GESTÃO DE RISCOS

Controladoria-Geral do Município

2019

PREFEITURA
BELO HORIZONTE

CONTROLADORIA | PREFEITURA BELO HORIZONTE
GOVERNANDO PARA QUEM PRECISA

Av. Álvares Cabral, 200 - 9º Andar
Centro – Belo Horizonte – MG

Controlador-Geral do Município

- Leonardo de Araújo Ferraz

Controladora-Geral Adjunta do Município
Subcontroladora de Transparência e Prevenção da Corrupção

- Cláudia Costa de Araújo Fusco

Diretora de Integridade, Prevenção e Combate à Corrupção

- Renata Kelly Cardoso de Rezende

Comitê de Integridade

- Aline Mendes Cerqueira
- Ana Luiza Figueiredo Pesce e Silva
- Ana Paula de Almeida Castro
- Fernanda de Lacerda Costa
- Gisele Leite Lima
- Karlla Moreira Carvalho
- Manoel Tolentino Oliveira
- Márcia Cristina Garcia Pessoa
- Marcus Vinícius Araújo Murad
- Maurício Dias Batista Filho

Belo Horizonte, outubro de 2019

HISTÓRICO DE REVISÕES

Versão	Data	Descrição
1.0.0	08/07/2019	■ Criação do documento

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

GLOSSÁRIO

Termo	Descrição
5W2H	Acrônimo de What, Where, Who, When, Why, How e How much (o que, onde, quem, quando, por que, como e quanto).
ABNT ISO 31000/2018	Associação Brasileira de Normas Técnicas – *International Organization for Standardization*
BPM CBOK	*Business Process Management Common Book of Knowledge*
BPMN	*Business Process Model and Notation*
CGU	Controladoria Geral da União
COSO ERM	*Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*
DAAP	Diretoria de Auditoria de Atos de Pessoal

DACI	Diretoria de Auditoria de Controle Interno
DACO	Diretoria de Atividades Correcionais
DALC	Diretoria de Auditoria de Licitações, Contratos e Instrumentos Congêneres
DASE	Diretoria de Auditoria de Obras e Serviços de Engenharia
Dashboard	Painel de controle que reúne informações consolidadas como indicadores, índices etc.
DATI	Diretoria de Auditoria de Tecnologia da Informação
DICC	Diretoria de Integridade, Prevenção e Combate à Corrupção
DITR	Diretoria de Transparência
DOUV	Diretoria de Ouvidoria
DNCP	Diretoria Normativa de Convênios, Parcerias e Congêneres
DPGF-CTGM	Diretoria de Planejamento, Gestão e Finanças - Controladoria-Geral do Município
DSEC	Diretoria da Secretaria de Correição
Framework	Estrutura ou plataforma para desenvolvimento de uma metodologia ou método
GAB-CTGM	Gabinete da Controladoria-Geral do Município
GAOUV	Gerência de Atividades Operacionais de Ouvidoria
GASEC	Gerência de Apoio à Secretaria de Correição
GDESE	Gerência de Defesa do Servidor
GECAP	Gerência de Comunicação dos Atos Processuais
GEDIS	Gerência Disciplinar
GESAU	Gerência da Secretaria de Auditoria
GR-CTGM	Gestão de Riscos da Controladoria-Geral do Município
GRCEX	Gerência de Relação com o Controle Externo
GUT	Acrônimo de Gravidade, Urgência e Tendência
IMA	*Institute of Management Accountants*
Input	Entrada do processo
ITIL	Information Technology Infrastructure Library
LOA	Lei Orçamentária Anual
MASP	Método de Análise e Solução de Problemas
PAD	Processo Administrativo Disciplinar
PBH	Prefeitura de Belo Horizonte
PDCA	*Plain-Do-Check-Act* (Planejar, Executar, Avaliar e Ajustar)
PFIP/BH	Programa de Fomento à Integridade Pública e à Gestão de Riscos da Prefeitura de Belo Horizonte
PPAG	Plano Plurianual de Ação Governamental
Output	Saída do processo
PMBOK	*Project Management Body of Knowledge*
RH	Recursos Humanos
SIPOC	Abreviação de Suplier (fornecedor), Input (entradas), Process (descrição do processo), Output (saída), Customers/Clients (clientes)
Stakeholder (parte interessada)	Todos os indivíduos que tem interesse ou participam da gestão de riscos.
SUAUDI	Subcontroladoria de Auditoria
SUCOR	Subcontroladoria de Correição
SUOUVI	Subcontroladoria de Ouvidoria
SUTRANSP	Subcontroladoria de Transparência e Prevenção da Corrupção
SWOT	*Strengts*/Forças; *Weakness*/Fraquezas; *Opportunities*/Oportunidades, *Threats*/Ameaças
TCU	Tribunal de Contas da União

Apresentação

É com muita satisfação que me dirijo a todos os servidores da CTGM para apresentar a versão final – decerto não a última - da nossa metodologia de Gestão de Riscos. Digo nossa, propositalmente, por que em estrita consonância com as melhores práticas internacionais (COSO, ISO, PMBOK) e nacionais, conseguimos de forma participativa e customizada, entregar uma poderosa ferramenta de trabalho que possibilitará, de forma estruturada e metodológica, o necessário processo de (auto)conhecimento e posterior mitigação daqueles eventos que podem impactar os resultados que são esperados deste órgão de controle, em especial nesta (pós)modernidade de transformações cada vez mais agudas e céleres.

Nesse cenário desafiador, é fundamental que consigamos, de forma estruturada como propõe a metodologia, fortalecer e (re)posicionar nosso órgão como aquele que outorga segurança ao gestor em seus processos de tomada de decisão e agrega valor à gestão, sempre com foco no melhor atendimento das demandas da sociedade.

Assim, se de um lado esta realidade sem volta nos imputa o dever de redobrar nossos esforços para avançar cada vez mais na direção da excelência do controle, de outro evidencia um giro qualitativo na atuação da CTGM, na medida em que espelha um incremento da nossa maturidade organizacional, ao exigir uma atuação concertada e coordenada, a partir da exata compreensão e delimitação dos nossos objetivos e entregas, concatenando os níveis de planejamento, execução e monitoramento.

Parabéns a todos os envolvidos e mãos à obra.

Leonardo de Araújo Ferraz

Controlador-Geral do Município

Introdução

Uma premissa da gestão de riscos é que toda organização, seja ela com ou sem fins lucrativos ou órgão de governo, existe para gerar valor para seus usuários e para a sociedade. As organizações enfrentam incertezas, e o desafio da administração é avaliar o nível de riscos que ela está preparada para enfrentar, na medida em que se empenha para aumentar o valor gerado. As incertezas geram ameaças e oportunidades com potencial para reduzir ou aumentar a qualidade dos resultados das organizações. A gestão de riscos possibilita aos administradores tratar com eficácia essas incertezas de forma a aprimorar a capacidade de geração de valor à sociedade (COSO ERM).

Gerir e gerenciar riscos de maneira estruturada e institucionalizada reflete o compromisso da Controladoria com a administração responsável dos recursos, dos seus servidores e demais partes interessadas, além de buscar estar alinhada à Administração Pública contemporânea, voltada para qualidade dos serviços providos aos cidadãos.

A plataforma de governança adotada pela CTGM conta com os seguintes instrumentos relacionados à sua gestão de riscos:

- **Decreto Municipal 16.738/2017** – Dispõe sobre a organização da Controladoria Geral do Município.
- **Portaria CTGM-019/2017** - Institui o Programa de Integridade e os Comitês de Gestão Estratégica e de Integridade da Controladoria-Geral do Município de Belo Horizonte.
- **Portaria CTGM-013/2018** - Dispõe sobre a Política de Gestão de Riscos da Controladoria-Geral do Município de Belo Horizonte e dá outras providências.
- **Portaria CTGM-004/2019** - Institui o Programa de Fomento à Integridade Pública e à Gestão de Riscos – PFIP/BH – da Controladoria Geral do Município de Belo Horizonte, para órgãos e entidades do Poder Executivo Municipal.

Sabemos que a gestão de riscos é um processo evolutivo e a CTGM, nesse começo de implementação, encontra-se em estágio incipiente. Contudo, a partir dos conhecimentos, experiências e apoio da alta administração, buscaremos condições para progredir nos níveis de maturidade em gestão de riscos e proveremos um instrumento eficaz à governança municipal e ao processo de tomada de decisão.

Este documento está dividido em duas seções principais: **Gestão de Riscos na CTGM** e **Informações Complementares**. Optamos por abordar a metodologia de gestão de riscos da Controladoria na primeira seção para maior objetividade do material; e os temas relevantes, porém de caráter genérico e informativo, foram organizados na seção seguinte, para nivelamentos conceituais. Há, também, um capítulo para **referências bibliográficas** e outro para os **anexos**.

Gestão de Riscos na CTGM

Organizações de todos os tipos e tamanhos enfrentam influências de fatores externos e internos que tornam incerto se elas alcançarão seus objetivos (ISO 31000). Conhecer essas ameaças e também as vulnerabilidades que as permeiam aumentam as possibilidades de alcançarem os seus propósitos.

Objetivos

A Gestão de Riscos da Controladoria-Geral do Município (GR-CTGM) tem o objetivo principal de **prover apoio à tomada de decisões**. Outras expectativas relevantes, são:

- Aumentar as possibilidades de alcance de objetivos.
- Melhorar a comunicação organizacional e acompanhamento dos trabalhos.
- Criar a mentalidade e cultura de riscos.
- Aperfeiçoar os mecanismos de controle interno.
- Proteger o ambiente interno, o patrimônio e as informações.
- Disseminar a melhoria de gestão nas demais unidades organizacionais da PBH.
- Favorecer a transparência e prestação de contas à sociedade.

A GR-CTGM não tem como finalidade identificar e tratar todos os riscos que possam existir na Controladoria, pois elencá-los e gerenciá-los seria muito custoso, senão impossível. Ao invés disso, presta-se a fornecer um arcabouço de conhecimentos e procedimentos que possa contribuir para melhor administração das incertezas significativas que permeiam o órgão.

Abaixo, são exibidos alguns atributos referentes à GR-CTGM.

O QUE É	O QUE NÃO É
■ Aplicado aos objetivos da organização.	■ Um método para eliminar todos os riscos da organização.
■ Apoia a tomada de decisões.	■ Lista "interminável" de riscos.
■ Aplicado em toda organização.	■ Uma garantia de que a organização evitará perdas.
■ Propicia garantia razoável da informação.	■ Um emaranhado de práticas confusas.
■ Sob medida.	■ Copiado de outras organizações.
■ Induz a cultura de riscos em todos os níveis da organização.	

Figura 1 – Atributos da Gestão de Riscos

Apesar de poderem adotar as mesmas referências metodológicas, cada organização deve elaborar seu planejamento e providenciar a sua implementação da gestão de riscos. Isso porque

os objetivos e o contexto de cada uma delas são diferentes, o que demanda uma estrutura própria (sob demanda), adequada à sua natureza funcional, aos recursos disponíveis e à maturidade em gerenciamento de riscos.

Princípios e diretrizes

Os princípios e diretrizes representam os direcionamentos que visam preparar o ambiente e ampliar as viabilidades para implementação da GR-CTGM.

- **Orientada a objetivos** - Sem objetivos claros é impossível identificar eventos que possam gerar riscos os quais possam comprometer uma determinada estratégia ou finalidade da organização (IMA, 2018). Conforme a própria definição de risco: "*efeito da incerteza nos objetivos*", há de se identificar ou estabelecer os objetivos da organização antes de realizar o gerenciamento ou gestão dos seus riscos.
- **Comprometimento da alta administração** – O estímulo, a liderança e o apoio da alta administração deverão estar presentes na gestão de riscos, uma vez que o bom exemplo para a cultura de riscos e demais aspectos da governança corporativa devem vir de cima (*tone at the top*). A alta administração deve também assegurar que os recursos necessários sejam alocados para gerenciar riscos e também atribuir autoridades, responsabilidades e responsabilizações nos níveis apropriados dentro da organização (ISO 31000).
- **Cultura de risco** – Todos os níveis da organização devem estar conscientes e mobilizados a identificar, reportar e tratar os riscos corporativos; desde gestores, servidores, terceirizados, estagiários e todas as demais partes interessadas que, de forma direta ou indireta, estejam envolvidas na prestação de serviços. Isso porque os riscos podem estar presentes em quaisquer pontos da cadeia operacional ou administrativa e eles devem ser observados e oportunamente gerenciados.
- **Objetividade e fidelidade** – A identificação e tratamento dos riscos devem ser realizados de maneira objetiva e assertiva. Eles não devem ser omitidos ou abreviados intencionalmente, apesar do senso comum poder julgá-los como algo depreciativo e indesejado. Os riscos são fatores intrínsecos de qualquer atividade e devem ser conhecidos e gerenciados de forma pragmática.
- **Melhoria contínua** – Baseado no modelo **PDCA (*Plain-Do-Check-Act*)**, a melhoria contínua preza pela evolução constante da gestão de riscos. As organizações que desejam implementar a sua gestão de riscos devem iniciar com as informações e conhecimentos disponíveis e, a partir dos erros, acertos, aprendizagens e experiências adquiridas ao longo do tempo, aprimorá-la continuamente. Em outras palavras, a melhoria contínua postula que, ao invés de aguardar por "condições perfeitas", a gestão de riscos deve iniciar com os recursos e experiências disponíveis e evoluir o modelo gradativamente a partir dos conhecimentos adquiridos com a implementação e capacitações.

