práticas consolidadas de gestão pública, integridade e governança.

A Política de Gestão de Riscos – PGR tem como finalidade identificar, corrigir e tratar os riscos existentes nos processos de trabalho estratégicos adotados no âmbito do órgão, agindo para a diminuição dos impactos que possam afetar, direta ou indiretamente, o alcance dos objetivos traçados no seu planejamento estratégico.

Sendo assim, a CGM-Rio resolveu adotar um modelo de gestão moderno, prático e desburocratizado, visando o aumento da efetividade das suas atividades. Isso tudo vem do entendimento de que a Administração Municipal precisa sempre estar atenta à melhoria da gestão dos seus recursos, os quais são escassos e merecem um gerenciamento mais profissionalizado, voltado para a continuidade dos serviços prestados ao principal cliente desta municipalidade, o cidadão carioca.

A Política de Gestão de Riscos da CGM-Rio apresenta um conjunto de princípios, objetivos, diretrizes, processos e informações, internas e externas, que formam as linhas gerais do gerenciamento de riscos, tendo como referência normas internacionais que tratam do tema, como o COSO ERM e a ISO 31.000:2009, bem como políticas de riscos já consolidadas no país, como as metodologias implantadas na CGU, no TCU e o manual do programa de gestão de riscos da SEFAZ/BA, todos esses de cunho pedagógico e orientador de grande valia para a elaboração do presente manual.

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

Princípios

A Política de Gestão de Riscos da CGM-Rio encontra suporte em **onze princípios** ou postulados que orientam a sua implantação e o seu desenvolvimento dentro do órgão.

São eles:

I. **AGREGARVALOR** e proteger o ambiente institucional;
II. **APOIAR A MELHORIA** contínua;
III. **CONSIDERAR FATORES** humanos e culturais;
IV. **ORIENTAR-SE PELO CUSTO BENEFÍCIO**, devendo sempre ser analisado o possível impacto do risco em relação ao custo de implantação das ações para tratamento.
V. **SER PARTE INTEGRANTE** dos processos organizacionais;
VI. **SER SISTEMÁTICA**, estruturada e oportuna;
VII. **SER SOB MEDIDA**, alinhada com o contexto interno e externo e com o perfil do risco;
VIII. **SER TRANSPARENTE** e conclusiva;
IX. **SER DINÂMICA**, interativa e capaz de reagir a mudanças;
X. **SUBSIDIAR** a tomada de decisões; e
XI. **ATUAR COM INTEGRIDADE E INCORRUPTIBILIDADE,** rejeitando e prevenindo quaisquer formas de fraude e corrupção.

Objetivos

Além dos princípios, a Política de Gestão de Riscos está alicerçada em **objetivos** claros, os quais correlacionam-se diretamente com a **IMPLANTAÇÃO, O DESENVOLVIMENTO E A DISSEMINAÇÃO** de metodologia de identificação e tratamento de riscos dos processos da CGM-Rio. São eles:

- Mitigar os efeitos dos eventos de riscos que impactam no alcance da missão e dos objetivos traçados no Planejamento Estratégico;
- Estimular uma gestão proativa que antecipe e previna ocorrências capazes de afetar seu desempenho;
- Melhorar a governança, o controle interno da gestão e a qualidade do gasto público;
- Prezar pelas conformidades legal e normativa dos processos organizacionais;
- Otimizar procedimentos em que haja a possibilidade de auferir novas receitas;
- Melhor gerir os riscos atrelados às compras e às contratações realizadas; e
- Prevenir, detectar e combater fraudes e corrupção.

Gestores de Riscos

Para que se coloque em prática todas as diretrizes previstas no manual, é de fundamental importância que se defina os **RESPONSÁVEIS** por cada tarefa prevista na metodologia. Dentre esses responsáveis estão os gestores dos riscos.

São considerados gestores dos riscos aqueles responsáveis por processos de trabalho, projetos e iniciativas estratégicas, táticas e operacionais da CGM-Rio, em seus respectivos âmbitos e escopos de atuação, sendo esses os verdadeiros responsáveis pelo desenvolvimento da política no âmbito organizacional:

O Controlador-Geral e os Subcontroladores, embora não sejam gestores dos riscos, tendo em vista que não são diretamente responsáveis pelas tarefas dos setores, são responsáveis, em última instância, pelo processo decisório que envolve a Gestão de Riscos, sendo fundamental o seu apoio para engajamento de todos no processo.

Figura 1 - Gestores de Riscos

Competências e responsabilidades

Uma vez definidos quem são os gestores dos riscos, é preciso delimitar as competências, não só destes, como de todos aqueles agentes públicos que atuarão no tratamento dos riscos identificados. Vejamos:

Comissão de Controle Interno - CONINT

- Estabelecer contexto e fixar os objetivos estratégicos.
- Definir cronograma de implantação da Política de Gestão de Riscos.
- Definir e revisar o apetite a risco alinhado ao planejamento estratégico.
- Revisar e validar grau de maturidade atribuído ao órgão.
- Analisar os riscos identificados e os controles adicionais a serem implementados.
- Validar as ações implementadas.
- Validar os indicadores propostos.

Núcleo de Apoio a Gestão de Riscos –CG/SUBAC/CCN

- Levantar e mapear os processos-chave associados aos objetivos fixados no Planejamento Estratégico.
- Orientar e capacitar os setores quanto à identificação, avaliação e tratamento dos riscos.
- Desenvolver ferramenta de gerenciamento de Riscos.
- Propor ações e apurar o grau de maturidade do órgão.
- Monitorar o desempenho do plano de gerenciamento de riscos.
- Propor indicadores de gerenciamento de riscos.

Gestores de Riscos

- Gerenciar os riscos atrelados aos seus processos de trabalho, conforme apetite a risco definido.
- Prover informações e auxiliar no mapeamento dos processos.
- Avaliar a gradação dos riscos identificados.
- Definir respostas aos riscos.
- Definir controles para tratar os riscos.
- Comunicar as ações realizadas.
- Designar servidor responsável pelo processo.

Servidor responsável pelo processo

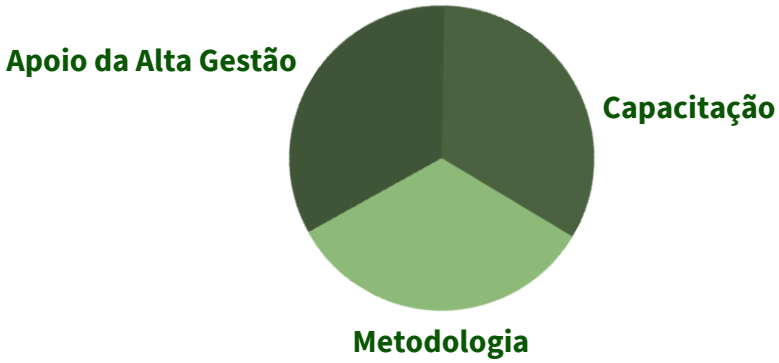
- Identificar os riscos dos processos a serem gerenciados.
- Implementar os controles internos propostos e comunicar ao gestor.
- Identificar e reportar tempestivamente eventos de risco emergente com potencial de impactar significativamente os processos.

Estratégia de implantação da Política de Gestão de Riscos

A Política de Gestão de Riscos – PGR da CGM-Rio consiste em um conjunto de procedimentos que visa estruturar mecanismos para mitigação dos efeitos dos eventos de riscos que impactam no alcance da missão do órgão.

A implantação da Política de Gestão de Riscos – PGR pressupõe a união de três medidas fundamentais:

Figura 2 - Pressupostos da Política de Gestão de Riscos



Apoio da Alta Gestão

Considerado medida fundamental para o sucesso da metodologia, o apoio da alta gestão serve de base para que todos os servidores tenham ciência da importância do processo e de que, com o respaldo do CONINT, serão ofertados todos os meios possíveis para o sucesso da proposta.

O chamado "*toneatthe top/ tonefromthe top*" é o comprometimento demonstrado pela alta gestão do órgão para que haja aderência à política em toda a CGM. Ou seja, o exemplo tem que vir de cima.

Pode-se dizer assim que a cultura do gerenciamento de riscos nasce junto daqueles que detêm o poder e a capacidade de direcionar o órgão no alcance dos seus objetivos, da sua missão institucional. Se a alta gestão da CGM não estiver voltada para a propagação da cultura da gestão de riscos, as equipes jamais serão "tomadas" por esse propósito.

O risco faz parte do "negócio" e todos aqueles que ocupam cargos de alta direção devem saber que não existe atividade que não incorra em riscos durante a sua execução, e com um órgão de controle do porte da CGM, em um município da magnitude do Rio de Janeiro não seria diferente. Deste modo, cada um desses tem

como dever transmitir aos seus colaboradores a importância de se tratar os riscos inerentes ao controle interno, discutindo a temática dos riscos organizacionais.

Em essência, cabe a esses gestores a identificação da melhor maneira de sensibilizar as suas equipes para que a implementação da metodologia continue sendo um sucesso.

Para isso, são recomendáveis comunicações diretas, a demonstração dos resultados após as análises junto à CG/SUBAC/CCN, e a solicitação constante de treinamento, mostrando os benefícios que o gerenciamento de riscos tem gerado, bem como os prejuízos que podem surgir se a CGM ou o setor não possuir um programa efetivo de gestão desses eventos.

Além disso, o Controlador Geral tem papel fundamental na disseminação da política, elaborando declarações para os servidores acerca da importância do gerenciamento de riscos, solicitando a inserção de trilha de conhecimentos voltada para Gestão de Riscos no Programa de Desenvolvimento de Pessoas - PDP (Portaria CGM nº 07/23) e ainda promovendo eventos de apresentação dos resultados alcançados ao final de cada exercício.

Com essas atitudes pode-se dizer que a CGM estará no caminho para obter o pleno apoio da alta gestão ao desenvolvimento da metodologia.

Capacitação em Gestão de Riscos

A capacitação é requisito essencial para que todos os agentes públicos do órgão desenvolvam gradualmente os conhecimentos, competências e habilidades necessários aos temas de gestão de riscos e mapeamento de processos.

Sendo assim, compete à CG/SUBAC/CCN promover aos servidores da CGM-Rio, a capacitação necessária sobre Gestão de Riscos e sobre Mapeamento de Processos, com o objetivo de dotar os integrantes das áreas dos conhecimentos metodológicos necessários para a implementação da metodologia proposta.

A estratégia de capacitação dos gestores e servidores poderá incluir reuniões, cursos, workshops e intercâmbios com órgãos/entidades que já possuam expertise na gestão de riscos, de modo a estimular a troca de experiências na implantação da metodologia aqui tratada.

Metodologia de Gerenciamento de Riscos

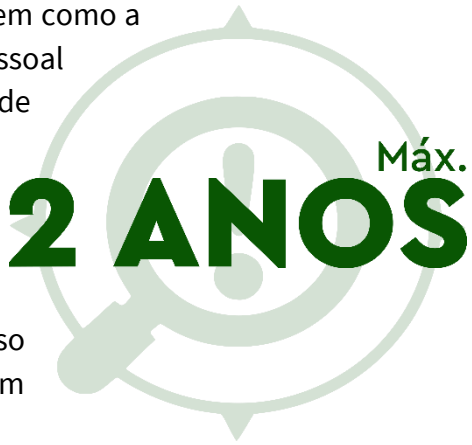
A metodologia apresentada é estabelecida e estruturada em seis etapas, as quais são necessárias para o gerenciamento dos riscos em todas as suas fases desde o seu planejamento até a entrega dos produtos, visando garantir que os riscos que possam impactar no alcance dos objetivos estratégicos sejam identificados, avaliados e tratados.

Adotar uma metodologia de gestão de riscos traz inúmeros benefícios às instituições, dentre os quais se destacam: a possibilidade de mitigar possíveis impactos provenientes de atos de corrupção e desvios éticos; fomentar o cumprimento de leis e regulamentos; evitar danos à imagem; aumentar a confiança e a credibilidade da gestão, e; contribuir para assegurar uma comunicação eficaz.

Além disso, a fim de dar maior eficiência e impacto à metodologia, o início da implantação deve se dar por meio do gerenciamento dos riscos dos processos-chaves selecionados a partir de atividades operacionais estratégicas para a CGM-Rio, podendo, de acordo com a evolução da maturidade do órgão e sua capacidade de monitoramento, expandir-se o escopo aos demais processos/projetos desenvolvidos, sem que haja perda de qualidade e efetividade.

Diretrizes para gerenciamento de riscos

O gerenciamento de riscos deve ser feito em ciclos **não superiores a dois anos,** ou ainda, **a cada revisão do planejamento estratégico**, o que ocorrer antes, abrangendo: os projetos de melhoria e ampliação previstos; os processos de trabalho desenvolvidos; os sistemas informatizados geridos; bem como a gestão orçamentária, patrimonial, financeira e de pessoal do órgão, com vistas a reduzir a possibilidade de ocorrência de riscos negativos, assim como, quando for o caso, potencializar os riscos positivos (oportunidades).



O limite temporal a ser considerado para o ciclo de gerenciamento de riscos de cada processo poderá ser decidido pelo respectivo gestor, levando em conta o limite máximo estipulado de 2 anos.

Sendo assim, pode-se dizer que o cerne da gestão de riscos será mapear, identificar e tratar vulnerabilidades de curto, médio e longo prazo que impactam à consecução dos objetivos estratégicos da CGM-Rio.

Embora seja fundamental dar início à implantação da política de gestão de riscos, ela não será efetiva caso não haja no âmbito do órgão uma diretriz de revisão e de retroalimentação do processo, uma vez que o fator tempo costuma ser imperativo na definição das formas de tratamento dos riscos. Dessa forma, realizar a análise periódica de todos os fatores apresentados deixa o órgão demasiadamente mais seguro, de modo a salvaguardar os seus ativos e objetivos estratégicos inerentes a projetos e processos de trabalho frente a novos riscos que possam ter sido identificados com o passar do tempo.

Etapas do Gerenciamento de Riscos

Na figura 3 estão descritas as etapas da metodologia que definem o ciclo a ser percorrido para o gerenciamento de riscos no órgão:

Figura 3 - Etapas do Gerenciamento de Riscos

As etapas acima apresentam particularidades que deverão ser criteriosamente analisadas, cabendo ao gestor dar a cada uma delas a importância necessária, de acordo com o momento do ciclo e a maturidade do órgão no tratamento dos riscos aos quais está exposto.

ANÁLISE DO CONTEXTO

Etapa 1 - Estabelecimento do contexto e fixação dos objetivos

Essa etapa envolve uma avaliação global do contexto no qual o órgão está inserido partindo da identificação dos fatores correlatos ao ambiente interno e externo.

A análise de contexto torna-se fundamental para a definição dos riscos a serem tratados com maior ou menor urgência de acordo com o grau de ameaça ou oportunidade que demonstre à continuidade do órgão.

O contexto demonstra ainda qual a posição estratégica do órgão frente ao município, aos seus pares e aos seus colaboradores, fornecendo, por meio da identificação do ambiente, indícios acerca do futuro e da continuidade de seus serviços a ser esperado pelos seus principais usuários.

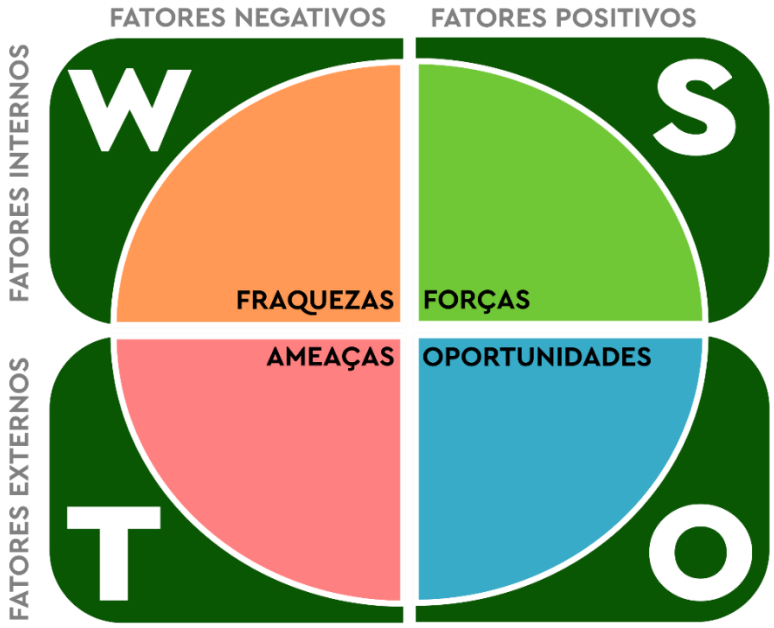
A definição do ambiente interno e externo pode ser realizada utilizando-se a ferramenta de análise de cenários conhecida como matriz “SWOT” ou “FOFA” e deve considerar, dentre outros, os seguintes critérios:

CONTEXTO EXTERNO	a) ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico e econômico, nacional, regional ou local; b) fatores-chave e tendências que tenham impacto sobre os objetivos da CGM-Rio; e c) relações com partes interessadas externas e suas percepções e valores;

a) governança, estrutura organizacional, funções e responsabilidades; b) políticas, objetivos e estratégias implementadas para atingi-los; c) capacidades, entendidas em termos de recursos e conhecimento; d) sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais); e) relações com partes interessadas internas e suas percepções e valores; f) cultura do Órgão; g) normas, diretrizes e modelos adotados pelo órgão; e h) forma e extensão das relações contratuais.	**CONTEXTO INTERNO**

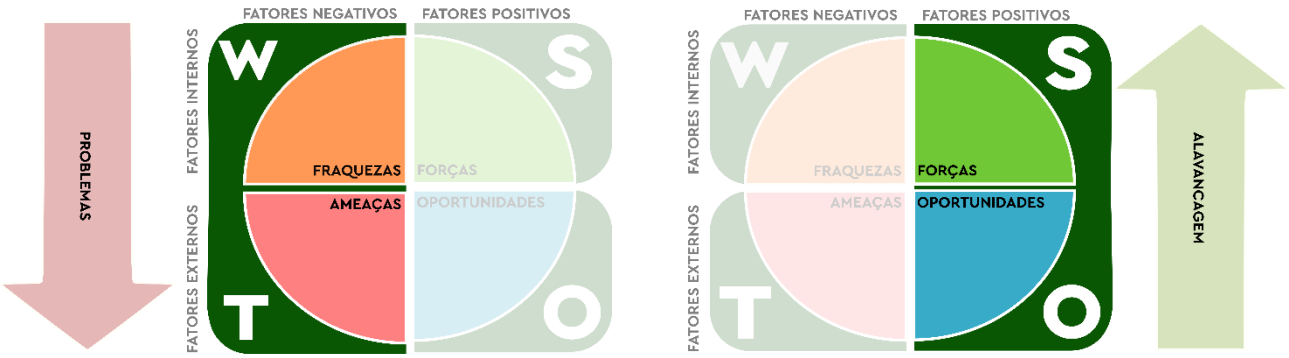
A matriz SWOT (FOFA) poderá ser utilizada para identificar, no ambiente interno, as forças e fraquezas da CGM-Rio, e, no ambiente externo, as ameaças e oportunidades do contexto ao qual está inserido, as quais sejam capazes de impactar positivamente ou negativamente a organização.

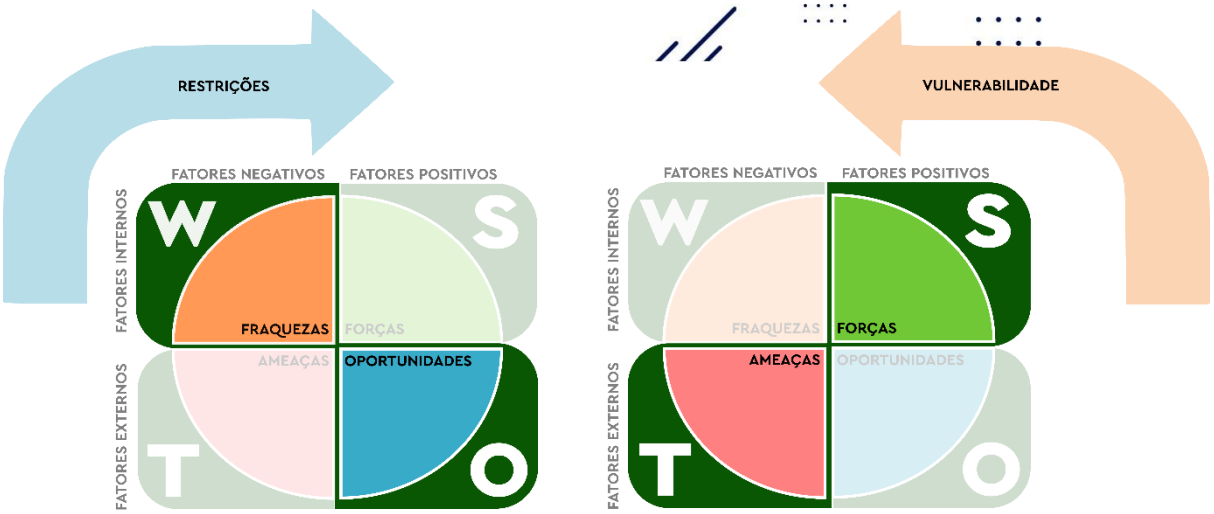
Figura 4 - Matriz SWOT



A identificação das forças, fraquezas, oportunidades e ameaças permite estabelecer a relação ambiental entre os quadrantes da SWOT, de modo a demonstrar a correlação entre eles, conforme as imagens a seguir:

Figura 5 - Relação ambiental entre os fatores da SWOT





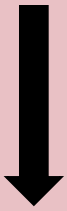
A figura 5 apresenta quadrantes de tonalidade mais colorida e outros esmaecidos. Os quadrantes coloridos demonstram predominância dos fatores em relação aos esmaecidos. Tal predominância é revelada sempre se cotejando fatores do mesmo ambiente, ou seja, internos com internos e externos com externos. Ou seja, uma vez identificadas mais forças do que fraquezas, o quadrante de forças estará colorido e o de fraquezas esmaecido. O mesmo vale para os fatores externos.

Em caso de empate na análise da correlação entre os fatores internos e entre os fatores externos, deve-se de acordo com o princípio da prudência, enquadrar o órgão no quadrante negativo, utilizando-se sempre que necessário o bom senso.

A partir da análise conjugada dos fatores internos e externos da SWOT, podemos identificar a seguir o ambiente no qual está inserido:

Quadro 1 – Análise de Tendência

Ambiente	Tendência	Análise
Alavancagem	↑	Em um ambiente de alavancagem, o órgão apresenta internamente mais forças do que fraquezas, ao passo que em relação ao ambiente externo, encontra-se em um cenário de maiores oportunidades do que ameaças. Sendo assim, há uma tendência de **consolidação** a partir do momento em que o órgão aceita o desafio de fortalecer-se cada vez mais aproveitando as oportunidades apresentadas externamente.
Restrições	↱	Em um ambiente de restrições (limitações), o órgão apresenta internamente mais fraquezas do que forças, ao passo que em relação ao ambiente externo, encontra-se em um cenário de maiores oportunidades do que ameaças. Sendo assim, há uma tendência de **superação** a partir do momento em que o órgão aceita o desafio de transformar seus pontos fracos em fortes, aproveitando as oportunidades apresentadas externamente. O objetivo é transformar pontos fracos em fortes, saindo de um ambiente de restrição para ambiente de alavancagem.

Ambiente	Tendência	Análise
Vulnerabilidades		Em um ambiente de vulnerabilidade, o órgão apresenta internamente mais forças do que fraquezas, ao passo que em relação ao ambiente externo, encontra-se em um cenário de maiores ameaças do que oportunidades. Sendo assim, há uma tendência de **deterioração** a partir do momento em que o órgão não enfrenta o desafio de defender seus pontos fortes cada vez que uma ameaça colocar em risco a sua integridade. O objetivo é se resguardar, evitando sair de um ambiente de vulnerabilidade para ambiente de problemas.
Problemas		Em um ambiente de problemas, o órgão apresenta internamente mais fraquezas do que forças, ao passo que em relação ao ambiente externo, encontra-se em um cenário de maiores ameaças do que oportunidades. Sendo assim, há uma tendência de **extinção** a partir do momento em que o órgão não busca de maneira urgente vencer o desafio de subsistir frente a um ambiente que só tende a expor ainda mais as suas fragilidades. O objetivo é sobreviver, atuando de maneira urgente nas maiores ameaças com potencial de impactar a continuidade do órgão.

De acordo com o ambiente identificado, poderá o órgão utilizar-se de diferentes estratégias de enfrentamento aos riscos. Metodologicamente, a fim de possibilitar o cálculo do apetite a risco sugerido foram atribuídos valores fixos aos ambientes e estratégias sugeridas, conforme tabela abaixo:

Quadro2 - Valores fixos atribuídos ao Ambiente

Ambiente	Valor
Alavancagem – Estratégia Ofensiva – Foco em Fortalecer	4
Restrições – Estratégia de Reforço – Foco em Aprender	3
Vulnerabilidades – Estratégia de Confronto – Foco em Defender	2
Problemas – Estratégia de Defesa – Foco em Resistir	1

Os resultados obtidos na análise do contexto devem ser registrados na planilha constante do apêndice I.

1.1 Definição do grau de maturidade no gerenciamento de riscos

Instituto de complexa definição, a maturidade em gerenciamento de riscos pode ser entendida como o discernimento que o órgão tem acerca dos riscos a que está exposto e a forma institucional como lida com eles, seja formal ou informalmente. A maturidade teria assim correlação direta com o preparo e o modo

como o órgão rotineiramente responde/trata os riscos visando mitigar os eventos que possam desvirtuá-lo do alcance dos seus objetivos.

A análise da maturidade deve ser realizada primordialmente em dois momentos. O primeiro quando se está realizando a análise ambiental no início do ciclo de gerenciamento de riscos, entendendo a atual cultura internado órgão. Já o segundo momento se dá ao final de cada ciclo, possibilitando assim verificar o quanto evoluiu durante o período, amadurecendo, otimizando e sistematizando processos ou estagnando, mantendo-se no mesmo *status quo* anterior. Há ainda a possibilidade de o órgão regredir em sua maturidade, a exemplo de quando descontinua práticas que vinham dando resultado na mitigação de determinados riscos.