Escopos dos riscos

Para melhor planejamento da GR-CTGM, são definidos os seguintes escopos de riscos que orientarão a implementação dos trabalhos: estratégico, tático, operacional e ambiental.

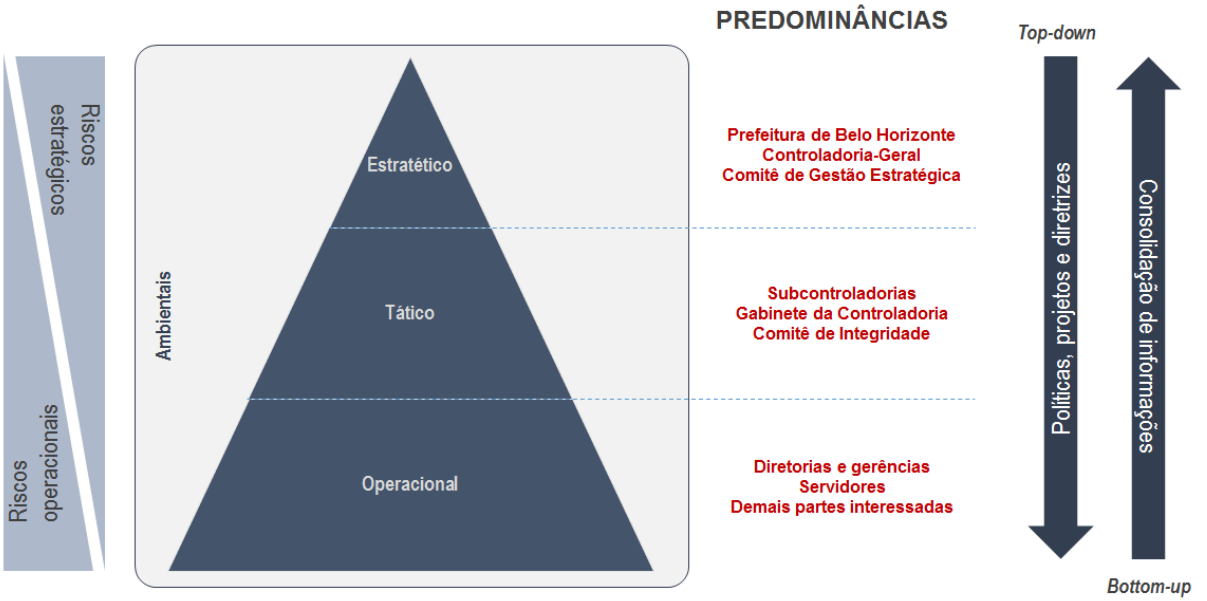


Figura 2 - Escopos dos riscos (BCB, 2017. Adaptado)

O **nível estratégico** concentra as decisões e orientações da alta administração da CTGM e é formado pela Prefeitura de Belo Horizonte, Controladoria-Geral e Comitê de Gestão Estratégica. Aqui estão concentradas as atividades de definição de políticas, normas e metas estratégicas; projetos e ações que sustentarão o planejamento estratégico; questões financeiras e orçamentárias; definição e acompanhamento do Programa de Integridade; imagem e reputação do órgão e provimento de recursos necessários à gestão de riscos.

O **nível tático** articula e coordena as atividades das unidades setoriais da Controladoria (Subcontroladorias e Gabinete) para o atingimento dos objetivos definidos pelo nível estratégico. As unidades devem entregar produtos e serviços especializados conforme a sua área temática (ouvidoria, auditoria, corregedoria, transparência e combate à corrupção). A **cadeia de valor** é uma ferramenta que auxilia no entendimento dos ambientes interno e externo de cada uma dessas unidades, seus clientes e os principais processos que dão suporte ou fornecem diretamente seus produtos e serviços. Esse nível atém-se, principalmente, à definição de diretrizes para o nível operacional e critérios relacionados à eficácia, efetividade e qualidade das entregas.

O **nível operacional** é voltado à execução das atividades dos processos organizacionais diante as diretrizes estabelecidas pelos níveis anteriores. O foco está na capacidade de realização dos trabalhos e no cumprimento dos planejamentos e dos critérios previamente definidos. O fluxo operacional deve ser constantemente analisado pelas gerências e diretorias buscando reduzir possíveis gargalos, ambiguidades e inseguranças que possam afetar a qualidade dos processos e resultados. Nesse nível, a atenção é voltada para a eficiência, economicidade, planejamento e agenda dos trabalhos, fluidez das atividades, qualidade da comunicação, alocação de recursos etc.

Por fim, o **escopo do ambiente** refere-se às questões de interesse comum da Controladoria ou assuntos não tratados de maneira específica pelos níveis anteriores, como, por exemplo, segurança das instalações (elétrica, hidráulica etc.), segurança física e da informação (confidencialidade, *backups*, acessos a sistemas e bancos de dados, acessos às dependências físicas etc.), infraestrutura (tecnologia e equipamentos, disponibilidade de materiais de trabalho etc.), dentre outros.

Estrutura da Gestão de Riscos na CTGM

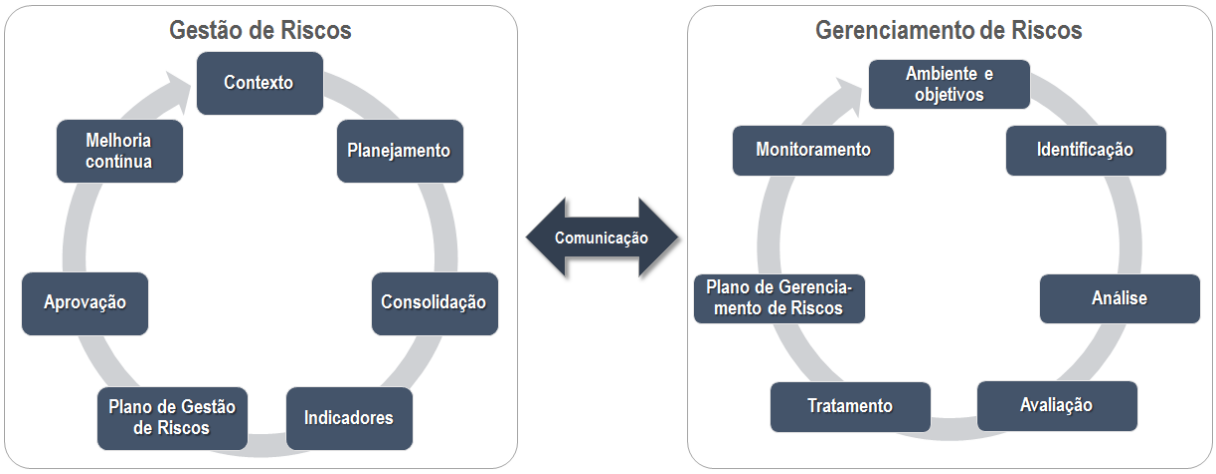


Figura 3 - Estrutura da GR-CTGM

A estrutura, ou *framework*, da gestão de riscos da CTGM é formada por dois núcleos de controle: **Gestão e Gerenciamento de Riscos**. Eles são conectados por canais de comunicação e trocas de informações que ocorrem constantemente entre os núcleos para orientações, alinhamentos, análises e consolidações de dados.

O núcleo de **Gestão de Riscos**[1] é representado pelo Comitê de Integridade e desenvolve atividades relacionadas à metodologia da GR-CTGM, planejamento, coordenação e integração dos núcleos de gerenciamento de riscos; além da divulgação de informações às partes interessadas.

O núcleo de **Gerenciamento de Riscos** refere-se às atividades de administração direta de riscos em cada unidade setorial da Controladoria. Ou seja, para cada Subcontroladoria e para o Gabinete, haverá um gerenciamento de risco próprio, porém condizente com a metodologia, o planejamento e os padrões acordados no núcleo de gestão de riscos.

A gestão de riscos não é um processo rigorosamente em série, pelo qual uma etapa afeta apenas a seguinte; é um processo multidirecional e interativo, segundo o qual quase todos os componentes podem e realmente influenciam os demais (COSO ERM).

A comunicação retrata a troca de informações entre os núcleos e entre esses e todas as partes interessadas envolvidas no processo, sendo ela fator preponderante para a condução dos trabalhos da gestão e do gerenciamento de riscos. A figura abaixo apresenta o fluxo principal de atividades e comunicação entre os núcleos.

[1] O termo "Gestão de Riscos" têm duas conotações na Controladoria. Ele pode abranger todo o conjunto de iniciativas e atividades para a administração de riscos na CTGM (sentido amplo) – sendo chamada de GR-CTGM; ou então, se referir a um dos núcleos de controle de riscos (sentido estrito). Nessa seção, estamos referindo ao sentido estrito, ou como sendo um dos núcleos de administração de riscos.

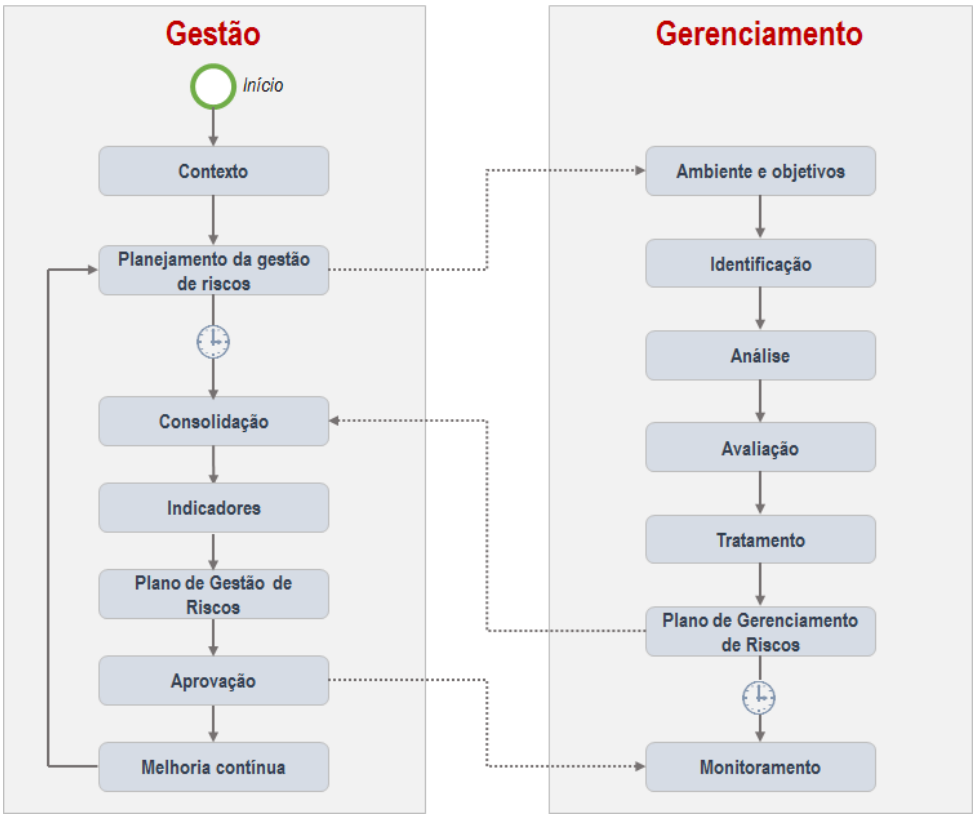


Figura 4 - Fluxo entre os núcleos de gestão e gerenciamento

Núcleo de gestão de riscos

O núcleo de gestão de riscos é formado pelas seguintes etapas:

- Contexto
- Planejamento
- Consolidação
- Indicadores
- Plano de Gestão de Riscos
- Aprovação
- Melhoria Contínua

Contexto

Antes de dar início ao processo de gestão de riscos, é necessário conhecer os aspectos do ambiente organizacional da Controladoria que possam influenciar a maneira como a metodologia de gestão e gerenciamento de riscos serão estruturadas no órgão. Essa etapa avalia a maturidade em gestão de riscos[2] bem como os ambientes interno e externo (forças, fraquezas, oportunidades e ameaças) de forma que esses exames preliminares possam auxiliar no "desenho" que a gestão de risco da CTGM terá.

[2] A maturidade em gestão de riscos é o "grau de adoção e aplicação, por parte da direção, de uma abordagem de gestão de riscos robusta, conforme planejada, em toda a organização, a fim de identificar, avaliar, decidir sobre respostas e relatar oportunidades e ameaças que afetam a consecução dos objetivos da organização" (QSP, 2012). Os modelos de maturidade em gestão de riscos geralmente apresentam uma escala de referência que representa o nível de maturidade da unidade, como, por exemplo: Ingênuo, Consciente, Definido, Gerenciado e Habilitado. A gestão de riscos deverá propiciar à organização a evolução na escala de maturidade ao passo que a experiência é adquirida e os instrumentos de controle são aplicados.