A partir da definição do grau de maturidade do órgão e em posse do resultado da análise ambiental deverá então ser definido o apetite a riscos sugerido, sendo este extremamente baixo (em ambientes de vulnerabilidades, restrições e problemas) ou muito baixo (ambiente de alavancagem)quando o grau de maturidade for igual a 1, o que poderá se dar, por exemplo,na implementação da política de gerenciamento de riscos, uma vez que poderá não haver ainda internamente uma cultura formal de tratamento e gestão dos riscos.

Os graus de maturidade poderão se dar nos 3 níveis, de acordo com as características encontradas, conforme a seguir:

Quadro 3 - Graus de Maturidade

Básico	Gestão de riscos tratada informalmente; sem tratamento formalizado dos riscos e com pouca comunicação sobre os riscos.	**Grau 1**
Intermediário	Há princípios e padrões documentados, treinamento básico sobre gestão de riscos, e engajamento parcial da equipe para o gerenciamento dos riscos do setor; há comunicação formal de identificação, tratamento e monitoramento dos riscos.	**Grau 2**
Avançado	Gestão de riscos otimizada e sistematizada; princípios e processos estão integrados aos processos-chave da organização; completo engajamento de toda a equipe no gerenciamento dos riscos; há comunicação formal, periódica e tempestiva de identificação, tratamento e monitoramento dos riscos.	**Grau 3**

1.2 Definição do apetite ao risco

Com base na análise de contexto realizada, o CONINT[1] deverá definir o apetite a risco que o órgão está disposto a aceitar, considerando a importância dos processos-chave instituídos para a consecução dos seus objetivos organizacionais.

Para auxiliar na decisão do CONINT, o apetite a risco poderá ser definido, multiplicando-se o valor correspondente ao ambiente pelo grau de maturidade atribuído ao órgão, obtendo-se os valores para apuração do apetite a risco sugerido, conforme a seguir:

Quadro 4 - Cálculo do Apetite a Risco Sugerido

Ambiente	Grau de Maturidade do Órgão	Resultado
4	3	**12**
	2	**8**
	1	**4**
3	3	**9**
	2	**6**
	1	**3**
2	3	**6**
	2	**4**
	1	**2**
1	3	**3**
	2	**2**
	1	**1**

Os valores obtidos como resultado da multiplicação do ambiente pelo grau de maturidade foram agrupados, dando origem ao quadro a seguir que fixa a faixa de valores para apuração do apetite a risco sugerido:

Quadro5 - Faixa de valores para apuração do Apetite a Risco Sugerido

Apetite a Risco Sugerido[1]	Faixa de Valores
Propenso/tolerável	12
Moderado	8 e 9
Conservador	4 e 6
Avesso	1 a 3

O apetite a risco poderá, ainda, ser classificado como alto quando o órgão entender que a maturidade na gestão de riscos, no nível avançado, atingiu um patamar sustentável a longo prazo e que o monitoramento dos riscos pode ser mais brando devido ao grande controle e preparo que o órgão detém acerca da possibilidade de ocorrência de quaisquer eventos identificados.

[1] A análise dos quadrantes da matriz SWOT conjuntamente com a maturidade apenas sugere um apetite a risco para o órgão, cabendo ao CONINT a definição.

A definição do apetite a riscos é fundamental para que se tenha a correta dimensão dos riscos que obrigatoriamente devem ter algum controle implantado pelo Órgão, guardando relação proporcional ao resultado encontrado na Matriz de Riscos (quadro 6).

Assim, a correlação Apetite *versus* Matriz é representada da seguinte forma:

Quadro 6– Correlação Apetite ao Risco x Riscos Inerentes a serem tratados

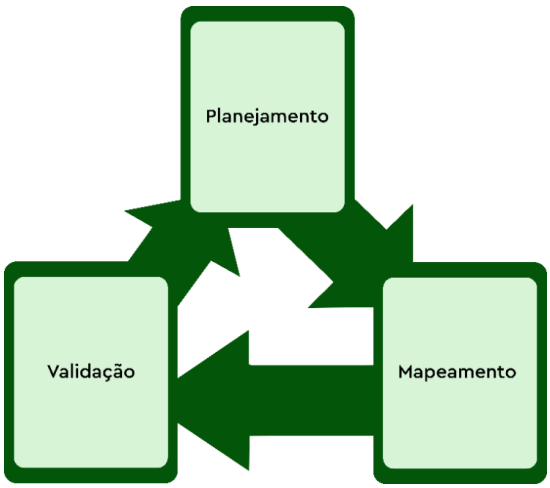
Apetite a Risco Sugerido[2]	Faixa de Valores	Nível do Riscos Inerentes a ser tratado
Propenso/tolerável	12	RI ≥ 16
Moderado	8 e 9	RI ≥ 11
Conservador	4 e 6	RI ≥ 08
Avesso	1 a 3	RI ≥ 04

Caso o CONINT entenda, ou, a CGM-Rio seja legalmente obrigada a tratar todos os riscos, considerar-se-á, o apetite nulo, e RI ≥ 1.

Etapa 2 - Mapeamento de Processos

O Mapeamento é a modelagem dos processos por meio de notação gráfica, que proporciona para a organização um melhor conhecimento do "como" seus processos de trabalho são executados, suas etapas desenvolvidas e seus produtos gerados, a partir dos insumos disponibilizados.

Figura 6 - Etapas do Mapeamento de Processos



O mapeamento, no contexto da PGR, tem como objetivo viabilizar a implantação da metodologia de gerenciamento de riscos, fornecendo informações relevantes sobre cada um dos passos executados no desenvolvimento de cada um dos principais processos de trabalho do órgão, sendo, portanto, ferramenta que auxiliará na identificação dos riscos com potencial para afetar o alcance dos objetivos da organização.

O Mapeamento de Processos proposto segue modelo simplificado, sendo composto por três passos: planejamento, mapeamento e validação.

[2] A análise dos quadrantes da matriz SWOT conjuntamente com a maturidade apenas sugere um apetite a risco para o órgão, cabendo ao CONINT a definição.

2.1 Planejamento

O planejamento consiste no levantamento dos processos-chave a serem mapeados. Neste passo também são definidas as funções associadas ao mapeamento e as ferramentas (formulário, entrevista, observação, etc.) a serem utilizadas para o levantamento de cada etapa do processo junto aos gestores.

2.1.1 Levantamento dos processos-chave

O levantamento dos processos-chave deverá ser realizado com base na análise do ambiente interno e externo, conforme análise de criticidade, levando-se em consideração a relação entre o custo, conforme o nível de complexidade do mapeamento de um processo, e os benefícios que ele poderá gerar à CGM-Rio. Os processos-chave levantados devem ser mapeados e associados aos objetivos estratégicos.

O levantamento dos processos será realizado pelo ponto focal de cada setor com o apoio da CCN e validado pela chefia, a qual deverá, uma vez levantados todos os processos, relacioná-los em planilha de modo a facilitar a identificação daqueles chaves, os quais serão mapeados com prioridade frente aos demais processos do setor.

Uma vez levantados e selecionados os processos-chave, deverá o órgão partir, em parceria com a CCN, para a etapa de mapeamento.

2.1.2 Definição de Funções

Ainda no planejamento deverão ser definidas as funções (responsabilidades) necessárias para o mapeamento de cada um dos processos selecionados, tais como:

Servidor Responsável pelo Processo: pessoa ou grupo de pessoas com responsabilidade sobre a execução e desempenho do processo.

Especialista do Processo: pessoa ou grupo de pessoas que tenham profundo conhecimento sobre as regras necessárias para o funcionamento do processo.

Modelador do Processo: função da CCN, por meio de equipe designada. A equipe realizará a modelagem dos processos em notação gráfica, a partir das orientações do servidor responsável pelo processo com validação do Especialista designado.

2.2 Mapeamento

O Mapeamento será a representação gráfica em notação de modelagem de processos de negócio, ou, como é comumente chamado, pela sigla em inglês, BPMN, com nível de completude e precisão dos processos de trabalho, identificando os atores do processo, os inputs e os outputs, bem como as tomadas de decisão atreladas ao negócio adequados às necessidades de implantação da PGR.

2.3 Validação

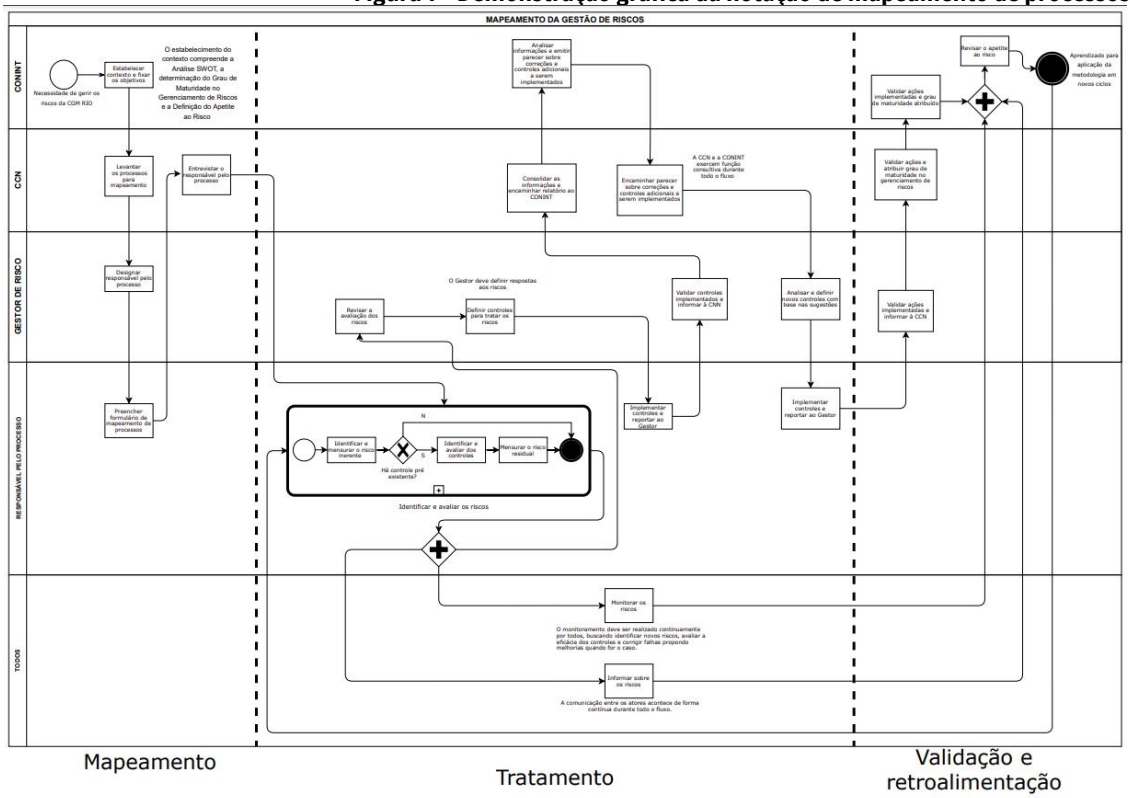
Será realizada a validação do processo-chave mapeado junto ao Especialista do Processo. O objetivo da validação é verificar se o que foi mapeado corresponde ao que é realizado na prática, tendo como resultados possíveis uma validação positiva ou uma sinalização de necessidade de correções no mapeamento.

2.4 Notação Gráfica e Software (ferramenta)

Para realizar o mapeamento de processos de forma ágil, simples e em ambiente gráfico intuitivo é necessária a adoção de procedimentos relacionados ao uso da notação BPMN 2.0 (notação desenvolvida com o objetivo específico de criar um padrão, uma linguagem comum para modelagem de processos de negócios) e o uso de *software* específico.

A seguir é apresentado exemplo de processo mapeado na ferramenta *diagrams.net*, o qual utiliza notação BPMN e diz respeito à Gestão de Riscos conforme as especificações deste manual:

Figura 7 - Demonstração gráfica da notação de mapeamento de processos



Significado dos principais elementos da notação gráfica BPMN:

Quadro 7 -Elementos da notação gráfica BPMN

Evento de Início	Indica o início do processo.	**Tarefa**	Representa um trabalho realizado.
Evento de fim	Indica o fim do processo.	**Gateway Paralelo**	Representa uma decisão a ser tomada ou um ponto de divergência no fluxo do processo.
Evento Intermediário	Indica que algo ocorreu durante o processo.	**Gateway Exclusivo**	Representa a divisão de caminhos que podem ser seguidos simultaneamente e um ponto de convergência no fluxo do processo.

Gestão de Riscos de Projetos

Além dos processos, a CGM-Rio desenvolve projetos, os quais são esforços temporários empreendidos para criar um produto, serviço ou resultado único.

Levando-se isso em consideração, cabe ressaltar que alguns dos Objetivos Estratégicos possuem ações com natureza própria de projeto.

Logo, atendendo ao objetivo geral da gestão de riscos da CGM-Rio de agir para a diminuição dos impactos que possam afetar o alcance dos objetivos traçados no seu planejamento estratégico, esses projetos devem fazer parte do escopo desta metodologia.

Sendo assim, serão considerados projetos-chave os mais importantes para o sucesso de um Objetivo Estratégico.

Esses projetos-chave deverão ser discriminados a partir do Plano de Gerenciamento de Projeto (plano que define como o projeto é executado, monitorado, controlado e encerrado).