Convém que o contexto da gestão de riscos seja estabelecido a partir da compreensão dos ambientes externo e interno no qual a organização opera, e convém que reflita o ambiente específico da atividade ao qual o processo de gestão de risco é aplicado (ISO 31000).

O contexto pode ser avaliado mediante a aplicação da **Matriz SWOT** junto às partes interessadas da organização. A matriz tem o propósito de evidenciar as forças e fraquezas percebidas pelos entrevistados (contexto interno), bem como as oportunidades e ameaças (contexto externo).

Planejamento

Na etapa de planejamento são definidos os procedimentos, os padrões e os controles a serem adotados na gestão de riscos da CTGM, incluindo a metodologia, os ciclos de implementação e os cronogramas de trabalho.

Após a elaboração do planejamento, a Controladoria pode dar início às atividades do núcleo de gerenciamento de riscos em cada uma de suas unidades setoriais. Neste ponto, a gestão de riscos deve aguardar a conclusão dos Planos de Gerenciamento de Riscos das unidades para, a partir daí, dar início à próxima etapa: Consolidação.

Consolidação

A consolidação consiste na integração das informações presentes em cada Plano de Gerenciamento de Riscos. Os dados presentes nos Planos devem estar dispostos de maneira padronizada para possibilitar o agrupamento de informações oriundas de cada unidade setorial da Controladoria.

Indicadores

Indicador de desempenho é um número, percentagem ou razão que mede um quesito de desempenho, com o objetivo de comparar esta medida com metas preestabelecidas (TCU, 2004).

Os indicadores de desempenho retratam a situação atual da gestão de riscos da CTGM e de suas unidades setoriais, bem como suas evoluções ao longo do tempo para avaliação dos efeitos do tratamento dos riscos.

A apresentação dos indicadores poderá ser em um painel de controle sintético e com recursos gráficos (*dashboard*) para rápida interpretação das informações pelas partes interessadas.

Plano de Gestão de Riscos

Ao final de cada ciclo da GR-CTGM, deverá ser elaborada uma versão do Plano de Gestão de Riscos da Controladoria, contendo os dados consolidados dos Planos de Gerenciamento de Riscos de cada ciclo desenvolvidos pelas unidades setoriais, bem como os indicadores de desempenho, que representarão a situação das unidades e os efeitos da gestão de riscos no ambiente interno da CTGM.

O Plano de Gestão de Riscos visa: a) comunicar as atividades e resultados da gestão de riscos às partes interessadas; b) fornecer informações para a tomada de decisão; c) melhorar os procedimentos das atividades de gestão de riscos e d) auxiliar a interação dos envolvidos e responsáveis pela gestão ou gerenciamento de riscos (ISO 31000).

O Plano de Gestão de Riscos da CTGM deve conter:

- Painel de controle (*dashboard*)
- Riscos abaixo (região verde) e acima (região vermelha) da tolerância e riscos sob análise crítica (região amarela)
- Estratificação de riscos por tipo de tratamento
- Análise da evolução de riscos
- Anexo com os Planos de Gerenciamento de Riscos das unidades setoriais.

O Plano de Gestão de Riscos é parte integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a alta administração e os órgãos de supervisão a cumprirem suas responsabilidades (ISO 31000).

Aprovação

O Plano de Gestão de Riscos é encaminhado ao Comitê de Gestão Estratégica para avaliação e aprovação dos planos de ação. Os tratamentos de riscos devem ter sido previamente sugeridos pelas unidades setoriais em seus respectivos planos de gerenciamento. Eles devem conter os procedimentos a serem realizados, responsáveis, prazos, custos e resultados esperados.

Após a aprovação, as unidades setoriais são comunicadas para início da execução e monitoramento das ações deferidas pelo Comitê de Gestão Estratégica.

Melhoria Contínua

A melhoria contínua é uma iniciativa que promove os meios para registrar propostas de aperfeiçoamentos na metodologia ou nos procedimentos da gestão de riscos. Essas propostas são avaliadas pelo Comitê de Integridade e podem ser incorporadas nos planejamentos dos ciclos seguintes.

As sugestões podem ser decorrentes de novos conhecimentos e capacitações nos temas relacionados ao gerenciamento de riscos, bem como percepções de aperfeiçoamento advindas das partes interessadas.

A cada ciclo, a GR-CTGM aplicará avaliações de maturidade em gestão de riscos e do ambiente de controle - as avaliações de maturidade e ambiente fazem parte da etapa “ambiente e objetivos”, abordado adiante no núcleo de gerenciamento de riscos. Essas avaliações funcionarão como **linhas de base** para acompanhamento dos efeitos e do progresso da gestão de riscos na Controladoria.

Gerenciar riscos é um processo iterativo (cíclico) e auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas. A gestão de

riscos é melhorada continuamente por meio de aprendizado e experiências (ISO 31000).

Núcleo de gerenciamento de riscos

Neste tópico serão abordadas as seguintes etapas do gerenciamento de riscos a serem aplicadas por cada unidade setorial da Controladoria:

- Ambiente e objetivos
- Identificação de riscos
- Análise
- Avaliação
- Tratamento
- Plano de Gerenciamento de Riscos
- Monitoramento

Ambiente e objetivos

A análise do ambiente e levantamento de objetivos busca organizar as informações preliminares das unidades setoriais da CTGM para que possam servir de referência para o início de um novo ciclo de gerenciamento de riscos.

Avaliação do ambiente

A **avaliação do ambiente** deverá fornecer as características principais da unidade e também qualificar as opiniões dos respectivos gestores sobre o quão estão preparados para gerenciar riscos, além do grau de conformidade às principais normas e do alinhamento às metas estratégicas da Prefeitura e da própria CTGM.

Essas informações serão úteis para, após aplicados os planos de ação para tratamento de riscos, avaliar os seus efeitos nos processos organizacionais e nas unidades setoriais da CTGM. Elas funcionarão como linhas de base ou indicadores qualitativos, que serão alimentados mediante aplicação de questionários aos gestores de cada unidade com os seguintes pontos de indagação:

- **Sistema de controle interno** - Opinião sobre o ambiente de controle de riscos da unidade.
- **Conformidade normativa** - Opinião sobre a conformidade às principais normas que regem as competências da unidade[3].
- **Alinhamento estratégico** - Opinião sobre o atingimento das metas estratégicas das unidades[4].

Levantamento de objetivos

Objetivos podem possuir diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis na organização (ISO 31000). Assim, podemos definir os objetivos sob várias perspectivas: podem ser objetivos que almejam alcançar situações ainda inexistentes (progressivos),

[3] Na CTGM, foram utilizadas as competências definidas no Decreto Municipal 16.736/17. Outras fontes devem ser consideradas para compor a relação de normas das unidades setoriais (Leis, normas técnicas, diretrizes, princípios etc.).
[4] Na CTGM, foram utilizados o Plano Plurianual de Ações Governamentais (PPAG) e a Lei de Orçamento Anual (LOA).

preservar situações atuais (mantenedores) ou eliminar/reduzir situações existentes, porém indesejadas (regressivos)[5].

Para o **levantamento dos objetivos**, poderão ser consideradas diretrizes, metas estratégicas, competências legais, serviços e produtos fornecidos, bem-estar dos colaboradores, satisfação dos clientes, etc.

A GR-CTGM contará com as seguintes classes de objetivos para melhor administração dos escopos da gestão de riscos:

1. **Estratégico** – Objetivos relacionados à visão de médio e longo prazo da CTGM, especificados pela alta administração.
2. **Tático** – Objetivos relacionados às normatizações, acompanhamentos e assistências às operacionalizações setoriais.
3. **Processo** – Objetivo relacionado à execução e melhoria contínua de processos organizacionais.
4. **Projeto** – Objetivo relacionado ao planejamento, execução e implementação de um novo projeto, considerando os critérios de sucesso e restrição tripla (escopo, tempo, custo e qualidade).
5. **Ambiente** – Objetivos concernentes ao ambiente físicos do trabalho, necessários à execução das atividades - infraestrutura, segurança, tecnologia etc.

Além dos "objetivos materiais" (produtos e serviços fornecidos pelo órgão aos seus clientes), é fundamental avaliar os meios que são utilizados para prover os resultados ("objetivos formais"); ou seja, é necessário que se atente aos princípios de integridade, ética e conduta dos agentes em toda a sua atuação nos trabalhos, combatendo a máxima de que os objetivos devem ser alcançados a qualquer custo, ou que "os fins justificam os meios".

Identificação de riscos

O propósito da identificação de riscos é reconhecer e descrever incertezas e ameaças que possam impactar o alcance dos objetivos organizacionais. Na identificação de riscos devem ser consideradas informações pertinentes, apropriadas e atualizadas (ISO 31000).

Como já mencionado anteriormente, a identificação de riscos deverá ser orientada aos objetivos organizacionais e planejada de acordo com os escopos de cada ciclo de gerenciamento.

A identificação deve inicialmente priorizar aos riscos de maior relevância para que não seja gerada uma listagem excessivamente extensa, que possa poluir e/ou comprometer a eficiência do gerenciamento de riscos.

Importante ressaltar que as pessoas envolvidas na identificação de riscos devem ter conhecimento sobre as áreas da organização que estão sendo examinadas e ter dedicação para esse propósito, pois é uma atividade que demanda comunicações, reflexões e revisões frequentes.

Técnicas para identificação de riscos

Algumas técnicas que podem auxiliar o gerenciamento a identificar riscos são apresentadas abaixo, mas não se restringem a essa relação.

[5] As categorias dos objetivos indicadas (progressivo, mantenedores e regressivos) são de criação própria da GR-CTGM.

- **Brainstorming e entrevistas**. Reuniões com pessoas com experiência no ambiente e nos processos da organização para identificar situações que possam gerar impactos nos objetivos, bem como analisar eventos históricos que geraram ameaças ou mesmo que incorreram em impactos ou perdas quantitativas ou qualitativas nos resultados.
- **Análise SWOT**. Análise dos ambientes internos e externos da organização, buscando identificar riscos negativos com base nos quadrantes referentes às fraquezas e ameaças, ou riscos positivos nos quadrantes referentes às forças e oportunidades.
- **Análise de cenário ("e-se?", "*what-if*?")**. Avaliação do fluxo dos processos buscando encontrar situações de vulnerabilidades, inseguranças ou instabilidades. A análise de cenário pode ser aplicada em um nível mais superficial, ao avaliar o fluxo mentalmente, ou então utilizar mapeamentos de processos para uma inspeção mais detalhada e criteriosa.
- **Questionários de risco**. Avaliação de processos e ambientes organizacionais com base na sua verificação diante de critérios que possam comprometer a entrega e a qualidade dos produtos e serviços; ou quesitos de segurança, eficiência, eficácia etc.
- **Mudanças de ambiente**. Mudanças nos processos ou no ambiente da organização podem alterar os riscos identificados anteriormente. Caso haja variação nas configurações organizacionais, os riscos devem ser revistos conforme a influência dessas mudanças.

(IMA, 2018)

Análise de riscos

Após a identificação dos principais **riscos**, eles devem ser analisados para reconhecimento de suas **causas** e possíveis **consequências** nos objetivos organizacionais. Além disso, são avaliados graus de **probabilidade** e dos **impactos**, caso os riscos se consolidem.

As causas, os eventos de riscos e as consequências nos objetivos são denominados **componentes do risco** e eles são importantes para o exame das circunstâncias onde as ameaças estão presentes e, com isso, auxiliar na elaboração de planos de ação para seus tratamentos. Os componentes do risco representam a sequência de ocorrências que podem impactar os objetivos (causa-evento-consequência). Durante a análise de riscos é frequente se deparar com situações onde o risco já tenha se concretizado, o que o torna um **problema**. Ou seja, o problema é a efetivação do risco negativo e representa uma consequência desfavorável aos objetivos da organização.

Na análise de riscos também são estimadas as **probabilidades** e **impactos** dessas consequências, utilizando a escala Likert[6]. O produto da probabilidade com o impacto é denominado **nível do risco**.

Inicialmente, a probabilidade e o impacto devem ser estimados sem levar em conta quaisquer controles que possam reduzir os riscos. Esses seriam os **riscos inerentes** ou riscos naturais.

Em um segundo momento, os controles existentes são considerados para avaliar se eles contribuem para a redução da probabilidade ou do impacto dos riscos inerentes. Os riscos remanescentes, após os efeitos dos controles, são chamados de **riscos residuais**.

[6] A **escala Likert** define os níveis de concordância sobre uma afirmação ou incidência de uma variável. Na gestão de riscos da CTGM, será usada a versão da escala de 5 pontos. A escala deve ser adotada em qualquer proposição que se deseja obter a opinião do entrevistado em perguntas objetivas (fechadas). Assim, 1 é a extremidade referente à mínima concordância ou incidência e 5 é a extremidade de máxima concordância ou incidência. A adoção da escala permitirá a padronização de respostas e comparabilidade de informações.

Os controles também podem gerar novos riscos, ou **riscos secundários**. Eles devem ser incorporados no gerenciamento, tendo como causa o controle que o originou.

O objetivo da observação dos riscos inerentes (anteriores ao controle) dos residuais (posteriores ao controle) é avaliar a eficácia dos controles internos.

Avaliação de riscos

O propósito da etapa de avaliação de riscos é apoiar decisões sobre o posicionamento diante os riscos identificados e analisados. A avaliação de riscos envolve a comparação dos resultados da análise de riscos (etapa anterior) com os critérios de aceitação (apetite) para determinar onde é necessária ação adicional para redução dos riscos (ISO 31000).

Os riscos devem ser priorizados de acordo com os níveis de risco calculados (probabilidade x impacto) na ordem decrescente de criticidade (do maior para o menor nível).

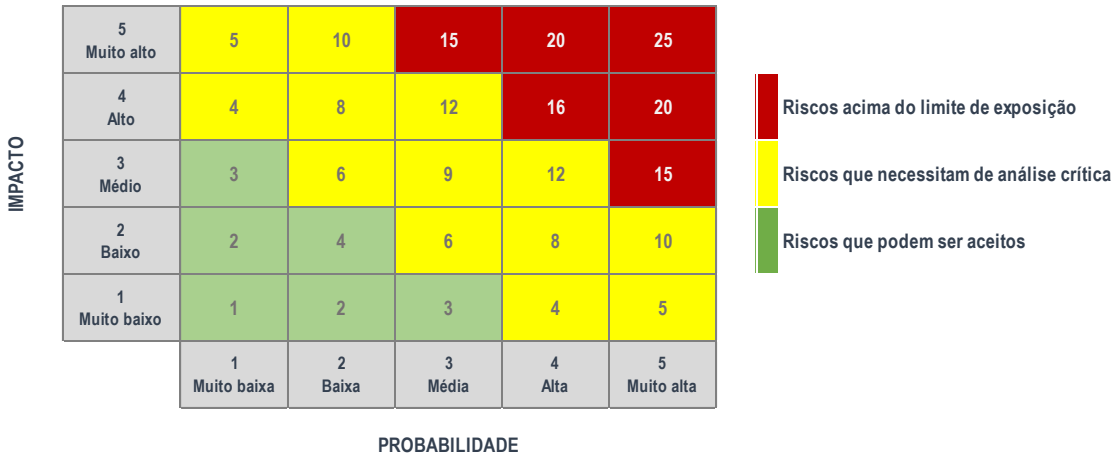


Figura 5 – Matriz de riscos (adaptado de TCU, 2018 e Orange Book, 2004)

O risco é posicionado na **matriz de riscos** de acordo com seu grau de impacto nos objetivos e a probabilidade de ocorrência. Os eixos da matriz (probabilidade x impacto) são divididos conforme a escala Likert para que sejam mensurados, avaliados e comparados.

As regiões da matriz são definidas pela organização, porém uma distribuição usual a divide em riscos acima do apetite (vermelha); riscos toleráveis, mas que demandam análise crítica (amarela) e riscos que, de antemão, são aceitáveis (verde).

Os riscos acima do apetite (região vermelha) necessitam de intervenções e tratamentos, pois podem impactar sobremaneira as operações ou a integridade da organização ou unidade.

Os riscos que necessitam de análise crítica (região amarela) devem ser continuamente monitorados, pois têm um grau considerável nos níveis de probabilidade e/ou impacto nos objetivos.

Os riscos que podem ser aceitos (região verde) devem constar na matriz e no gerenciamento de riscos, pois eles podem variar e a sua observação reduz a chance de uma "fagulha se transformar em um incêndio".

Tratamento de riscos

Com os riscos classificados e ordenados, o tratamento deverá indicar as respostas para cada um deles.

As possíveis respostas ao risco são:

- **Evitar** – O risco não será assumido pela unidade. Seja por não haver opções de tratamento adequado ou porque os benefícios não deverão compensar os possíveis danos. Para se evitar o risco, a sua fonte deverá ser eliminada; e com ela, provavelmente haverá paralisação ou descontinuação de algum procedimento operacional.
- **Aceitar** – O risco será assumido pela unidade sem qualquer tratamento para redução do impacto ou da probabilidade. Esse caso pode se dar devido à pouca relevância do risco ou por não haver alternativas para mitigação ou eliminação da sua fonte (causa).
- **Mitigar** – A mitigação ocorrerá em casos de intervenções nas probabilidades e/ou nos impactos mediante a implantação ou aprimoramento de controles internos. As medidas mitigatórias podem consumir recursos materiais, humanos e financeiros. Ao decidir por essa alternativa, deve-se levar em conta se a relação custo-benefício será vantajosa. Sempre existirá algum nível de risco residual após a mitigação e o desejável é que ele seja reduzido até um patamar aceitável.
- **Compartilhar** – O compartilhamento de risco geralmente envolve custos financeiros pois, paga-se para que entidades externas assumam o risco para a organização. Essa modalidade de tratamento ocorre, por exemplo, em contratação de seguros ou empresas terceirizadas.

O tratamento de riscos deve considerar o nível do risco diante o apetite definido. A finalidade é que ocorram tratamentos de riscos até que esse nível fique abaixo do limite aceitável[7].

Plano de Gerenciamento de Riscos

O Plano de Gerenciamento de Riscos concentra informações dos riscos relativos às unidades setoriais da CTGM.

O Plano de Gerenciamento de Riscos deverá conter:

- Relação de riscos - Código do risco; descrição; data de inclusão; escopo; objetivo impactado; níveis de risco (inerente e residual); resposta sugerida; plano de ação sugerido (cronograma), resultados esperados, prazos, custos, responsável pelas ações e situação atual do risco.
- Relação de controles internos.
- Relação de monitoramentos realizados.
- Painel de controle - Riscos abaixo (região verde) e acima (região vermelha) da tolerância e riscos sob análise crítica (região amarela); estratificação de riscos por tipo de tratamento.

[7] **Consequências do tratamento de riscos** - Do tratamento de riscos podem surgir novas situações: 1) **Não modificarem suficientemente o risco**. Nesse caso, convém que este seja registrado e mantido sob análise crítica contínua; 2) **Gerar riscos remanescentes (residuais)**. Estes devem ser documentados e submetidos a monitoramento, análise crítica e, onde apropriado, tratamento adicional e 3) **Introduzir novos riscos (secundários)**. Os novos riscos necessitam ser gerenciados, seguindo as etapas do núcleo de gerenciamento de riscos (ISO 31000).

O Plano de Gerenciamento de Riscos é submetido ao Comitê de Integridade (núcleo de gestão de riscos) para consolidação das informações das unidades setoriais. Nesse ponto, o gerenciamento de riscos nas unidades setoriais deve aguardar a avaliação e aprovação do plano de ação pelo Comitê de Gestão Estratégica. Só então, dar-se-á o início à execução das atividades de tratamento de riscos e também aos monitoramentos periódicos, conforme descrito na etapa seguinte.

Monitoramento

O monitoramento é o acompanhamento da execução do plano de ações para tratamento dos riscos. O plano de ações deve ter sido aprovado previamente pelo Comitê de Gestão Estratégica.

O monitoramento tem como objetivos:

- Avaliar periodicamente desvios em relação aos prazos, custos e procedimentos.
- Avaliar os efeitos das ações na redução de riscos negativos, ou na elevação dos riscos positivos.
- Propor melhorias à gestão de riscos na CTGM.

O monitoramento será realizado pelos núcleos de gerenciamento e acompanhado pelo Comitê de Integridade. Para isso, deverá ser usado cronograma contendo as ações de tratamento, responsáveis, unidades envolvidas, estimativas de prazos e custos.

Comunicação

Os núcleos de gestão e de gerenciamento de riscos devem estar constantemente compartilhando informações. De maneira geral, as comunicações devem se dar de maneira flexível e objetiva para que sejam acessíveis, assertivas e ágeis, propondo diálogos francos e constantes em todos os níveis da organização e reduzindo eventuais entraves decorrentes de burocracias desnecessárias ou rigidez hierárquica.

Por ser um instrumento interno de gestão, as informações levantadas e tratadas durante a gestão de riscos da CTGM terão caráter restrito. Os relatórios finais e Planos de Gestão de Riscos gerados poderão ser publicados conforme decisão da alta administração.

Espera-se que todo o pessoal receba mensagens claras da alta administração, alertando que as responsabilidades da gestão de riscos devem ser levadas a sério; do mesmo modo, presume-se que os níveis operacionais comuniquem aos demais níveis ou ao Comitê de Integridade informações de risco de maneira tempestiva e oportuna.

Cada um deve entender a sua própria função no gerenciamento de riscos, assim como as atividades individuais que se relacionam com o trabalho dos demais. As pessoas deverão ter uma forma de comunicar informações significativas dos escalões inferiores aos superiores. Deve haver, também, uma comunicação eficaz com terceiros, como clientes, fornecedores e instituições externas (COSO ERM).

As três linhas de defesa

A abordagem das Três Linhas de Defesa é um modelo simples e eficaz para definir e comunicar os papéis e as responsabilidades das partes interessadas na gestão de riscos da CTGM.

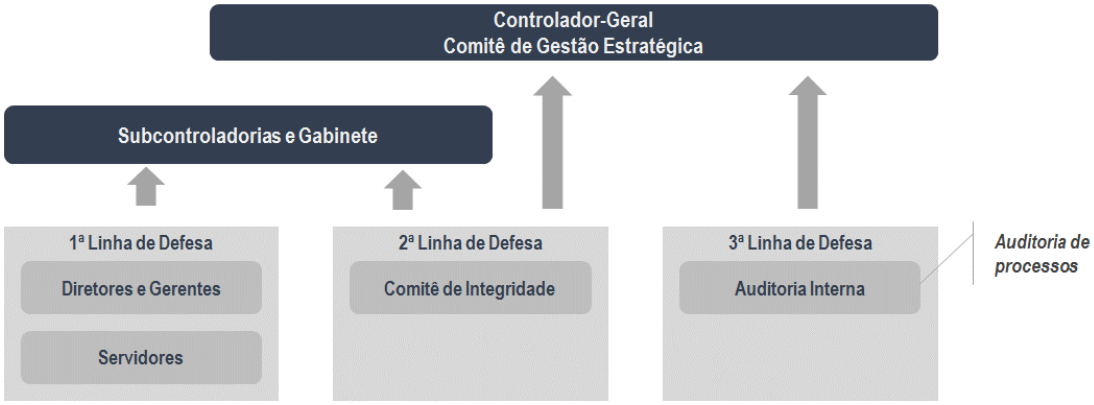


Figura 6 - Linhas de defesa na CTGM

Abaixo são apresentadas as três linhas de defesa da CTGM.

Atuação	Envolvidos	Descrição
1ª Linha de defesa	■ Diretores ■ Gerentes ■ Servidores ■ Terceirizados etc.	Funções que gerenciam e têm propriedade dos riscos operacionais. São funções que lidam diretamente com os processos, procedimentos e controles internos e, por isso, têm maior domínio sobre os riscos relacionados à execução das atividades.
2ª Linha de defesa	■ Comitê de Integridade	Funções que coordenam e supervisionam as práticas de gerenciamento de riscos da primeira linha de defesa, além de atuar como segunda instância no controle de riscos.
3ª Linha de defesa	■ Auditoria interna (auditoria de processos)	Funções de avaliação independente dos ambientes, gerenciamento de riscos e eficácia dos controles internos.

Tabela 1 - Linhas de defesa na CTGM

A auditoria de processos caracteriza-se por avaliar os controles internos, eficiência dos processos organizacionais e riscos associados, sendo, portanto, considerada um tipo de auditoria mais adequada à terceira linha de defesa na CTGM.

Apesar da alta administração (Controlador-Geral e Comitê de Gestão Estratégica) e os gestores das Subcontroladorias e do Gabinete não serem considerados nas três linhas de defesa, eles são informados constantemente sobre o gerenciamento de riscos, além de possíveis eventos atípicos relevantes. Sendo os incentivadores e patrocinadores pela implementação da gestão de riscos, o seu papel, ao invés de estar diretamente ligada às três linhas de defesa, é apoiar, zelar, intervir e dirimir questões sobre a gestão de riscos na CTGM com o propósito de manter a harmonia do ambiente e qualidade dos trabalhos.

Plano de implementação da GR-CTGM

Aqui serão abordados os planos para a implantação física da gestão de riscos na CTGM.

Núcleos de gerenciamento

A Controladoria-Geral é constituída, diretamente, pelo Gabinete, quatro Subcontroladorias, duas Diretorias e uma Gerência, sendo que as Subcontroladorias também contêm Diretorias e Gerências. Assim, foram criados cinco núcleos de gerenciamento de riscos e um núcleo de gestão de riscos para coordenação dos demais, conforme apresentado na tabela abaixo.