O mapeamento de projetos seguirá todas as etapas da gestão de risco presentes neste manual, com exceção do Mapeamento de Processos, respeitando-se diferenças metodológicas pontuais para gestão de risco de projeto quando for necessário.

Desta forma, quando este manual se referir à processo-chave, também há referência à projeto-chave.

IDENTIFICAÇÃO, ANÁLISE E AVALIAÇÃO

Etapa 3– Identificação, análise e avaliação dos riscos e controles

Essa é a etapa por meio da qual são identificados, analisados e registrados os riscos que podem afetar os processos e projetos-chave relacionados aos objetivos estratégicos organizacionais.

Por meio da identificação e análise dos riscos, pode-se planejar as ações de tratamento adequadas e qual o tipo de resposta a ser dada a determinado risco, com base no apetite a risco definido pela organização.

3.1 Como identificar e analisar os riscos?

Levando-se em conta as informações obtidas na etapa análise do contexto, servidores e gestores com conhecimento do processo-chave e visão holística do órgão/setor devem identificar e relacionar riscos negativos ou positivos (oportunidades) que possam impactar o atingimento dos objetivos. Para isso é importante que tenham conhecimento da metodologia de gerenciamento de riscos.

Utilizando o modelo vigente na CGU como parâmetro, cabe dizer que os riscos podem ser identificados a partir de perguntas, como:

Quais eventos podem **EVITAR** 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?

Quais eventos podem **IMPEDIR** o atingimento de um ou mais objetivos do processo organizacional?

Os riscos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa, e, para tanto, podem ser utilizadas as seguintes questões:

O evento é um risco que pode **COMPROMETER** claramente um objetivo do processo?

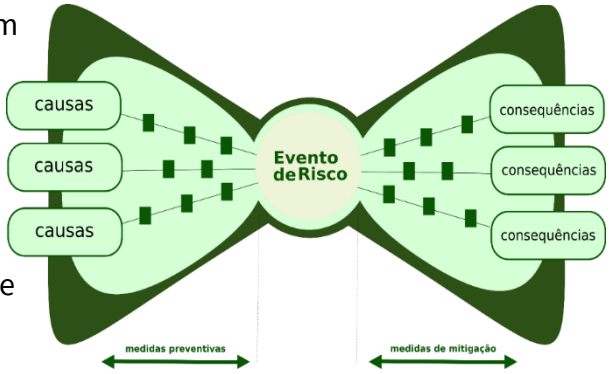
O evento é uma **FALHA** no desenho do processo organizacional?

À luz dos objetivos do processo, o evento identificado é um **RISCO**, uma **CAUSA** ou uma **CONSEQUÊNCIA** do risco?

O evento é uma **FRAGILIDADE** em um controle para tratar um risco do processo?

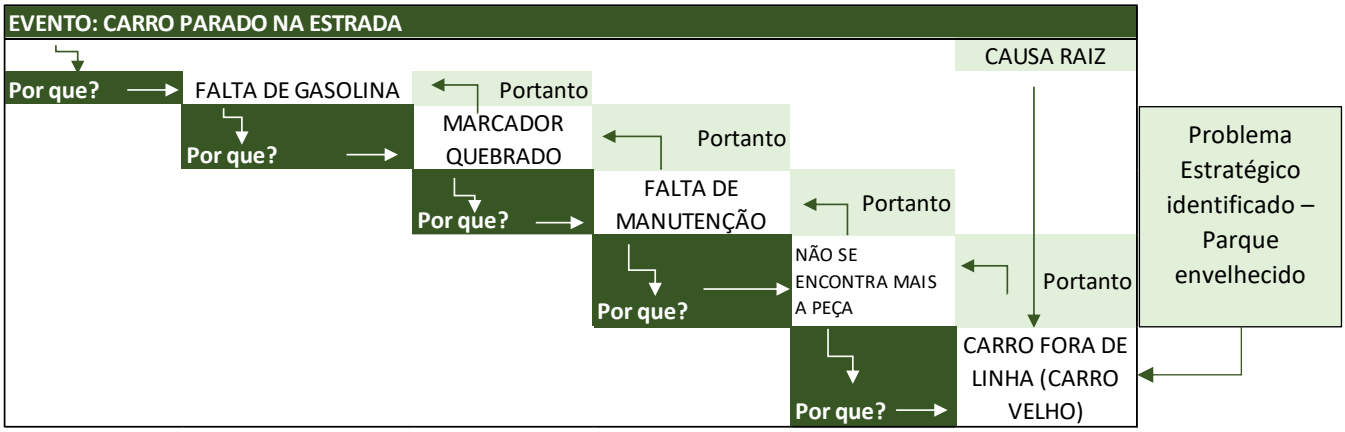
Uma vez identificado o risco, deverá o órgão utilizar a técnica do diagrama de gravata borboleta (*bowtie*) apresentada a seguir, a qual poderá auxiliar na análise do risco, a fim de determinar suas causas e consequências:

Figura 8 - Diagrama de BowTie

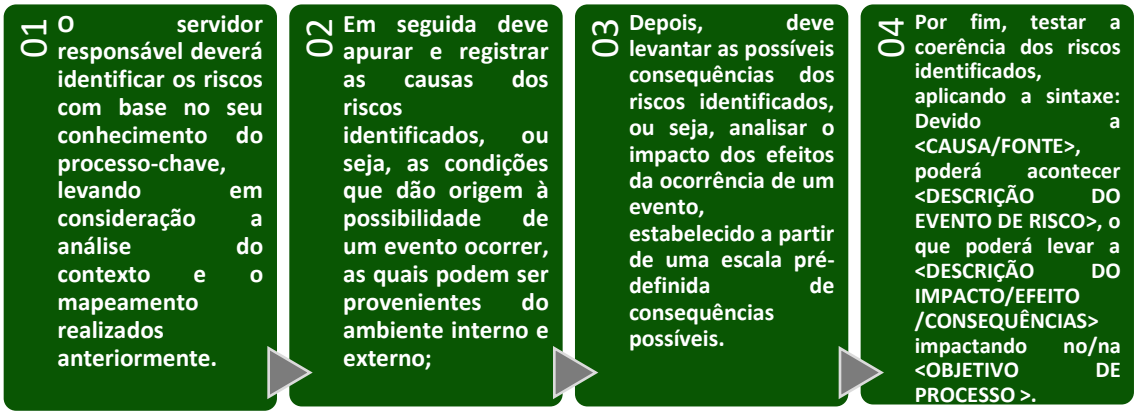


O diagrama de *bowtie* consiste em se determinar os caminhos que um evento de risco percorre desde as causas até as consequências, de modo a identificar as formas de prevenir a ocorrência do risco e as formas de mitigar as consequências caso o risco se materialize.

Além das causas e consequências diretas identificadas no diagrama de *bowtie*, é de fundamental importância que se busque junto ao gestor identificar a causa raiz do evento, a qual se dá pelo constante questionamento dos "porquês" de cada possível causa do evento. Essa causa raiz deve demonstrar ao Órgão questões mais estratégicas de gestão, as quais muitas vezes culminam na identificação de problemas de cunho estrutural, como recursos humanos e/ou materiais.



Passo a passo para realizar essa etapa:



Obtidos os resultados, deve-se fazer o registro nos campos apropriados do formulário de riscos do processo/projeto (apêndice II), conforme a seguir:

Quadro 8 – Campos do formulário de riscos do processo/projeto

PROCESSO-CHAVE	Preencher com o nome do processo-chave ao qual o risco está associado.
RISCOS IDENTIFICADOS	Descrever o evento de risco identificado.
CAUSAS	Descrever as possíveis causas para o evento de risco correspondente.
CONSEQUÊNCIAS	Descrever as possíveis consequências para o evento de risco correspondente.
DIMENSÕES DE RISCOS	Selecionar dentre as opções a categoria de risco correspondente ao risco identificado.

3.2 Dimensões dos riscos

Os riscos que podem afetar o alcance dos objetivos estratégicos da CGM-Rio, observadas as características de sua área de atuação e as particularidades do setor público, podem ser classificados nas dimensões a seguir:

Quadro 9 – Dimensões do Risco

OPERACIONAL	Oriundo de eventos cuja estimativa de perda direta ou indireta seja resultante de falha, deficiência ou inadequação de processos internos, de pessoal ou de sistemas, com a capacidade de impactar diretamente os processos operacionais;
IMAGEM	Eventos que podem comprometer a confiança, credibilidade e reputação junto aos demais órgãos da PCRJ e à sociedade.
CONFORMIDADE	Eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis.
ORÇAMENTÁRIO	Eventos que podem comprometer a capacidade de contar com os recursos orçamentários necessários à realização das atividades; e
INTEGRIDADE	São aqueles relacionados a ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

3.3 Apuração do risco inerente

A apuração do risco inerente será realizada com base nos resultados da análise de contexto e identificação de riscos e na percepção do gestor, seguindo o passo a passo demonstrado a seguir:

1. Estimar e registrar os valores de frequência, observando a escala constante do quadro 9.
2. Estimar e registrar os valores de impacto, observando os fatores para análise e escala constante do quadro 10.
3. Calcular o nível de risco inerente.

Quadro 10 - Escala de Frequência

ESCALA DE FREQUÊNCIA DE OCORRÊNCIA

Aspectos Avaliativos	Evento IMPROVÁVEL (Pode ocorrer apenas em circunstâncias excepcionais)	Evento RARO (Pode ocorrer em algum momento)	Evento ESPERADO (Deve ocorrer em algum momento)	Evento PROVÁVEL (Provavelmente ocorra na maioria das circunstâncias)	Evento CERTO (Em condições normais, o evento ocorrerá)
Frequência	Muito baixa	Baixa	Média	Alta	Muito Alta
Peso	1	2	3	4	5

Quadro 11 - Escala de Impacto

ESCALA DE IMPACTO NOS OBJETIVOS					
Aspectos Avaliativos	Evento de Mínimo impacto	Evento de Pequeno impacto	Evento de Impacto moderado, porém recuperável	Evento de Impacto significativo, de difícil reversão	Evento de Impacto catastrófico, irreversível
Impacto	Muito baixo	Baixo	Médio	Alto	Crítico
Peso	1	2	3	4	5

Os riscos inerentes são calculados pela combinação da frequência da ocorrência do risco e de seu impacto nos objetivos, ou seja, a multiplicação entre os valores provenientes da escala de frequência e os da escala de impacto definem o nível de risco inerente da CGM-Rio.

RI = FE x IR
RI: Nível do Risco inerente / FE: Frequência do Evento / IR: Impacto do risco

A matriz de risco a seguir mostra os níveis de risco inerente que podem ser identificados no Órgão com o resultado da multiplicação dos fatores impacto x frequência:

Figura 9 - Matriz de Riscos e Escala de Nível de Risco

IMPACTO (a)	CRÍTICO	5	RISCO BAIXO 5	RISCO MÉDIO 10	RISCO ALTO 15	RISCO CRÍTICO 20	RISCO CRÍTICO 25
	ALTO	4	RISCO BAIXO 4	RISCO MÉDIO 8	RISCO ALTO 12	RISCO CRÍTICO 16	RISCO CRÍTICO 20
	MÉDIO	3	RISCO MUITO BAIXO 3	RISCO BAIXO 6	RISCO MÉDIO 9	RISCO ALTO 12	RISCO ALTO 15
	BAIXO	2	RISCO MUITO BAIXO 2	RISCO BAIXO 4	RISCO BAIXO 6	RISCO MÉDIO 8	RISCO MÉDIO 10
	MUITO BAIXO	1	RISCO MUITO BAIXO 1	RISCO MUITO BAIXO 2	RISCO MUITO BAIXO 3	RISCO BAIXO 4	RISCO BAIXO 5
MATRIZ DE RISCOS INERENTES (a) x (b)			1	2	3	4	5
			MUITO BAIXA	BAIXA	MÉDIA	ALTA	MUITO ALTA
			FREQUÊNCIA (b)				

Escala de Nível do Risco Inerente		
Tipo	Pontuação	Nível do Risco
RC - Risco Crítico	16 a 25	25
RA - Risco Alto	11 a 15	15
RM - Risco Médio	8a 10	10
RB - Risco Baixo	4 a 7	7
RMB - Risco Muito Baixo	1 a 3	3

NOTA: Para fins de aplicação da metodologia, considerar-se-á como nível do risco o limite superior da pontuação encontrada para cada tipo. Assim, para os riscos críticos, por exemplo, considerar-se-á sempre nível 25 quando pontuar entre 16 e 25 e assim em diante. Tal conhecimento se faz necessário para o entendimento da matriz de risco residual apresentada nas próximas páginas.

3.4 Identificação e avaliação dos controles internos

Esse procedimento tem início com a seguinte pergunta: Existem controles capazes de mitigar os riscos inerentes identificados para os processos-chave selecionados? Caso a resposta seja positiva, deve-se identificar e avaliar os controles internos existentes.

São controles internos os procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros. Os controles internos podem ser classificados quanto ao tipo, quanto à natureza, quanto a sua relação com o risco e, ainda, quanto ao controle compensatório.

3.4.1 Classificação dos controles internos

Quanto ao tipo:

Preventivos– tem como objetivo prevenir falhas, limitando a possibilidade do evento de risco vir a ocorrer. Exemplo: segregação de funções para reduzir a ocorrência de erros.

Evento de risco

Corretivos– tem como objetivo corrigir falhas identificadas após o evento de risco ter ocorrido. Exemplo: rompimento de barragens.