Núcleo de gestão	Núcleos de gerenciamento	Abrangência[8]
Alta administração Comitê de Gestão Estratégica Comitê de Integridade	GAB-CTGM	■ Gabinete do Controlador ■ DNCP ■ DPGF-CTGM ■ GRCEX
	SUAUDI	■ Subcontroladoria de Auditoria ■ DAAP ■ DATI ■ DACI ■ DASE ■ DALC ■ GESAU
	SUCOR	■ Subcontroladoria de Correição ■ DSEC ■ GECAP ■ GASEC ■ DACO ■ GEDIS-1 ■ GEDIS-2 ■ GDESE
	SUOUVI	■ Subcontroladoria de Ouvidoria ■ DOUV ■ GAOUV
	SUTRANSP	■ Subcontroladoria de Transparência ■ DITR ■ DICC

Tabela 2 - Núcleos de gerenciamento da CTGM

Ciclos de gerenciamento

A gestão de riscos da Controladoria será implantada em ciclos; sendo que cada um deles dará prioridade a um determinado escopo de riscos (estratégico, tático, operacional e ambiental).

Importante ressaltar que a predominância dos escopos nos ciclos de gerenciamento não impede que riscos pertencentes a escopos diferentes àquele abordado em um ciclo não possam ser incorporados ao gerenciamento. Quaisquer riscos podem ser incorporados em quaisquer ciclos. A definição dos ciclos pretende apenas auxiliar no planejamento dos trabalhos ao tratar os escopos de maneira sequencial, porém não exclusiva.

Abaixo são apresentados os ciclos planejados para a GR-CTGM.

Primeiro ciclo	Segundo ciclo	Terceiro ciclo
■ Alinhamentos e imersões na gestão de riscos da CTGM ■ Levantamento de objetivos das unidades setoriais (táticos) ■ Gerenciamento de riscos do escopo tático	■ Levantamento dos objetivos operacionais ■ Mapeamento e análise de processos operacionais ■ Gerenciamento de riscos do escopo operacional	■ Levantamento e desdobramento de objetivos estratégicos ■ Levantamento de projetos da Controladoria que sustentam o planejamento estratégico ■ Gerenciamento de riscos do escopo estratégico
Riscos de ambiente		
■ Gerenciamento de riscos gerais da CTGM, que não sejam enquadrados nos ciclos anteriores, como, por exemplo: riscos associados ao **ambiente de trabalho** (instalações, infraestrutura, equipamentos, tecnologia etc.); riscos relacionados à segurança de **acesso a locais restritos**; riscos relacionados à **segurança da informação** (confidencialidade, integridade da informação, disponibilidade, autenticidade, irretratabilidade); riscos relacionados a **fatores humanos** (conflitos, comunicação, treinamento etc.); **demais riscos** que não sejam específicos dos escopos estratégico, tático ou operacional.		

Tabela 3 - Ciclos de implementação da GR-CTGM

[8] As unidades compreendidas em cada núcleo de gerenciamento foram extraídas do Decreto Municipal 16.738/2017, conforme o organograma da estrutura atual da Controladoria-Geral.

Além dos escopos definidos, a gestão de riscos da CTGM contou com uma etapa de iniciação para preparação de políticas, definição das equipes, treinamentos preliminares e mobilização das unidades.

Abaixo é apresentado quadro com as atividades e resultados esperados em cada fase da gestão de riscos da CTGM.

Fases	Atividades	Produtos gerados
Iniciação **Objetivos:** ■ Preparar a CTGM para a implementação da gestão de riscos	**Gestão:** 1. Definição de equipes 2. Elaboração da Política de Riscos 3. Autoavaliação da maturidade 4. Autoavaliação do contexto 5. Elaboração da metodologia da GR-CTGM 6. Planejamento do ciclo 1	■ Port. CTGM-019/2017 ■ Port. CTGM-013/2018 ■ Matriz SWOT ■ Metodologia e controles da GR-CTGM ■ Cronograma do ciclo 1
Ciclo 1 **Objetivos:** ■ Alinhamentos com o Comitê de Integridade ■ Entendimento do estágio das unidades quanto ao gerenciamento de riscos ■ Levantamento de competências e principais processos organizacionais ■ Gerenciamento de riscos táticos e ambientais ■ Imersão dos gestores na GR-CTGM **Escopos predominantes:** ■ Tático ■ Ambiental	**Gerenciamento:** 1. Autoavaliação do sistema de controle interno. 2. Avaliação da conformidade normativa 3. Autoavaliação do alinhamento com metas da PBH (PPAG e LOA) 4. Elaboração da cadeia de valor 5. Execução do ciclo de gerenciamento de riscos **Gestão:** 6. Consolidação de informações 7. Alimentação de indicadores 8. Registros de melhoria 9. Planejamento do ciclo seguinte 10. Aprovação dos planos de ação	■ Questionários de avaliação ■ Cadeias de valor ■ Gerenciamentos de riscos ○ Identificação ○ Análise ○ Avaliação ○ Tratamento ■ Planos de Gerenciamento de Riscos ■ Plano (integrado) de Gestão de Riscos ■ Planos de ação aprovados ■ Cronograma do ciclo seguinte
Ciclo 2 **Objetivos:** ■ Análise dos fluxos operacionais ■ Gerenciamento de riscos operacionais ■ Imersão de demais servidores na GR-CTGM **Escopo predominante:** ■ Operacional ■ Ambiental	**Gerenciamento:** 1. Autoavaliação do sistema de controle interno. 2. Priorização e mapeamento dos processos operacionais 3. Execução do ciclo de gerenciamento de riscos 4. Monitoramento de riscos **Gestão:** 5. Consolidação de informações 6. Alimentação de indicadores 7. Registros de melhoria 8. Planejamento do ciclo seguinte 9. Aprovação dos planos de ação	■ Questionários de avaliação ■ Processos operacionais prioritários mapeados ■ Gerenciamentos de riscos ○ Monitoramento dos ciclos anteriores ○ Identificação ○ Análise ○ Avaliação ○ Tratamento ■ Planos de Gerenciamento de Riscos ■ Plano (integrado) de Gestão de Riscos ■ Planos de ação aprovados ■ Cronograma do ciclo seguinte
Ciclo 3 **Objetivos:** ■ Integração da gestão de riscos ao planejamento estratégico da CTGM e da PBH ■ Gerenciamento de riscos estratégicos	**Gerenciamento:** 1. Autoavaliação do sistema de controle interno. 2. Decomposição dos objetivos estratégicos em ações e projetos 3. Definição de responsáveis (unidades e pessoas) 4. Execução do ciclo de gerenciamento	■ Questionários de avaliação ■ Objetivos e metas estratégicas decompostas ■ Gerenciamentos de riscos ○ Monitoramento dos ciclos anteriores ○ Identificação ○ Análise

e de projetos **Escopo predominante:** ■ Estratégico ■ Ambiental	de riscos 5. Monitoramento de riscos **Gestão:** 6. Consolidação de informações 7. Alimentação de indicadores 8. Registros de melhoria 9. Planejamento de eventual ciclo seguinte 10. Aprovação dos planos de ação	○ Avaliação ○ Tratamento ■ Planos de Gerenciamento de Riscos ■ Plano (integrado) de Gestão de Riscos ■ Planos de ação aprovados ■ Cronograma do ciclo seguinte

Tabela 4 - Atividades dos ciclos da GR-CTGM

Informações complementares

Organizações e processos organizacionais

Organizações são quaisquer agrupamentos de pessoas e recursos que funcionam de maneira coordenada e integrada com o **objetivo** principal de **agregar valor** aos seus **clientes** (cidadãos, sociedade ou outras organizações).

A agregação de valor é alcançada com os produtos, serviços e benefícios que as organizações proveem aos seus clientes. Além desses resultados (finalísticos), a organização também pode definir objetivos intermediários, como critérios sobre a forma que os produtos e serviços serão disponibilizados (conformidade, eficiência, economicidade), quesitos de integridade (ética, conduta, responsabilidades das partes interessadas), requisitos de qualidade (tempestividade, efetividade, satisfação dos clientes), dentre outros.

As organizações podem ser estruturadas em **unidades** internas segmentadas para melhor distribuição do trabalho e eficiência no uso dos recursos. Essas unidades, por sua vez, podem ser divididas em outras unidades para aumentar as especialidades dos trabalhos. Dessa forma, teremos a organização como sendo a estrutura de toda a corporação, que pode ser dividida em unidades e que, por sua vez, podem se subdividir em outras unidades.

*A Prefeitura de Belo Horizonte será representada na gestão de riscos da CTGM como **organização**, enquanto as Secretarias, Entidades e seus órgãos e setores internos serão representados como **unidades**.*

Qualquer organização é formada por **processos** (processos organizacionais, ou processos de negócio) e os produtos e serviços disponibilizados são resultados da execução de um ou vários processos. Por outro lado, todos os processos devem participar direta ou indiretamente da geração de produtos e serviços. Na concepção mais usual, processo é definido como qualquer atividade ou conjunto de atividades que toma uma **entrada** (*input*), adiciona valor a ela e fornece uma **saída** (*output*). Os processos utilizam os recursos da organização para oferecer resultados a seus clientes (Harrington, 1991 apud Gonçalves, 2000). Ou ainda, processo organizacional é uma agregação de atividades e comportamentos executados por humanos ou máquinas para alcançar um ou mais resultados (BPM CBOK, 2013).

Podemos classificar os processos organizacionais em dois tipos: **finalísticos**, que se destinam a prover produtos e serviços diretamente voltados para os clientes e os **de suporte**, que dão apoio aos processos finalísticos[9].

[9] Há outras classificações e denominações para os processos organizacionais, mas para efeito de simplificação e melhor entendimento, a gestão de riscos da CTGM utilizará os termos **finalísticos** e **de suporte**.

A divisão e estruturação dos processos são importantes para analisar o funcionamento interno das organizações em diversos níveis de detalhamento. Para os propósitos da Gestão de Riscos da Controladoria (GR-CTGM), apresentaremos, a seguir, conceitos sucintos sobre análise de processos organizacionais, como: cadeia de valor, decomposição e mapeamento de processos, dentre outros pontos relevantes para contextualização da GR-CTGM.

Cadeia de valor

A cadeia de valor[10] enfatiza a captura de processos e atividades que adicionam valor ao serviço ou produto entregue ao cliente. Proporciona uma visão geral dos processos de negócio e demonstra um fluxo simples contínuo da esquerda para a direita dos processos que diretamente contribuem para gerar valor[11] (BPM CBOK, 2013).

A organização (ou cada uma de suas unidades) é vista como um grande processo que transforma as entradas (eventos, materiais, informações etc.) em saídas (produtos, serviços, benefícios etc.) aos clientes (internos e externos) por meio de funcionalidade internas (processos finalísticos e de suporte). Por ela proporcionar uma visão holística da unidade, também é utilizada em setores de diversos ramos e naturezas como ferramenta de análise do ambiente e dos objetivos organizacionais.

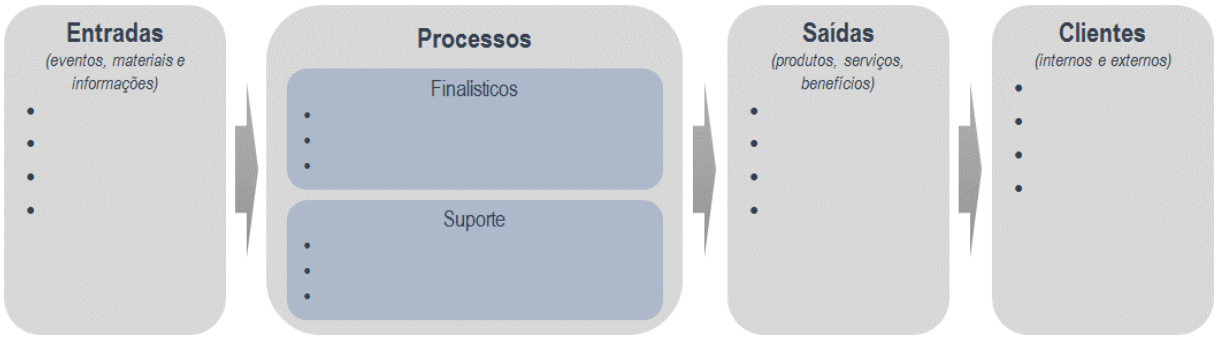


Figura 7 - Cadeia de valor

Decomposição de processos

A decomposição separa e desmembra os processos para melhor organização e detalhamento de suas funcionalidades. Os processos devem ser segmentados de uma maneira lógica, de forma que o conjunto de atividades pertencentes a um processo colaborem entre si para fornecimento de uma saída em comum (produto ou serviço).

Os processos devem ser decompostos até o ponto que seja satisfatório para atender às análises e controles gerenciais e operacionais. Não há necessidade de termos o mesmo nível de decomposição para cada um, é tudo uma questão de conveniência para quem o está modelando; ou seja, os processos são decompostos até o ponto que se julgar necessário para analisar o fluxo no nível que se deseja.

[10] A cadeia de valor foi desenvolvida por Michael Porter em seus trabalhos sobre estratégia corporativa e é tipicamente aplicada à modelagem organizacional em nível de planejamento.
[11] A disposição da cadeia de valor pode variar conforme as necessidades de análise das organizações. Algumas delas descrevem os componentes em um nível maior de detalhes, incluindo elementos do planejamento estratégico (missão, visão, valores), informando os fornecedores das entradas ou segregando os processos nas unidades que compõem a organização.

Alguns autores e metodologias definem nomes diferenciados, conforme o nível do processo dentro da decomposição, como **macroprocesso** para os mais abrangentes, isto é, aqueles que estão no alto ou no início da decomposição, ou **subprocessos** para os que definem maior nível de detalhamento ou de reutilização de atividades. Para fins práticos e também didáticos, chamaremos todos de **processos**, sem fazer nenhuma diferenciação do seu nível de detalhamento. A única distinção que teremos é para **atividades**, que não são decompostas e representam o menor nível do desmembramento (Sordi, 2018). Dessa forma, os processos poderão ser decompostos em outros processos ou em atividades. Já as atividades é o nível mais detalhado da decomposição e representa a menor unidade de trabalho[12].

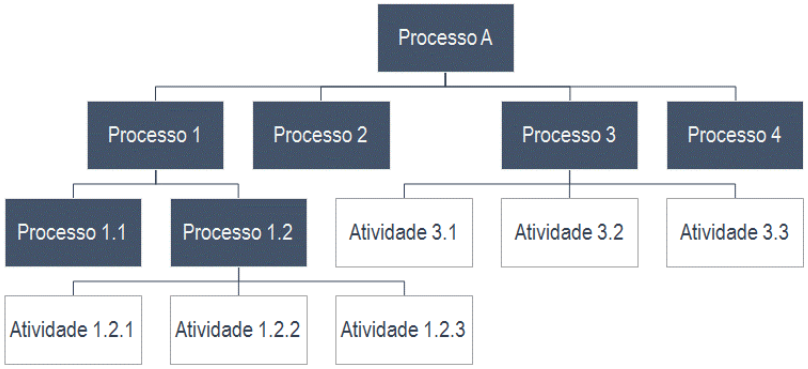


Figura 8 - Decomposição de processos (Sordi, 2018)

A gestão de riscos da CTGM adotará dois conceitos principais para a identificação e decomposição de processos organizacionais: ***processos*** *e* ***atividades****.*

Mapeamento de processos

O mapeamento é um modelo que representa o funcionamento interno dos processos, dando uma visão sequencial das atividades de forma que possamos analisar os principais pontos críticos, controles, gargalos, ambiguidades, vulnerabilidades operacionais etc.

Podemos mapear processos utilizando quadros, diagramas ou mesmo textos para descrever o arranjo e encadeamento de suas atividades.

O mapeamento é como um "Raio X" dos processos organizacionais, utilizado para análises e diagnósticos de fragilidades do fluxo operacional, controles internos, riscos etc.

O mapeamento de processos deverá ser aplicado com maior frequência no gerenciamento de riscos do nível operacional da organização, pois seus fluxos de trabalho deverão ser avaliados em um grau de detalhamento que possibilite reconhecer os riscos a partir da execução das atividades.

[12] TCU (2012) acrescenta que as atividades de uma organização podem ser vistas sob diversas dimensões, dependendo do nível de agregação conveniente para um determinado processo. Assim, é comum ouvirmos alguém perguntar: "qual é a atividade da sua organização?" A resposta a essa pergunta representa o macroprocesso finalístico da organização. Contudo, esse macroprocesso, que ainda pode ser desdobrado em outros grandes processos, que também podem ser denominados, e daí por diante em processos, subprocessos, atividades e tarefas, representam uma hierarquia de atividades. Portanto, essas denominações são adotadas meramente por convenção, para delimitar as diversas dimensões que as atividades da organização assumem, as quais, genericamente, denominam-se processos.

Abaixo são apresentadas algumas técnicas de mapeamento de processos para descrever fluxos e características dos processos a fim de analisá-los de maneira pormenorizada:

- **Fluxogramas (mapa de processos)** – Diagramas que representam o circuito de execução de um processo organizacional. Atualmente utiliza-se, como maior regularidade a notação BPMN (*Business Process Model and Notation*) por prover uma linguagem de fácil compreensão, ao mesmo tempo que disponibiliza modelos que podem ser analisados e simulados de forma semiautomática por ferramentas de tecnologia.
- **5W2H** – Acrônimo de *What, Where, Who, When, Why, How e How much* (o que, onde, quem, quando, por que, como e quanto). Com um quadro de mapeamento, os processos são dispostos nas linhas e as colunas indicam o 5W2H, possibilitando a análise dos processos utilizando uma abordagem semântica dos seus objetivos, destinações e modos de operação.
- **Matiz GUT** – A Matriz GUT poderá ser empregada para definir as prioridades dos processos organizacionais mediante a indicação de sua *Gravidade*, *Urgência* e *Tendência*. O produto dos três fatores dará a prioridade de um processo diante os demais e auxiliará no gerenciamento de riscos ao focar, inicialmente, os de maior criticidade.
- **SIPOC** – Abreviação de *Suplier* (fornecedor), *Input* (entradas), *Process* (descrição do processo), *Output* (saída), *Customers/Clients* (clientes). Essa disposição é análoga à utilizada na cadeia de valor, porém em forma de quadro.
- **Texto** – É a descrição textual da sequência das atividades do processo de forma objetiva. Deve incluir os atores, os recursos, os controles e outras informações relevantes para a análise.

Processos e projetos

Os processos organizacionais fazem parte da rotina operacional da organização. Seus elementos são previamente conhecidos e o seu funcionamento e resultados são relativamente previsíveis.

Já os projetos são esforços temporários empreendidos para criarem um produto, serviço ou resultado exclusivo. A natureza temporária dos projetos indica que eles têm um início e um término definidos. O término é alcançado quando os objetivos do projeto são atingidos ou quando o projeto é cancelado (PMBOK, 2013).

Após a conclusão bem-sucedida de um projeto, pode-se criar uma rotina a partir da sua implantação e definir, a partir daí, um processo organizacional para sua continuidade operacional.

A tabela abaixo apresenta as diferenças elementares entre processos e projetos.

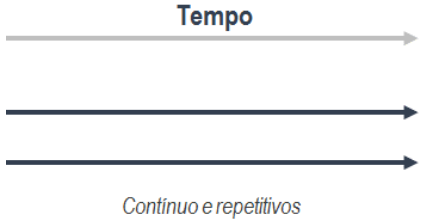
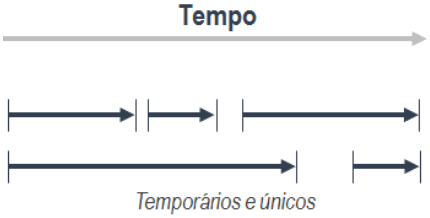
PROCESSOS	PROJETOS
Objetivos contínuos para realização de procedimentos repetitivos	Objetivos bem definidos com prazos e equipes pré-estabelecidos.
Ex: Atendimentos de ouvidoria, abertura de PAD, solicitação de férias etc.	Ex: Construção de um prédio, corregedoria itinerante, Programa de Integridade etc.
 Contínuo e repetitivos	 Temporários e únicos

Tabela 5 - Processos e projetos

PDCA e melhoria contínua

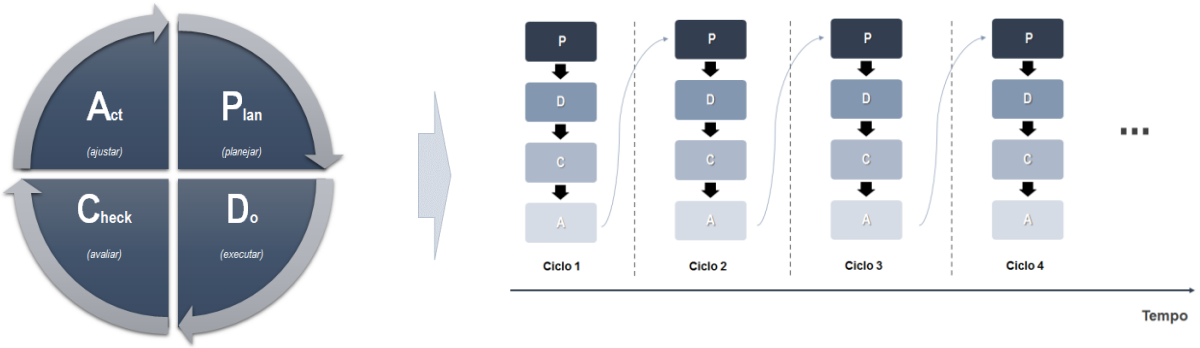


Figura 9 - Ciclo PDCA

O ciclo PDCA, acrônimo de *Plan*, *Do*, *Check*, *Act* (planejar, executar, avaliar, ajustar), ou ciclo de Deming, foi concebido como técnica no Gerenciamento pela Qualidade Total (GQT) e se tornou um padrão amplamente utilizado no desenho e melhoria de processos organizacionais com intuito de agregar qualidade e valor contínuos às operações e aos resultados dos processos. As etapas do PDCA são as seguintes:

- **Planejar (*plan*)**. Estabelecimento de objetivos e metas do processo; análise do ambiente e problemas; definição do plano de ação.
- **Executar (*do*).** Execução do plano de ação; coleta de dados de monitoramento.
- **Avaliar (*check*).** Os processos são analisados para verificar se eles cumprem o que foi proposto no planejamento.
- **Ajustar (*act*).** De acordo com o resultado da etapa anterior, serão observadas as falhas ou ineficiências nos processos e se os objetivos foram atingidos. Caso contrário, estes devem ser melhorados e as etapas se reiniciam.

A cada ciclo, a organização adquire conhecimento com o que foi realizado e melhora sua percepção sobre quais procedimentos foram benéficos ou não à qualidade e, assim, incorpora essas novas experiências aos ciclos seguintes.

Além de prover uma sistemática iterativa (cíclica) e incremental (evolutiva), o PDCA auxilia no planejamento das fases e na redução de riscos de implantação da GR-CTGM.

Na gestão de riscos da CTGM, o processo de planejar, executar e monitorar a implementação da metodologia de riscos trará aperfeiçoamentos gradativos a cada ciclo implementado. Esses aperfeiçoamentos dependerão também da constante capacitação em gestão de riscos organizacionais.

Matriz SWOT

Figura 10 - Matriz SWOT

A Matriz SWOT (*Strengts*/Forças; *Weakness*/Fraquezas; *Opportunities*/Oportunidades, *Threats*/Ameaças) possibilita análise dos contextos interno e externo da organização. Por ser de fácil e rápida implementação, é utilizada na avaliação inicial de suas potencialidades e vulnerabilidades, além de facilitar a comunicação e a proposição de ações de melhoria.

Por estarem sob o domínio da organização, os **fatores internos** são mais fáceis para serem alterados ou corrigidos se comparados com os **fatores externos**. Os **fatores positivos** devem ser potencializados, ao passo que os **negativos** devem ser minimizados.

- **Forças**. Características positivas internas que devem ser exploradas para o atingimento de objetivos. Referem-se às habilidades, capacidades e competências básicas da organização. Ex.: equipe experiente e motivada, recursos tecnológicos adequados.
- **Fraquezas**. Características negativas internas que podem inibir ou restringir o desempenho da organização. Referem-se à ausência de capacidades e/ou habilidades críticas. São, portanto, deficiências e características que devem ser superadas ou contornadas para que a organização possa alcançar o nível de desempenho desejado. Ex.: alta rotatividade de pessoal, sistemas de informação obsoletos, processos internos excessivamente burocratizados.
- **Oportunidades**. Características do ambiente externo, pouco controláveis pela organização, com potencial para ajudá-la a crescer e atingir ou exceder as metas planejadas. Ex.: diretrizes governamentais favoráveis ao fortalecimento institucional, novas fontes orçamentárias, parcerias com outras instituições.
- **Ameaças**. Características do ambiente externo, pouco controláveis pela organização, que podem impedi-la de atingir as metas planejadas e comprometer o crescimento organizacional. Ex.: dispersão geográfica do público alvo, disparidades regionais, conflito de competência.

(TCU, 2010, adaptado).

A Matriz SWOT também é chamada de "**Matriz FOFA**", em decorrência da tradução para o Português (Forças, Oportunidades, Fraquezas e Ameaças).

Riscos

Risco é o efeito da incerteza nos objetivos (ISO 31000).

A partir desse conceito, podemos verificar que antes de se falar em riscos, precisamos conhecer os objetivos da organização ou da unidade que estamos avaliando e, a partir disso, identificar quais incertezas poderão impactá-los de maneira significativa.

Temos a definição do risco pela ISO 31000 apresentada esquematicamente na figura abaixo.