Quanto à natureza:

Manual

- controles que são realizados por pessoas. Exemplo: conferência de assinatura.

Automatizado

- controles processados por um sistema, não havendo intervenção humana na sua realização. Exemplo: Limite de liberação de verba.

Híbridos

- controles que mesclam atividades manuais e automatizadas

Quanto à Relação com o Risco:

Controles Diretos	Têm como objetivo mitigar o risco. Estão mais relacionados aos controles operacionais. Exemplo: Conferência dos pagamentos a serem efetuados.
Controles Indiretos	Têm como objetivo a prevenção e a detecção de eventos de risco, auxiliando na mitigação do risco. Estão mais relacionados ao ambiente de controle. Exemplo: Grade de treinamentos obrigatórios para os funcionários.

Quanto ao Controle Compensatório:

Existe ainda o controle compensatório que é o controle adotado **provisoriamente** para mitigar o risco até que seja implementado o controle interno definitivo. É utilizado quando o controle ideal não pode ser implementado no curto prazo em razão da sua complexidade, alto custo e etc.

Exemplo: Informatização de processo cuja implementação ocorrerá no longo prazo, demandando adotar, temporariamente, controles manuais.

3.4.2 Requisitos para manutenção/implementação de controles internos

Uma vez identificados os riscos inerentes e os controles internos preexistentes em seus respectivos níveis, será necessário avaliar se esses controles internos são eficazes, proporcionais, adequados e razoáveis ao risco encontrado, de modo a decidir pela manutenção, adaptação, melhoria dos controles existentes ou pela implementação de novos controles que atendam aos requisitos especificados.

Ao lado podem ser encontrados os requisitos a serem levados em consideração na análise da dosimetria correta do controle aplicado a determinado risco.

Figura 10 - Requisitos controles internos

Cumpre ressaltar que os controles internos devem atender primordialmente o requisito da eficácia, sendo este o primeiro que deverá ser analisado. A eficácia é considerada condição mínima para a análise dos demais, ou seja, somente cabe falar em proporcionalidade (2), por exemplo, se o controle de algum modo, produzir efeitos. Caso não tenham atendido o requisito da eficácia devem os controles ser classificados diretamente no nível ineficaz constante do quadro a seguir:

Quadro12 - Nível dos Controles Internos Existentes

NÍVEL DOS CONTROLES INTERNOS EXISTENTES			
Nível	**Descrição**	**Análise de Requisitos**	**Fator de Avaliação de Controles**
Ineficaz	Controles ineficazes, mal desenhados ou mal implementados, não funcionais.	Não atende nenhum dos requisitos.	**1,0**
Fraco	Controles não institucionalizados, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Atende somente 1 dos requisitos.	**0,8**
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiência no desenho ou nas ferramentas utilizadas. O controle é considerado mediano quando não atende 2 dos requisitos para manutenção/implementação.	Atende 2 dos requisitos.	**0,6**
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente. O controle é considerado satisfatório quando atende 3 dos 4 requisitos para manutenção/implementação.	Atende 3 dos requisitos.	**0,4**
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco. O controle é considerado forte quando atende todos os requisitos para manutenção/implementação.	Atende todos os requisitos.	**0,2**

3.5 Apuração do risco residual

Uma vez identificados e avaliados os controles existentes, deve-se apurar o risco residual.

Multiplicando-se o nível obtido para o risco inerente pelo fator de avaliação dos controles obtém-se o nível de risco residual, que pode variar de 1 a 25, conforme fórmula a seguir:

RR = RI x FAC
RR: Nível do Risco Residual / RI: Nível de risco inerente/ FAC: Fator de Avaliação de Controles

A matriz de risco a seguir mostra os níveis de risco residual que podem ser identificados no Órgão com o resultado da multiplicação risco inerente x fator de avaliação dos controles:

Figura 11–Matriz de Riscos e Escala de Nível de Risco

NÍVEL DO RISCO INERENTE (a)	CRÍTICO	25	RISCO BAIXO 5	RISCO MÉDIO 10	RISCO ALTO 15	RISCO CRÍTICO 20	RISCO CRÍTICO 25
	ALTO	15	RISCO MUITO BAIXO 3	RISCO BAIXO 6	RISCO MÉDIO 9	RISCO ALTO 12	RISCO ALTO 15
	MÉDIO	10	RISCO MUITO BAIXO 2	RISCO BAIXO 4	RISCO BAIXO 6	RISCO MÉDIO 8	RISCO MÉDIO 10
	BAIXO	7	RISCO MUITO BAIXO 1,4	RISCO MUITO BAIXO 2,8	RISCO BAIXO 4,2	RISCO BAIXO 5,6	RISCO BAIXO 7
	MUITO BAIXO	3	RISCO MUITO BAIXO 0,6	RISCO MUITO BAIXO 1,2	RISCO MUITO BAIXO 1,8	RISCO MUITO BAIXO 2,4	RISCO MUITO BAIXO 3
MATRIZ DE RISCOS RESIDUAIS (a) x (b)			0,2	0,4	0,6	0,8	1
			FORTE	SATISFATÓRIO	MEDIANO	FRACO	INEFICAZ
			FATOR DE AVALIAÇÃO DE CONTROLES (b)				

Escala de Nível de Risco Residual		
Tipo	Pontuação	Nível do Risco
RC - Risco Crítico	16 a 25	25
RA - Risco Alto	11 a 15	15
RM - Risco Médio	8 a 10	10
RB - Risco Baixo	4 a 7	7
RMB - Risco Muito Baixo	0 a 3	3

NOTA: Apenas os riscos inerentes com controles preexistentes terão o risco residual apurado. Os riscos inerentes para os quais não foram identificados controles irão diretamente para as etapas seguintes do gerenciamento de riscos. Depois da avaliação da existência ou não de controles e da apuração do risco residual, ambos convergirão para as etapas seguintes, não havendo diferença na nomenclatura dos riscos, assim não se fará mais diferenciação entre riscos inerentes e riscos residuais.

Em função do caráter mitigador dos controles internos existentes, o valor do risco residual pode fazer com que o risco se enquadre em uma faixa de classificação igual ou inferior ao da faixa definida para o risco inerente.

Os resultados obtidos tanto para o risco inerente como para o risco residual devem ser registrados em campo específico do mapa de riscos, o qual servirá de base para a definição do tratamento proposto.

De posse das escalas de cada um dos riscos levantados, deve o órgão partir para a interpretação de cada um dos níveis, os quais demonstram o possível impacto daquele risco na continuidade do órgão devido à sua criticidade.

A seguir pode ser vista a relação criticidade x impacto de cada risco (inerente e residual) identificado na CGM-Rio:

CRÍTICO: aqueles caracterizados por riscos associados à **paralisação**/**interrupção** de operações, atividades, projetos, programas ou processos, que causam impactos **irreversíveis** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas;

ALTO: aqueles caracterizados por riscos associados à **interrupção** de operações, atividades, projetos, programas ou processos, que causam impactos de **reversão muito difícil** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas;

MÉDIO: aqueles caracterizados por riscos associados à **interrupção/degradação** de operações ou atividades, de projetos, programas ou processos, que causam impactos **significativos** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/ serviços às partes interessadas, porém recuperáveis;

BAIXO: aqueles caracterizados por riscos associados à **degradação** de operações, atividades, projetos, programas ou processos, que causam impactos **pequenos** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas; e

MUITO BAIXO: caracterizados por riscos associados à **degradação** de operações, atividades, projetos, programas ou processos, que causam impactos **mínimos** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Uma vez finalizada a apuração do risco residual, deverá o servidor responsável informar ao gestor do processo-chave para que este proceda a revisão da avaliação realizada, a fim de subsidiar a definição dos controles novos/ou otimizados.

Tratamento e Implementação do Gerenciamento de Riscos

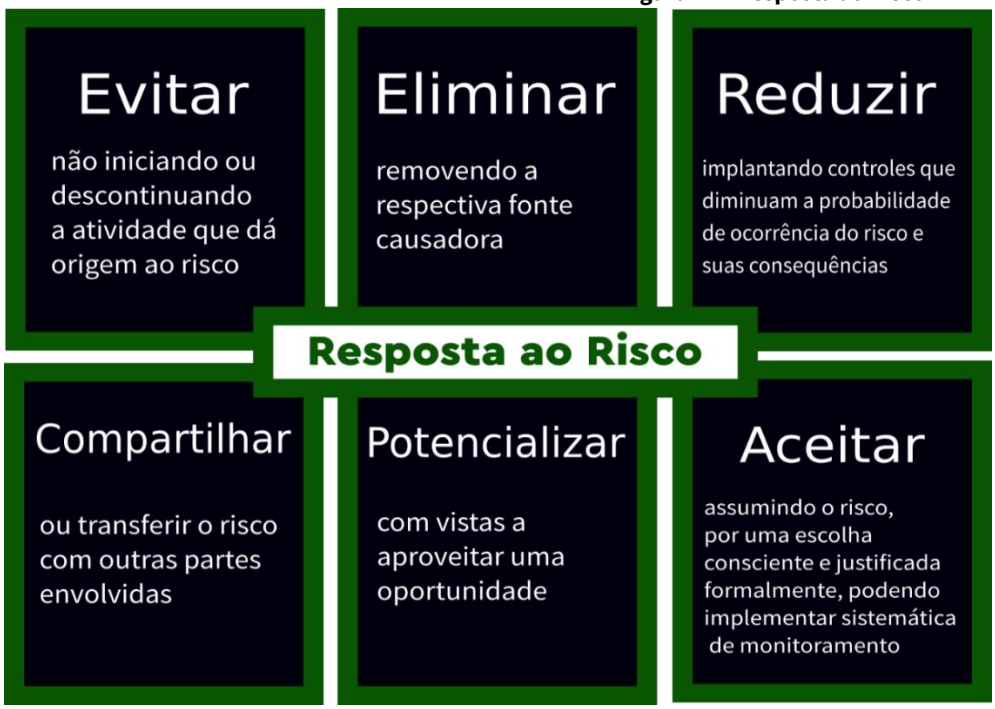
Etapa 4 - Tratamento dos riscos

Nessa etapa serão definidos os controles novos/ou modificados a serem implementados para tratamento dos riscos identificados. O tratamento tem como objetivos a identificação e seleção das estratégias de ação mais viáveis e adequadas, e o desenvolvimento de controles internos capazes de evitar, eliminar, reduzir, aceitar, compartilhar ou transferir riscos negativos, ou potencializar riscos positivos.

A estratégia de ação a ser implementada para o tratamento dos riscos deve ser escolhida de acordo com o nível de risco residual a que se está exposto após a avaliação da efetividade dos controles internos existentes. Dependendo da estratégia de ação definida, poderão ser propostos novos controles ou modificados os controles existentes.

Após revisão da etapa de análise e avaliação dos riscos e em função do nível de risco residual apurado, sugere-se adotar as estratégias de ação (respostas ao risco) correspondente, conforme a seguir:

Figura 12 - Resposta ao Risco



Quadro 13 – Respostas ao Risco sugeridas

Apetite a Risco Sugerido	Nível do Risco Residual	Resposta ao Risco Sugerido
Moderado	Crítico	Evitar, eliminar, reduzir, compartilhar
	Alto	Evitar, eliminar, reduzir, compartilhar
	Médio	Aceitar, evitar, eliminar, reduzir, compartilhar
	Baixo	Aceitar, evitar, eliminar, reduzir, compartilhar
	Muito Baixo	Aceitar, evitar, eliminar, reduzir, compartilhar
Baixo	Crítico	Evitar, eliminar, reduzir, compartilhar
	Alto	Evitar, eliminar, reduzir, compartilhar
	Médio	Evitar, eliminar, reduzir, compartilhar
	Baixo	Aceitar, evitar, eliminar, reduzir, compartilhar
	Muito Baixo	Aceitar, evitar, eliminar, reduzir, compartilhar
Muito Baixo	Crítico	Evitar, eliminar, reduzir, compartilhar
	Alto	Evitar, eliminar, reduzir, compartilhar
	Médio	Evitar, eliminar, reduzir, compartilhar
	Baixo	Evitar, eliminar, reduzir, compartilhar
	Muito Baixo	Aceitar, evitar, eliminar, reduzir, compartilhar
Extremamente Baixo	Crítico	Evitar, eliminar, reduzir, compartilhar
	Alto	Evitar, eliminar, reduzir, compartilhar
	Médio	Evitar, eliminar, reduzir, compartilhar
	Baixo	Evitar, eliminar, reduzir, compartilhar
	Muito Baixo	Evitar, eliminar, reduzir, compartilhar

As respostas ao risco devem ser definidas levando-se em consideração o nível de risco residual apurado em relação ao apetite ao risco da CGM-Rio, conforme as sugestões de respostas possíveis do quadro a seguir:

Deve-se implementar as ações de tratamento obedecendo aos seguintes critérios para:

AÇÕES DE IMPLANTAÇÃO IMEDIATA

- Quando a avaliação realizada indicar níveis de **RISCO ALTO OU CRÍTICO**, ou, nos casos de risco negativo, quando a continuidade ou repetição das vulnerabilidades tiver potencial para transformá-lo em risco alto ou crítico;

AÇÕES DE IMPLANTAÇÃO DE CURTO PRAZO

- Quando a avaliação realizada indicar níveis de **RISCO MÉDIO**, ou, nos casos de risco negativo, quando a continuidade ou repetição das vulnerabilidades tiver potencial para transformá-lo em risco médio;

AÇÕES DE IMPLANTAÇÃO DE MÉDIO PRAZO

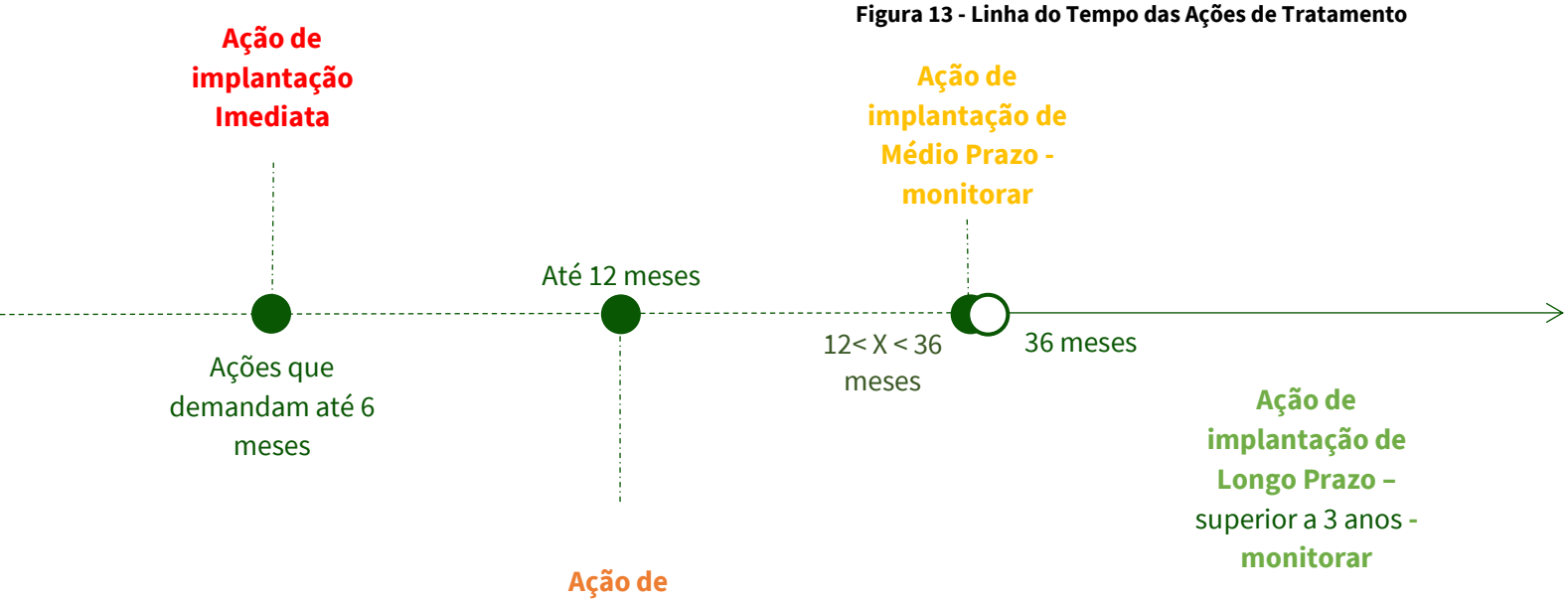
- Quando a avaliação realizada indicar níveis de **RISCO BAIXO**; e

AÇÕES DE IMPLANTAÇÃO DE LONGO PRAZO

- Quando a avaliação realizada indicar níveis de **RISCO MUITO BAIXO**.

Para implementação das ações de tratamento, considera-se os seguintes prazos:

Figura 13 - Linha do Tempo das Ações de Tratamento



4.1 Formulário de riscos do processo/projeto

As ações de tratamento propostas serão implementadas por meio do formulário de riscos do processo/projeto (apêndice II). Nele serão concebidos os controles necessários para tratar os riscos identificados e as ações de monitoramento para avaliar a efetividade desses controles, priorizando-se os riscos situados nos níveis “crítico” e “alto”, ou seja, na faixa em que o risco residual esteja entre 16 a 25 (Vide pág. 30).

As ações implementadas devem ser validadas pelo gestor do processo-chave e informadas à CCN para elaboração de relatório consolidado a ser encaminhado a CONINT.

O CONINT efetuará a análise das informações e poderá emitir parecer sobre correções e controles adicionais a serem implementados. O parecer emitido pela CONINT será devolvido à CCN e encaminhado aos gestores dos processos-chave para análise e definição de controles com base nas sugestões apresentadas.

Nos casos de riscos positivos (oportunidades), quando priorizados, as ações respectivas terão o objetivo de potencializá-los, com vistas ao seu aproveitamento.

Os riscos considerados de nível mínimo poderão ser apenas monitorados, sendo facultado ao respectivo gestor do processo-chave implantar as ações de gerenciamento, sempre considerando o custo benefício entre o impacto gerado em relação à complexidade e a demanda de trabalho imposta pela ação de tratamento.

Os riscos classificados como institucionais deverão ser imediatamente submetidos a avaliação da CONINT. Já os riscos setoriais deverão ser identificados e avaliados pelo servidor responsável e revisados e validados pelo gestor de riscos, sendo posteriormente submetidos à análise da CONINT.

O gestor do processo-chave pode alterar a ação de tratamento adotada se assim achar necessário, desde que seja apresentada justificativa válida a CONINT.

4.2 Plano de Ação para tratamento do risco

Para o efetivo tratamento do risco, recomenda-se a estruturação de um trabalho. O plano de ação para tratamento de riscos é um documento detalhado que estabelece as etapas específicas que a CGM-Rio, através de suas unidades, seguirá para tratar um risco identificado. Ele descreve as ações a serem realizadas, os responsáveis por essas ações, os prazos para sua conclusão e os recursos necessários.

O plano de ação é desenvolvido como parte do processo de gestão de riscos para (conforme já mencionado) aceitar, evitar, eliminar, reduzir, compartilhar, ou potencializar riscos que podem afetar a organização. Deve ser detalhado e orientado por prazos realistas. Suas ações devem ser atribuídas a indivíduos ou equipes responsáveis, e o monitoramento contínuo é fundamental para garantir que as ações sejam implementadas conforme planejado. Além disso, a revisão e atualização regulares do plano garantirão que ele permaneça relevante ao longo do tempo e continue a lidar eficazmente com o risco residual identificado.

Quadro 14 – Plano de Ação

Risco Residual	*Nome do risco identificado*
Nível do Risco	*Crítico, alto, médio, baixo, muito baixo*
Estratégia de Resposta	*Aceitar, evitar, eliminar, reduzir, compartilhar, potencializar*
Objetivo/ Meta	*Informar o resultado esperado do plano de ação com base no(s) indicador(es) chave de desempenho (KPIs)*

Plano de Ação para tratamento do risco				
Etapa/ Ação N	**Descrição**	**Responsável**	**Recursos**	**Prazo**
Nome da etapa/ ação	*O quê e/ou quanto será feito*	*Quem responde pela implementação*	*Os insumos ou participantes necessários para a etapa/ ação*	*De quando até quando*
Etapa/ Ação N +1	**Descrição**	**Responsável**	**Recursos**	**Prazo**
(...)	*(...)*	*(...)*	*(...)*	*(...)*
Avaliação		**Alterações**		
O que possa afetar o cronograma geral e as ações necessárias para para cumprimento do objetivo/ meta		*Com base na avaliação, quais alterações devem ocorrer para cumprimento do objetivo/ meta*		

4.3 Indicador-Chave de Desempenho (KPI)

Os Indicadores-Chave de Desempenho (KPIs) em um plano de ação para tratamento de riscos são métricas quantitativas ou qualitativas usadas para medir o progresso, o sucesso e a eficácia das ações implementadas para lidar com um risco específico. Eles fornecem uma maneira objetiva de avaliar se as estratégias de resposta estão funcionando conforme o planejado e se o risco está sendo gerenciado de maneira eficaz. A correta identificação dos indicadores medirá o sucesso da implementação das ações e a eficácia da mitigação do risco.

A elaboração de um eficaz KPI baseia-se em atributos conforme a seguir:

Quadro 15 – Atributos de um KPI

Atributo	Descrição
Relevância	Deve estar diretamente relacionado aos objetivos estratégicos da CGM-Rio e às áreas/ unidades dimensionadas.
Mensurabilidade	Precisa ser quantificável ou qualificável de alguma forma. Ele deve ser mensurável em termos numéricos ou em categorias que permitam a comparação ao longo do tempo.
Alinhamento	Deve estar alinhado com as metas e os objetivos estratégicos da CGM-Rio, refletindo a contribuição do desempenho em direção ao sucesso geral.
Tempo	Deve ter um período de referência definido, como diário, semanal, mensal ou anual. Isso permite a comparação de dados ao longo do tempo e a identificação de tendências.
Clareza	Deve ser fácil de entender e interpretar. Ele deve comunicar claramente o que está sendo medido, como está sendo medido e por que é importante.
Objetividade	Deve ser objetivo, baseado em fatos concretos, não em opiniões ou interpretações subjetivas. Isso ajuda a garantir a consistência na medição.
Disponibilidade	Deve ser possível coletar os dados necessários para calcular o KPI de maneira eficaz e precisa, preferencialmente sem custo ou com custo mínimo de tempo.
Comparabilidade	Um bom KPI é comparável ao longo do tempo ou em relação a *benchmarks*, metas anteriores ou outras referências relevantes. Isso ajuda a avaliar o desempenho relativo
Limitação	É mais eficaz focar em um número limitado de KPIs significativos e relevantes. Isso evita a sobrecarga de informações e permite uma análise mais aprofundada.

Além disso, a clareza na divulgação da fórmula de cálculo é essencial para a precisão e a consistência na medição do desempenho por meio de KPIs. Tal fórmula precisa ser claramente definida e compreendida por todas as partes interessadas envolvidas na medição e interpretação do KPI.

Monitoramento

Etapa 5 - Monitoramento dos Riscos

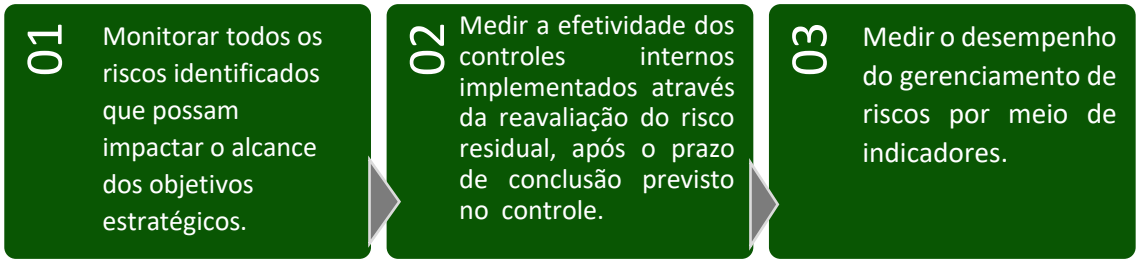
O gerenciamento dos riscos de uma organização pode passar por mudanças com o passar do tempo devido a: alterações nos objetivos institucionais; legislação e normas; controles internos que não estão mais produzindo os resultados desejados ou que deixaram de ser executados; ou por qualquer outra condição que possa afetar o alcance dos objetivos institucionais.

Essa etapa destina-se a assegurar a sustentabilidade e eficiência do gerenciamento de riscos implementado, no longo prazo, através do monitoramento contínuo e cíclico da sua execução, buscando aferir a adequação, suficiência e eficácia dos controles internos propostos e se os prazos estão sendo cumpridos.

O monitoramento deve perpassar todo o processo de gerenciamento, desde a identificação dos riscos até a atribuição da maturidade.

É importante salientar que tal procedimento deve ser realizado com base na análise e observação crítica das informações pelos setores da CGM-Rio e na prestação de contas através da elaboração de relatório consolidado anual dos resultados das ações implementadas.

Em razão disso, pode-se dizer que convém durante o monitoramento:



A tabela a seguir relaciona os indicadores mínimos que devem ser utilizados para medir o desempenho do gerenciamento de riscos e a eficácia dos controles internos propostos, podendo ser implementados outros conforme a necessidade do setor/órgão:

Quadro 16 – Indicadores de Risco

INDICADOR	FÓRMULA
% riscos tratados por setor	riscos tratados/total de riscos identificados
% controles concluídos por setor	controles concluídos/total de controles do setor
% controles em andamento por setor	controles em andamento/total de controles do setor
% controles atrasados por setor	controles atrasados/total de controles do setor

Para o cálculo do indicador de riscos tratados serão considerados os processos-chave que tiverem como resposta reduzir, compartilhar/ou transferir e potencializar o risco, podendo incluir também "aceitar o risco" quando houver a opção de implementar sistemática de controle para riscos aceitos.

Ao final do processo de monitoramento deverá ser realizada uma reavaliação da maturidade do órgão com base no gerenciamento/tratamento dos riscos realizado pelos setores. Tal reavaliação não precisa ter necessariamente formato ou escopo padronizado, devendo somente seguir as diretrizes propostas nesse manual, adaptando-se às alterações identificadas no ambiente interno e externo da organização e modificando-se conforme as necessidades de informações a serem fornecidas ao CONINT.