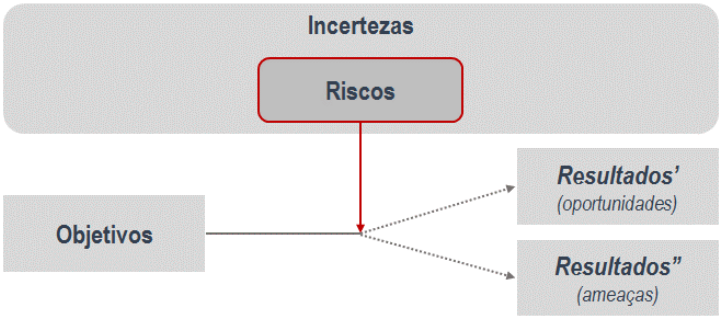


Figura 11 - Risco: efeito da incerteza nos objetivos

A ISO 31000 acrescenta que:

- **Nota 1**: Um **efeito** (impacto) é um desvio em relação ao esperado. Pode ser **positivo, negativo ou ambos**, e pode abordar, criar ou resultar em **oportunidades** ou **ameaças**.
- **Nota 2**: **Objetivos** podem possuir diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis.
- **Nota 3**: **Risco** é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

Corroborando com a importância de se definir e conhecer previamente os objetivos, seguem outras fontes para a definição de risco:

- Risco é a possibilidade de que um evento ocorrerá e afetará negativamente a realização dos **objetivos** (COSO ERM).
- Risco é um evento ou condição incerta que, se ocorrer, tem um efeito em pelo menos um **objetivo** do projeto (PMBOK 5a. Edição).
- Risco é possibilidade de ocorrência de um evento que venha a ter impacto negativo no cumprimento dos **objetivos** (Port. CTGM 013/2018).

O risco é representado como sendo o produto entre a sua **probabilidade** de ocorrência e o grau do **impacto** nos objetivos, caso se consolide. Esse resultado é denominado **nível de risco**. Ambas as grandezas (probabilidade e impacto) devem usar a mesma escala de graduação que permitam a sua multiplicação. Para a gestão de riscos da CTGM, será usada a escala Likert de cinco níveis.

Riscos negativos x Riscos positivos

A incerteza que um evento ocorra e impacte os objetivos nos abre as possibilidades dele (o impacto) ser benéfico (positivo) ou danoso (negativo) aos objetivos. Os riscos negativos são gerenciados de forma que eles sejam reduzidos ao máximo, ao passo que os riscos positivos são administrados para que ocorra com maior frequência e impacto para que possam potencializar (positivamente) os objetivos.

A gestão de riscos da CTGM abordará, inicialmente, apenas os riscos negativos uma vez que eles têm maior prioridade de gerenciamento por ser um fator que pode deteriorar a qualidade dos processos organizacionais.

Risco x Problema

Como já abordado, risco é um evento incerto que pode ou não ocorrer e, se ocorrer, possivelmente impactará os objetivos. Problema, por sua vez, é um fato, é o risco negativo já consolidado. O quadro abaixo apresenta as principais diferenças entre risco e problema.

	Risco	Problema
Características	Eventos incertos, perigos, oportunidades	Risco consolidado, incidentes
Momento	Futuro	Presente
Efeito nos objetivos	Pode interferir	Interfere
Tratamento	Plano de gerenciamento	Ação de correção
Visibilidade dos efeitos do tratamento	Pouco visível	Visível
Foco	Prevenção	Correção
Atratividade política[13]	Baixa	Alta
Custo	Menor	Maior

Tabela 6 - Risco x Problema

Problemas podem demandar ações urgentes e empenho de recursos humanos e financeiros para suas soluções. Dependendo da magnitude do problema, pode ser necessário um planejamento para a sua correção e, porventura, tratá-lo em uma frente de trabalho (projeto) específica.

Um problema também pode ser uma causa para novos riscos. Dessa forma, eles são abordados tacitamente no gerenciamento de riscos da CTGM ao realizar a análise dos componentes do risco. O gerenciamento de problemas e incidentes também pode contar com ferramentas distintas da gestão de riscos[14]; no entanto, a princípio, abordaremos os problemas que são causas dos riscos identificados.

Componentes do risco

Os riscos (eventos) podem ser relacionados aos fatores que os precedem (causas dos riscos) e os que os sucedem (consequências ou impactos nos objetivos).

Figura 12 - Componentes do risco

A separação dos componentes é parte da etapa de análise do gerenciamento de riscos e auxilia na agregação das suas causas-raízes. Essa agregação orienta a definição dos tratamentos dados aos riscos, uma vez que eles devem definir ações que incidam nas causas (fontes), de forma que os riscos, por consequência, sejam reduzidos (ou aumentados, em caso de oportunidades). Ou seja, a efetividade dos tratamentos de riscos é maior se as ações forem direcionadas às suas causas.

É comum ocorrer dúvidas quanto o que seria o risco (evento incerto), a causa ou a consequência. Na análise do risco, se percorrermos o caminho inverso, buscando o nexo de causalidade, talvez

[13] Pela maior urgência, o gerenciamento de problemas pode incorrer em maior prioridade de ação, se comparado ao gerenciamento de riscos, atribuindo maior visibilidade aos "solucionadores de problemas", embora o desejável sejam ações preventivas relacionadas à gestão de riscos.

[14] Alguns exemplos que podem ser adotados no gerenciamento de problemas são: **Método de Análise e Solução de Problemas** (MASP), **ITIL** (*Information Technology Infrastructure Library*) e **Análise de Causa Raiz**.

possamos enquadrar melhor os componentes do risco. Assim, a partir do objetivo, buscamos os impactos diretos do risco (consequência), o porquê desses impactos (riscos) e, por fim, o motivo desses riscos (causas).

Além disso, devemos ter em mente que:

- As causas devem ser entendidas como um **fato** ou um **requisito** da organização.
- O risco é um **evento** incerto que poderá gerar consequências nos objetivos.
- A consequência é o **prejuízo** ou **benefício** que incide diretamente nos objetivos.

Em seguida, é apresentado esquema sugerido pela GR-CTGM para identificação dos componentes do risco e problemas.

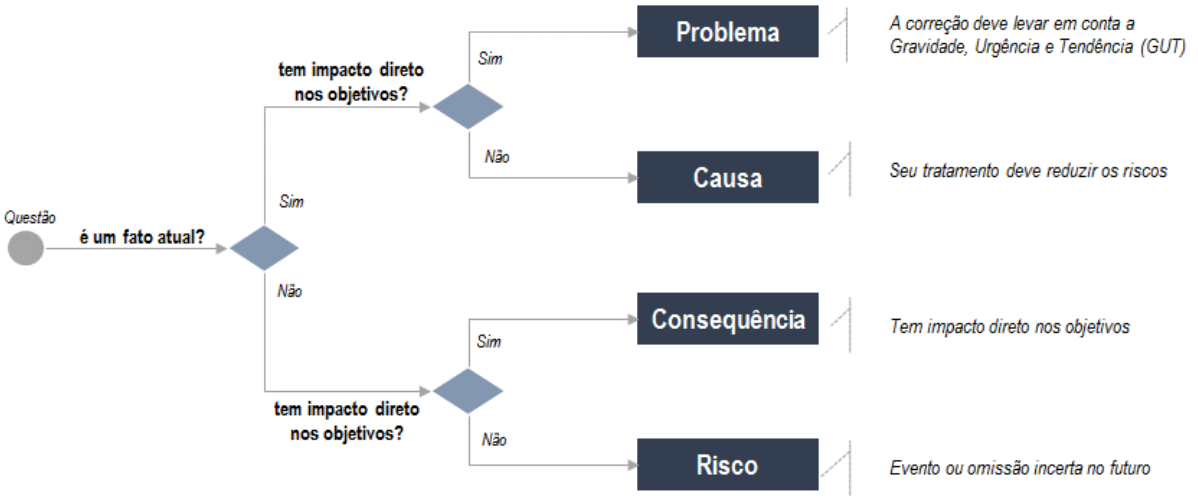


Figura 13 - Avaliação dos componentes do risco

Para avaliar os componentes do risco, também recomenda-se a "sintaxe" de descrição do risco, que auxilia na formação da estrutura causa-risco-consequência-objetivo, conforme apresentado abaixo.

Sintaxe do risco: "Devido à <CAUSA>, poderá acontecer <RISCO>, o que poderá levar à <CONSEQUÊNCIA>, impactando no <OBJETIVO>"

(CGU)

Controles internos

Os controles internos são adotados pelas organizações com a finalidade de reduzir os riscos, ou os seus efeitos, a níveis aceitáveis. Os controles podem ser **preventivos**, atuando nas causas do risco; **concomitantes**, quando aplicados durante a consolidação do risco; ou **posterior**, buscando reduzir os impactos negativos, após a sua ocorrência.

O controle interno é um processo **dinâmico e integrado**, aplicável a qualquer tipo e tamanho de organização, porém adaptado à sua situação e cenário. O sistema de controle interno de uma organização de pequeno porte, por exemplo, pode ser menos formal e estruturado, se comparado com outra organização maior, mas, ainda assim, ser eficaz (COSO Controle Interno).

A **relação custo-benefício** também deve ser levada em conta para se avaliar as vantagens na implantação de controles internos. *A priori*, os custos de implantação e manutenção dos controles não devem ser maiores que os seus benefícios.

Riscos inerentes e residuais

Riscos inerentes são as ameaças (ou oportunidades) que, naturalmente, incidem nos objetivos e nos processos organizacionais. Nesse cenário, não se considera a presença de controles internos. Em um segundo momento, após a aplicação dos controles, os processos anteriormente desprotegidos continuarão suscitando riscos, mas agora com um nível menor do que antes (ao menos se espera). Esses novos níveis dão aos riscos um caráter residual, ou remanescente.

Os **riscos residuais** não vão deixar de existir, mesmo após a aplicação de controles altamente eficazes; mas os seus níveis devem ser reduzidos até um limite tolerável pela organização. Espera-se, assim, que sejam realizadas ações mitigadoras (melhoria dos controles internos) até que o risco esteja em um grau concebível. O aprimoramento dos controles, portanto, deve ser um trabalho contínuo e evolutivo.

Apetite a riscos

Apetite de riscos é o nível de incerteza julgada tolerável pela organização. Refere-se, portanto, ao nível de riscos, que, de forma ampla, uma organização dispõe-se a aceitar na busca de valor (COSO ERM).

Para se definir o apetite a riscos, leva-se em conta a criticidade do processo ou serviço envolvido e as disponibilidades de recursos necessários para atingir seus objetivos. Assim, se a organização não vê escassez de recursos ou de competências para alcançar um determinado objetivo, o risco é reduzido e, por conseguinte, o apetite é baixo. Ou, se o serviço prestado não for crítico, a organização poderá se dispor a enfrentar riscos mais elevados, definindo, assim, um apetite maior.

Embora oportuno que o apetite seja estabelecido no início da avaliação dos riscos, eles são dinâmicos; e convém que sejam continuamente analisados criticamente e alterados, se necessário (ISO 31000).

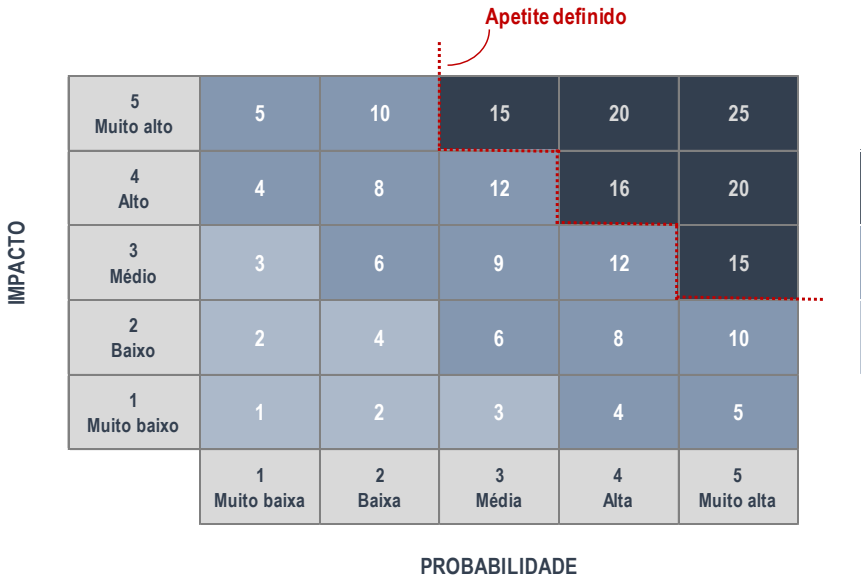


Figura 14 - Exemplo de apetite a riscos

A rigor, o setor público não tem a mesma predisposição a correr riscos como a iniciativa privada, adotando um perfil mais conservador na prestação de serviços aos cidadãos. O setor privado, devido ao ambiente competitivo e à busca pela inovação e lucro, precisa constantemente enfrentar situações incertas.

Taxonomia dos riscos

Os riscos podem ser relativos a diversas matérias conexas à organização. Há os riscos que se originam no **ambiente externo** e outros do **ambiente interno**, como os exemplos apresentados no quadro abaixo.