Nota: O monitoramento dos riscos poderá ser realizado pela CCN e também pelo Núcleo de Monitoramento Estratégico – NUME da Controladoria.

Informação e Comunicação

Etapa 6 - Informação e Comunicação de Alteração de Riscos e Controles

A etapa de informação e comunicação tem por finalidade o aprimoramento contínuo do gerenciamento dos riscos, por meio da comunicação regular, tempestiva e periódica de novos riscos, de alteração de status dos riscos já identificados (agravamento / mitigação), das alterações ocorridas nos processos de trabalho ou do grau de eficácia dos controles realizados, de modo a garantir a possibilidade de tomada de decisão pelo CONINT visando manter efetividade e a eficácia das ações adotadas para o tratamento dos riscos.

Durante todo o ciclo de gerenciamento de riscos, os responsáveis pelas tarefas devem manter um fluxo regular e constante de comunicação com os setores envolvidos, mantendo-os informados sobre cada alteração nesse processo.

Sendo assim, toda informação relevante deverá ser identificada, registrada e comunicada tempestivamente, a fim de permitir a aplicação da metodologia de gerenciamento de riscos e a atribuição de responsabilidades, orientar a tomada de decisão e contribuir com o monitoramento do sistema.

Fazem parte dessa etapa de informação e comunicação, a disponibilização das ações realizadas ao CONINT, aos servidores envolvidos no processo-chave ao qual o risco está associado e a Coordenadoria Técnica de Controles e Normas - CCN, bem como a ampla divulgação desse Manual a todos os servidores.

Continuidade do Negócio (ISO 22301)

Ainda que considerada implantada a metodologia, não há como se extinguir um risco, com exceção da eliminação de suas causas. No entanto, como para grande parte das organizações, a descontinuidade dos processos de trabalho que apresentam riscos significaria a paralisação dos serviços prestados, uma vez que tais riscos são, muitas vezes, inerentes aos processos, controles são implantados para atenuar as causas (impacto e frequência), e consecutivamente, os danos causados por suas consequências.

Essas consequências, por sua vez, ainda que mitigadas, podem vir a gerar alto impacto no alcance dos objetivos da organização. E, para que não ocorram danos irreversíveis ou de difícil reparação, que interrompam total ou parcialmente a prestação de serviços, recomenda-se que sejam elaborados para os riscos de maior repercussão organizacional, protocolos de contingenciamento capazes de conferir à organização maior capacidade de responder tempestivamente aos impactos gerados pelo evento danoso.

E é nesse estágio que surge o Sistema de Gestão de Continuidade de Negócios (SGCN) da CGM-RIO Rio, o qual, com base na ISO 22301, cria o Plano de Contingência de Riscos de Alto Impacto - PCR e o Comitê de Gestão de Crises da Organização, este a cargo da CONINT e cujas atribuições serão definidas em resolução específica.

O SGCN, portanto, é uma etapa avançada da Política de Gestão de Riscos, devendo ser moldado pelos requisitos legais, regulatórios e organizacionais da CGM-RIO, de modo a agregar em seu produto principal maior senso de urgência aos servidores do órgão àquelas demandas que são mandatórias cujo atraso poderia ensejar prejuízos à municipalidade e responsabilização nas esferas administrativa, cível ou penal dos gestores do órgão.

O SGCN surge da experiência dos últimos anos, nos quais surgiram dois exemplos claros de eventos que demonstraram a necessidade da existência de planos de continuidade do negócio. O primeiro foi a pandemia global da COVID-19 que, com a instituição das quarentenas, obrigou boa parte dos trabalhos a serem realizados de maneira remota, alterando completamente rotinas de trabalho e gerando grande necessidade de adaptação dos colaboradores. O segundo evento fora o ataque cibernético sofrido pela Prefeitura da Cidade do Rio de Janeiro em agosto de 2022, o qual suspendera por semanas a utilização de grande parte dos sistemas informatizados do município, gerando inclusive enorme receio de perda/vazamento de dados e o descumprimento de prazos da Lei de Responsabilidade Fiscal, do STN, a ordem cronológica de pagamentos, entre outros.

Sendo assim, deve a CGM-RIO, além detratar os riscos gerais do órgão, se voltar com prioridade ao tratamento daqueles que possam afetar a continuidade dos serviços prestados ao cidadão.

É importante destacar que não se deve confundir impacto com gravidade. A gravidade deve ser considerada forma de medição do impacto. Exemplo é um fenômeno de queda de energia. A depender da duração da queda do fornecimento a gravidade irá aumentar. O impacto ocorre já com a interrupção do fornecimento, uma vez que suspende o uso dos equipamentos e dos serviços, no entanto, sua gravidade poderá ser mínima, se a duração for de apenas alguns segundos ou minutos, ou máxima, se durar dias, semanas ou for permanente.

A título exemplificativo, traçando-se um paralelo com uma unidade hospitalar, não se pode falar em gravidade mínima, uma vez que o impacto e a gravidade já serão altos ainda que com baixa duração, caso não exista gerador em funcionamento para a manutenção dos atendimentos/procedimentos hospitalares.

Segundo a ISO 22301[3], os efeitos do SGCN podem ser demonstrados pela imagem a seguir:

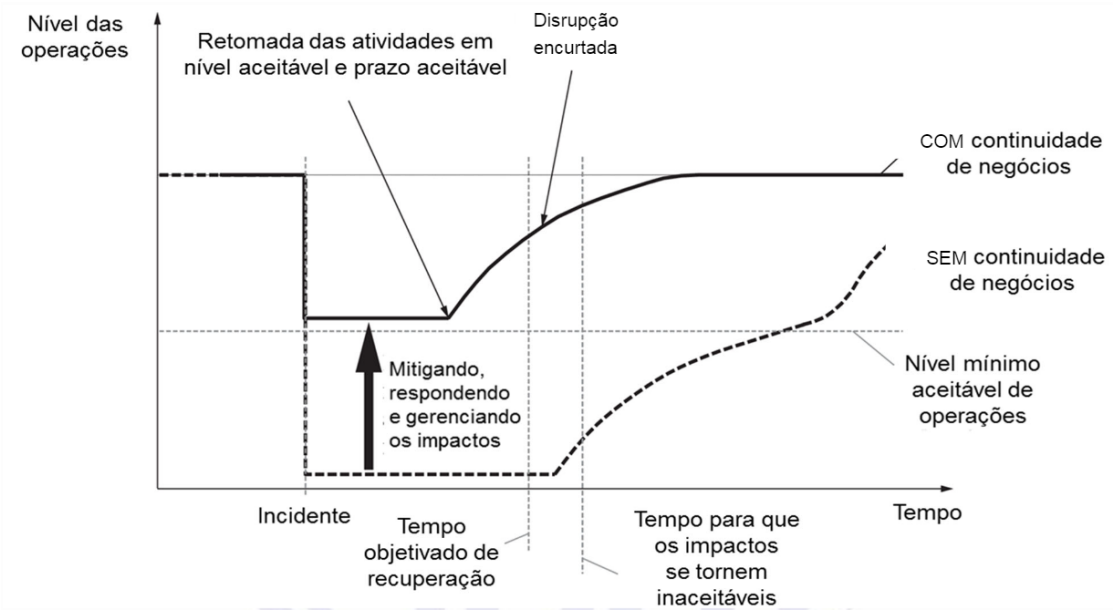


Figura 14 –Eficácia do SGCN (Fonte ISO 22301)

[3] ISO 22301 (Segurança e Resiliência – Sistema de gestão de continuidade de negócios – requisitos) – Segunda Edição – 01.06.2020.

É importante ressaltar que o SGCN envolve toda a organização, uma vez que as respostas precisam ser dadas de forma tempestiva, o que só é possível se todos estiverem cientes do plano traçado. Exemplo disso é um plano de evacuação em caso de incêndio. A tendência é que a resposta seja melhor dada pelo órgão se todos souberem como se comportar e como agir na situação colocada.

A seguir pode-se visualizar um modelo simplificado de formulário de Análise

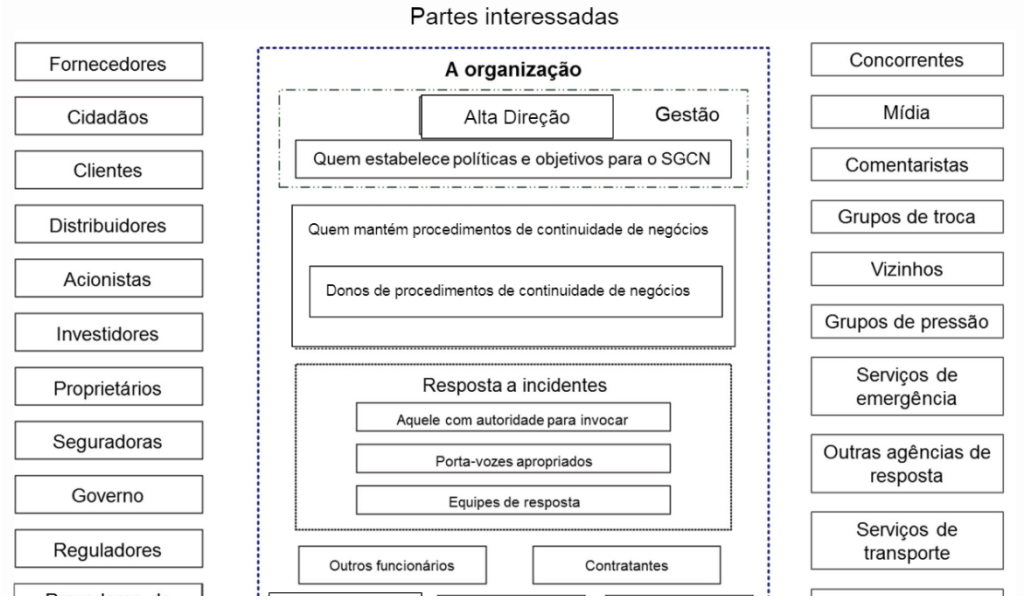


Figura 15 – Na área azul todos aqueles que participam do SGCN, fora dela, aqueles que são stakeholders, mas não detém ações a tomar.

de Impacto do risco no desempenho das atividades do órgão e sua gravidade quando analisada de modo temporal.

BIA - Análise de Impacto no Negócio			
Processo-Chave			
Gestor do Processo			
Data da Avaliação		Revisão:	
Evento Crítico			
IMPACTO CGM-RIO / PCRJ			
TEMPO:	IMPACTO		
- Primeiras 24h			
- 24h - 48h			
- 48h - 72h			
≥ 1 semana			
≥ 1 mês			
≥ 3 meses			
PARA RECUPERAÇÃO			
TEMPO:	QUEM:	REQUISITOS:	COMO:
- Primeiras 24h			
- 24h - 48h			
- 48h - 72h			
≥ 1 semana			
≥ 1 mês			
≥ 3 meses			

Quadro 17 – Modelo de BIA

Gestão de Riscos de Integridade, Fraude e Corrupção (ISO 37001)

A CGM-Rio reconhece que **os riscos de fraude e de corrupção possuem natureza crítica e demandam tratamento específico, ainda que integrados à Política de Gestão de Riscos institucional**. Por seu potencial de comprometer a integridade, a credibilidade e a legitimidade da Administração Pública, exigem **protocolos próprios** de prevenção, detecção, resposta e monitoramento, alinhados ao Programa Nacional de Prevenção à Corrupção (PNPC), à Política da Prefeitura do Município do Rio de Janeiro e às diretrizes da ISO 37001:2016 (Sistema de Gestão Antissuborno).

A gestão de riscos de fraude e corrupção será conduzida com base em princípios fundamentais:

- **Compromisso da liderança** com a prevenção e o combate a fraudes e atos de corrupção, assegurando a responsabilização efetiva dos envolvidos;
- **Integração à governança**, alinhada ao Código de Ética, à Política de Integridade e às normas internas da CGM-Rio;
- **Prevenção como prioridade**, com foco na redução das oportunidades e no fortalecimento dos controles internos;
- **Transparência e a accountability**, assegurando a divulgação responsável das ações e resultados; e
- **Proteção ao denunciante**, com confidencialidade e não retaliação.

O processo de gestão de riscos de fraude e corrupção da CGM-Rio é periódico e sistemático, estruturado nas mesmas etapas da metodologia de gerenciamento de riscos institucional, com ênfase nas seguintes particularidades:

Ambiente de Controle

O objetivo é fomentar uma cultura que desestimule a fraude e a corrupção, fortalecendo a integridade e a ética desde a alta administração (*tone at the top*), as lideranças intermediárias (*tone in the middle*) e os profissionais que atuam nas pontas (áreas técnicas e atividades-meio).

Isso inclui a revisão contínua e sistemática de aspectos culturais, legais, regulatórios, políticos, governança, estruturas, estratégias, processos, normas e relações com partes interessadas, identificando pontos de vulnerabilidade e oportunidades de melhoria no ambiente de controle, especialmente no que tange aos aspectos de fraude e corrupção.

Identificação de Riscos Inerentes de Fraude e Corrupção

A CGM-Rio realiza o mapeamento sistemático e multidisciplinar dos riscos de **fraude e corrupção que potencialmente podem ocorrer na ausência de controles internos eficazes,** utilizando o **Triângulo da Fraude**:

- **Pressão/Motivação:** análise dos incentivos ou necessidades que poderiam levar um indivíduo a cometer um ato de fraude ou corrupção (ex: dificuldades financeiras, metas irrealistas, ambição, ganância).
- **Oportunidade:** identificação de falhas, lacunas ou fragilidades nos controles internos, procedimentos ou na supervisão que permitem a execução do ato ilícito sem detecção imediata. Isso inclui a falta de segregação de funções, ausência de rotação de servidores em funções sensíveis, processos complexos e a discricionariedade excessiva sem devida responsabilização.
- **Racionalização:** compreensão dos argumentos ou justificativas internas que um indivíduo pode usar para aceitar e perpetrar o ato ilícito (ex: "ninguém vai perceber", "todos fazem", "é para o bem do órgão", "eu mereço").

A aplicação do Triângulo da Fraude visa compreender não apenas onde, mas *por que* e *como* a fraude e a corrupção podem se manifestar. Isso envolve:

- **Análise de Processos Críticos:** identificação de fluxos e atividades com maior exposição a riscos, como licitações, contratos, gestão orçamentária e financeira, fiscalização, auditoria e correição, com foco em identificar as oportunidades de desvio.
- **Avaliação de Incentivos e Oportunidades:** investigação de fatores que podem criar incentivos indevidos ou oportunidades para atos ilícitos, como a ausência de rotação de servidores em funções sensíveis e lacunas regulatórias.
- **Equipes Multidisciplinares:** a constituição de equipes de identificação de riscos com indivíduos de diversas áreas, garantindo uma visão abrangente e a consideração de como o servidor fraudador ou corrupto poderia burlar os controles existentes.
- **Fontes de Informação Diversificadas:** utilização de dados de auditorias anteriores, denúncias, processos disciplinares, análises de mercado e *benchmarking* com outras instituições, para identificar padrões e potenciais *modus operandi* e as pressões e racionalizações envolvidas.

Avaliação e Tratamento dos Riscos

Uma vez identificados os riscos inerentes, eles são avaliados quanto à **probabilidade de ocorrência e ao impacto**, utilizando matrizes de risco previstas na metodologia. Este julgamento é baseado na experiência dos gestores e no histórico de ocorrências (internas e externas), o que resulta em uma classificação ordenada dos riscos, do mais grave ao menos severo. Esta classificação orientará a priorização e a alocação de recursos para o tratamento dos riscos.

Prevenção, Detecção e Resposta

Para mitigar os riscos de fraude e corrupção, a CGM-Rio adota e aprimora controles específicos e customizados, que podem e devem ser particularizados conforme o risco oferecido pelo agente ou processo, garantindo eficiência e eficácia:

- **Política Antifraude e Anticorrupção:** instituição e manutenção de uma política clara, integrada ao Código de Ética e às regras de conduta funcional, comunicada a todos os servidores, colaboradores e fornecedores estratégicos.
- **Controles Administrativos:** implementação de segregação de funções e rodízio de servidores em atividades críticas, visando reduzir as "oportunidades" identificadas.
- **Declaração de Conflito de Interesse:** exigência de declaração de potenciais conflitos de interesse, com monitoramento periódico e análise de possíveis incompatibilidades.
- **Análise de perfil:** realização de procedimentos de *background check* (sindicância de vida pregressa) para elucidar possíveis conflitos e históricos dos profissionais ligados às atividades estratégicas.
- **Capacitação Contínua:** programas de treinamento obrigatório para servidores, colaboradores e fornecedores estratégicos em temas de integridade, ética e combate à fraude, com foco em exemplos práticos e dilemas éticos, visando fortalecer a cultura e combater as "racionalizações".
- **Cultura da Integridade:** estímulo à valorização da liderança ética de toda a organização, promovendo um ambiente onde a integridade é valorizada e recompensada.
- **Canais de Denúncia:** manutenção de canais de denúncia independentes, acessíveis, seguros e com gestão sistemática da admissibilidade, encaminhamento e resposta, garantindo proteção ao denunciante. As manifestações registradas por meio do canal 1746 devem ser devidamente encaminhadas às instâncias competentes para apuração.

- **Auditorias e Monitoramento Proativo:** realização de auditorias focadas em riscos de fraude e corrupção com análises de dados e uso de técnicas de monitoramento proativo, como inteligência artificial e cruzamento de informações para identificar padrões anômalos e indicadores de alerta, atuando sobre as "oportunidades" e as consequências das "pressões".

Comunicação e Monitoramento

Implantação de sistema contínuo de acompanhamento da eficácia dos controles e das ações implementadas para prevenção à fraude, com indicadores e relatórios periódicos. Principais instrumentos:

- **Pontos Focais de Integridade:** designação de um ponto focal responsável pelo monitoramento contínuo de riscos de integridade e pelas demais demandas relacionadas a essa temática, trabalhando em parceria com a CCI.
- **Reporte Periódico:** apresentação regular de relatórios de monitoramento ao Comitê de Integridade (CONINT) e à Alta Direção, detalhando o status da gestão de riscos, a eficácia dos controles e a ocorrência de incidentes de integridade.
- **Avaliação de Eficácia:** avaliação periódica da efetividade das medidas implementadas, contemplando o número de riscos de fraude e corrupção identificados e tratados, o quantitativo de treinamentos realizados, as denúncias recebidas e tratadas, a reincidência de casos semelhantes e a eficácia dos planos corretivos.
- **Planos de Resposta a Incidentes:** implementação de protocolos claros de investigação e apuração, com atuação coordenada entre as áreas de auditoria, corregedoria e ouvidoria para assegurar a celeridade. Após cada ocorrência, serão adotados planos de ação corretiva, com revisão de controles internos e promoção de ajustes normativos e procedimentais.
- **Comunicação Transparente:** divulgação, de forma transparente e pedagógica, dos resultados de treinamentos, auditorias, investigações concluídas e medidas corretivas, incluindo em seus relatórios anuais uma seção específica dedicada à gestão de riscos de fraude e corrupção, respeitando o caráter sigiloso das informações que assim o exigirem.

Considerações Finais

Instituir uma metodologia de gestão de riscos em um órgão de controle nos remete de antemão a uma dubiedade. Isso porque, ao mesmo tempo em que parece uma prática moderna, recente e atual de monitoramento e identificação de vulnerabilidades, do ponto de vista da existência de controles internos, a gestão de riscos já é uma prática inerente ao cotidiano das controladorias desde sempre.

A metodologia de gerenciamento de riscos apresentada neste manual foi estruturada de forma simples e direta para facilitar a implementação dos componentes do COSO ERM (ambiente interno e fixação de objetivos, identificação dos eventos de riscos, análise e avaliação de riscos e controles, informações, comunicações e monitoramento) na CGM-Rio. Nesta segunda revisão, a política passou a destacar ainda mais a necessidade de um enfoque específico para o tratamento dos riscos relacionados a integridade e fraude, demonstrando assim o compromisso desta Controladoria com o combate a quaisquer práticas que possam ensejar indícios de desvios ou irregularidades.

Com o produto deste trabalho esperamos contribuir para a implementação gradual de uma cultura sistematizada de aferição e acompanhamento dos eventos identificando, tratando e monitorando os principais riscos fora do controle do órgão, de modo a proporcionar a evolução sustentável do grau de maturidade da organização e assim atingir seu propósito de agregar valor para uma tomada de decisão responsável dos gestores e baseada em controles internos eficientes.

Sendo assim, faz-se necessário analisar criticamente de forma periódica se a política, o plano e a estrutura da metodologia de gerenciamento de riscos ainda são adequados, de modo a garantir a sua eficácia no longo prazo dado o contexto externo e interno da CGM-Rio.

O foco é, e sempre será, melhorar a eficiência, a eficácia e a efetividade do controle interno municipal, afinal a CGM-Rio tem muito clara a sua missão que é a de promover e fortalecer o sistema de controle interno na PCRJ para a efetividade da Gestão Municipal.

Resumo

Etapa 1. Estabelecimento do contexto e fixação dos objetivos

Preparação para mapeamento e identificação dos riscos

- Análise -SWOT (pontos fortes, pontos fracos, oportunidades e ameaças estratégicos)

- Ambiente de acordo com análise conjugada da SWOT:

- Alavancagem - 4
- Restrições - 3
- Vulnerabilidade – 2
- Problema - 1

1.1 Definição do grau de maturidade no Gerenciamento de Riscos

- Básico - 1
- Intermediário - 2
- Avançado - 3

1.2 Definição do apetite ao risco

- Moderado - 12
- Baixo - 8 e 9
- Muito baixo - 4 e 6
- Extremamente baixo - 1 a 3

Etapa 2. Mapeamento de Processos

2.1 Planejamento
2.1.1Levantamento dos processos-chave
2.1.2 Definição das funções associadas ao mapeamento
2.2 Mapeamento
2.3 Validação

Etapa 3 – Identificação, análise e avaliação dos Riscos e controles

3.1Como identificar e analisar os riscos?

3.2 Dimensões dos Riscos

- Operacional
- Imagem
- Conformidade
- Orçamentário
- Integridade

3.3 Apuração do Risco Inerente

RI = FR X IR

3.4 Identificação e avaliação dos controles internos

3.4.1 Classificação dos controles internos

- Quanto ao tipo: preventivo e corretivo
- Quanto à natureza: manual, automatizado e híbrido
- Quanto à relação com o risco: diretos e indiretos
- Quanto ao controle compensatório

3.4.2 Requisitos para manutenção/implementação de controles internos

- Ser eficaz
- Ser proporcional
- Ter custo x benefício adequado
- Estar de acordo com o apetite a riscos

3.5 Apuração do risco residual
RR = RI X FAC

Etapa 4 – Tratamento dos riscos

Possíveis respostas ao risco:

- Evitar
- Compartilhar
- Eliminar
- Potencializar
- Reduzir
- Aceitar

4.1 Formulário de riscos do processo/projeto

- Formulário para preenchimento dos riscos e controles associados ao processo-chave/projeto.

Etapa 5 – Monitoramento dos riscos

- Monitorar Fatores e Eventos
- Monitorar Controles
- Monitorar Indicadores

Referências Bibliográficas

Manual de Gestão de Riscos do TCU. Brasília: TCU, 2018. Disponível em: <https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/>. Acesso em: novembro, 2025.

Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. Brasília: MP, 2017. Disponível em: <https://www.gov.br/economia/pt-br/centrais-de-conteudo/publicacoes/planejamento/controle-interno/manual_de_girc___versao_2_0.pdf>. Acesso em: novembro, 2025.

Resolução Administrativa no 60 de 15 de julho de 2014 - Dispõe sobre a política de gestão de riscos da Agência Nacional de Saúde Suplementar - ANS. Disponível em: <https://www.gov.br/ans/pt-br/arquivos/acesso-a-informacao/transparencia-institucional/gestao-de-riscos/cartilha-gestao-de-riscos.pdf>. Acesso em: novembro, 2025.

Orientação Técnica n.o 02/2020 - Manual do Programa de Gestão de Riscos. Bahia: SEFAZ, 2020. Disponível em: <http://www. https://www.sefaz.ba.gov.br/controle-interno/gestao-de-riscos/programa-de-gestao-de-riscos/>. Acesso em: novembro, 2025.

Metodologia de Gestão de Riscos da CGU. Brasília: CGU, 2018. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf>. Acesso em: novembro de 2025.

Cartilha de Gestão de Riscos. Brasília: CNJ, 2019. Disponível em: <https://bibliotecadigital.cnj.jus.br/jspui/bitstream/123456789/218/1/Cartilha%20de%20Gest%c3%a3o%20de%20Riscos.pdf >. Acesso em: novembro de 2025.

BPM CBOK V.3.0 Guia para o Gerenciamento de Processos de Negócio. Brasil: ABPMP, 2013. Disponível em:<https://www.cnj.jus.br/wp-content/uploads/2019/09/7024d861818eb159b58d88870e93c911_d986a5c2fc3e0a7edeb000e51692606b.pdf>. Acesso em: abril de 2021.

Manual de Gestão por Processos. Sergipe: IFS, 2018. Disponível em: <https://ifs.edu.br/images/prodin/2018/E-book_Manual_de_gest%C3%A3o_por_processos_final_final_e_definitiva_02_10.pdf>. Acesso em: novembro de 2025.

PMI - PROJECT MANAGEMENT INSTITUTE. Guia PMBOK®: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos, Sexta edição, Pennsylvania: PMI, 2017. Disponível em: <https://dicasliderancagp.com.br/wp-content/uploads/2018/04/Guia-PMBOK-6%C2%AA-Edi%C3%A7%C3%A3o.pdf>. Acesso em: abril de 2021

PARA SABER NOVOS PRODUTOS, ATUALIZAÇÕES E MAIS INFORMAÇÕES, ACESSE:

website

https://controladoria.prefeitura.rio/

instagram

@cgmrio

CASO QUEIRA RECEBER DIRETAMENTE AS DIVULGAÇÕES NO SEU E-MAIL, ENCAMINHE SUA SOLICITAÇÃO PARA:

e-mail

controlesenormas.cgm@prefeitura.rio

COLABORE NA MELHORIA NOS NOSSOS PRODUTOS RESPONDENDO AO FORMULÁRIO ON-LINE A SEGUIR:

forms

https://forms.gle/Q7zeATJpgT218ueAA

Rio PREFEITURA | CONTROLADORIA GERAL DO MUNICÍPIO