Ambiente interno	Ambiente externo
■ Estratégicos	■ Legais
■ Integridade	■ Políticos
■ Operacionais	■ Econômicos
■ Financeiros e orçamentários	■ Sociais
■ Segurança	■ Tecnológicos
■ Pessoas	■ Imagem e reputação

Tabela 7 - Riscos internos e externos

Os riscos também podem ser classificados a partir da perspectiva do gerenciamento. Há os riscos **conhecidos** e os **desconhecidos**. Para os primeiros, deverá ser realizado um gerenciamento adequado à criticidade e essencialidade dos serviços e produtos oferecidos pelas organizações e, para os desconhecidos, deveria haver reservas (financeiras, de recursos etc.) para tratá-los caso se efetivem.

Riscos de integridade x Riscos do Programa de Integridade

Riscos de integridade. Eventos que podem favorecer ou facilitar práticas de corrupção, fraudes, conflito de interesses e nepotismo (Art. 6, II, Dec. CTGM 013/2018).

Riscos do Programa de Integridade. Enquadram-se como riscos de projetos, os quais ameaçam a implantação do Programa de Integridade.

O quadro abaixo apresenta um modelo geral da disposição dos riscos e alternativas previstas de tratamento.

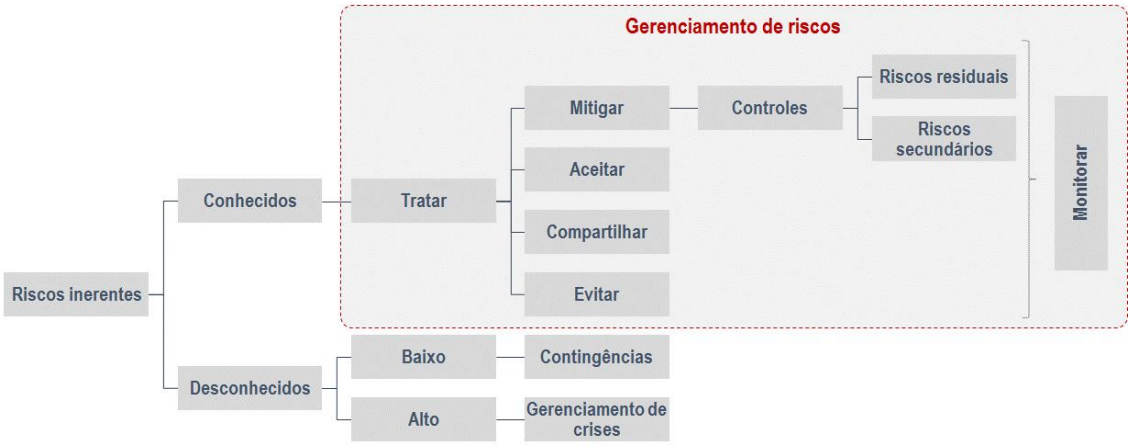


Figura 15 - Disposição geral dos riscos

Buscar conhecer os riscos previamente possibilita o tratamento tempestivo e oportuno de eventos futuros, evitando ou reduzindo seus efeitos, em caso de eventos indesejados (ameaças), ou potencializando as ocorrências, se eventos desejados (oportunidades). O gerenciamento de riscos negativos, além de ser um procedimento menos custoso, evita que a organização instaure uma rotina de "apagar incêndio" a cada problema inesperado que possa surgir.

Gestão de Riscos

A gestão de riscos envolve todas as iniciativas de uma organização voltadas para se proteger diante de ameaças dos ambientes interno e externo e também para aproveitar as oportunidades quando os eventos incertos forem benéficos à organização.

Quando realizada com base em fontes reconhecidas e apropriadas, a gestão de riscos oferece uma base de conhecimentos sobre como tratar as ameaças e oportunidades que possam surgir. **Importante compreender que na gestão de riscos se converge as diversas perspectivas administrativas (custos, prazos, qualidade etc.) e outras questões relevantes que possam influenciar o atingimento dos objetivos da organização.**

A gestão de riscos é uma abordagem estratégica e pragmática para administrar organizações.

A eficácia da gestão de riscos dependerá da sua integração com a governança e com todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da alta administração (ISO 31000).

Instituir a gestão de riscos é um processo dinâmico e contínuo, e convém que seja personalizado às necessidades e cultura de cada organização. A gestão de riscos deve ser parte, e não separada, do propósito organizacional, governança, liderança, estratégia, objetivos e operações (ISO 31000).

Referências bibliográficas

Análise SWOT e Diagrama de Verificação de Risco Aplicado em Auditoria. Portaria SEGECEX 31/2010. Tribunal de Contas da União (TCU). 2010.

GONÇALVES, José Ernesto Lima. **As empresas são grandes coleções de processos**. 2000.

Avaliação de Controles Internos. Instituto Serzedello Corrêa. Tribunal de Contas da União (TCU). 2012.

Como avaliar e testar a Maturidade da Gestão de Riscos de sua organização? Centro de Qualidade, Segurança e Produtividade (QSP).2012. *http://www.iso31000qsp.org/2012/11/como-avaliar-e-testar-maturidade-da.html*.

Controle Interno – Estrutura Integrada. Sumário Executivo. COSO – Committee of Sponsoring Organizations of the Treadway Commission. Instituto dos Auditores Internos do Brasil. 2013.

COSO ERM. Gerenciamento de Riscos Corporativos – Estrutura Integrada. Sumário Executivo. COSO – Committee of Sponsoring Organizations of the Treadway Commission. PriceWaterHouseCoopers. 2007.

COSO ERM. Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance. Sumário Executivo. COSO – Committee of Sponsoring Organizations of the Treadway Commission. The Institute of Internal Auditors, PriceWaterHouseCoopers. 2017.

Enterprise Risk Management: Frameworks, Elements, and Integration. Institute of Management Accountants (IMA). 2018. *https://www.imanet.org/insights-and-trends/risk--management/enterprise-risk-management-frameworks-elements-and-integration?ssopc=1.*

Enterprise Risk Management: Tools and Techniques for Effective Implementation. Institute of Management Accountants (IMA). 2018. *https://www.imanet.org/insights-and-trends/risk--management/test?ssopc=1*

Gestão de Riscos – Avaliação da Maturidade. Tribunal de Contas da União (TCU). 2018. *https://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm*.

Gestão de Riscos – Diretrizes. Associação Brasileira de Normas Técnicas - ABNT NBR ISO 31000. 2018.

Gestão de Riscos – Princípios e Diretrizes. Associação Brasileira de Normas Técnicas - ABNT NBR ISO 31000. 2009.

SORDI, José Osvaldo. **Gestão por processos: Uma nova abordagem da moderna administração**. 2018.

Guia do Conhecimento em Gerenciamento de Projetos – PMBOK. Project Management Institute. 5ª. Edição. 2013.

Guia da política de governança pública. Presidência da República do Brasil (PR). 2018.

Guia de Orientação para o Gerenciamento de Riscos. Versão 1.0 Final. Gespública. Ministério do Planejamento, Orçamento e Gestão (MPOG). 2013.

Guia para o Gerenciamento de Processos de Negócio. Corpo Comum de Conhecimento ABPMP BPM CBOK v.3.0. 1ª Edição. Association of Business Process Management Professional. Brasil. 2013.

Indicadores de desempenho como instrumentos de auditoria e gestão, a partir da experiência do TCU. Tribunal de Contas da União (TCU). 2004.

Kaizen: A Filosofia da Melhoria Contínua. Portal Administração. 2019. *http://www.portal-administracao.com/2014/10/kaizen-filosofia-melhoria-continua.html*

Metodologia de Gestão de Riscos. Ministério da Transparência e Controladoria-Geral da União (CGU). 2018. *http://www.cgu.gov.br/Publicacoes/institucionais/ arquivos/cgu-metodologia-gestao-riscos-2018.pdf*.

PDCA. Gestão da Qualidade. *http://gestao-de-qualidade.info/ferramentas-da-qualidade/pdca.html*.

Planejamento de Auditoria com uso de Matriz de Riscos. TCU. 2016. *http://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2016/ii-seminario-de-auditoria-interna-governamental/arquivos/22_11-tcu.pdf*

GONÇALVES, José Ernesto Lima. **Processo, que processo?** 2000.

Qual é a diferença entre gerenciar um risco e gerenciar um problema? Ricardo Vargas. *https://ricardo-vargas.com/pt/podcasts/what-is-the-difference-between-managing-a-risk-and-managing-an-issue/.* 2016.

Questionário para Avaliação da Maturidade Organizacional em Gestão de Riscos. Tribunal de Contas da União (TCU). *https://contas.tcu.gov.br/etcu/ObterDocumentoSisdoc?seAbrirDocNoBrowser=true&codArqCatalogado=8115424*

Referencial Básico de Gestão de Riscos. Tribunal de Contas da União. 2018. *https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm*

Referencial Básico de Governança. 2ª Versão. Tribunal de Contas da União (TCU). 2014.

Seminário Gestão de Riscos: Desafios para Implementação da Instrução Normativa Conjunta MP/CGU nº 1/2016. Escola Nacional de Administração Pública. Ministério da Fazenda (MF). Banco Central do Brasil (BCB). *http://repositorio.enap.gov.br/handle/1/3283*

.

Anexos

Anexo 1 - Resumo dos fluxos da gestão de riscos CTGM

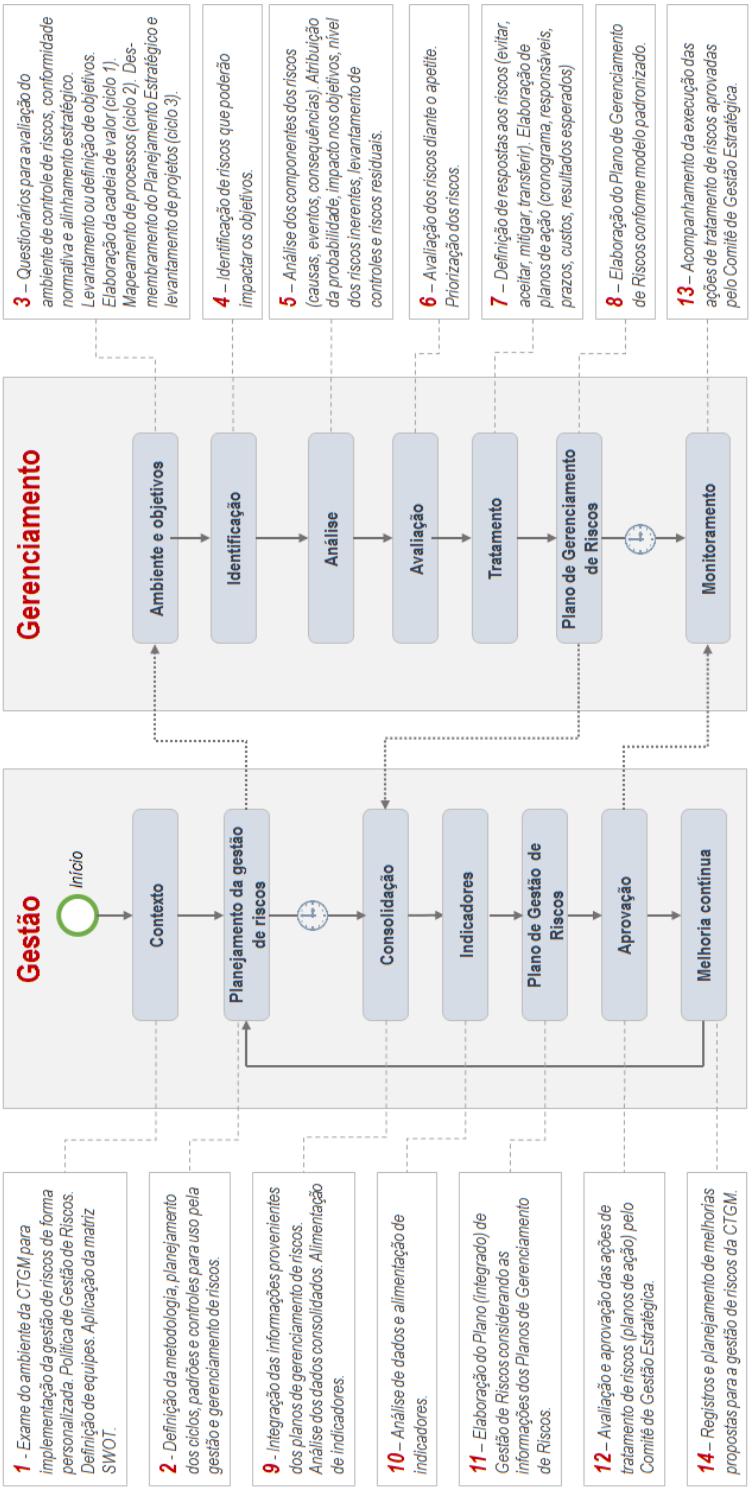


Figura 16 - Resumo dos núcleos de gestão e gerenciamento

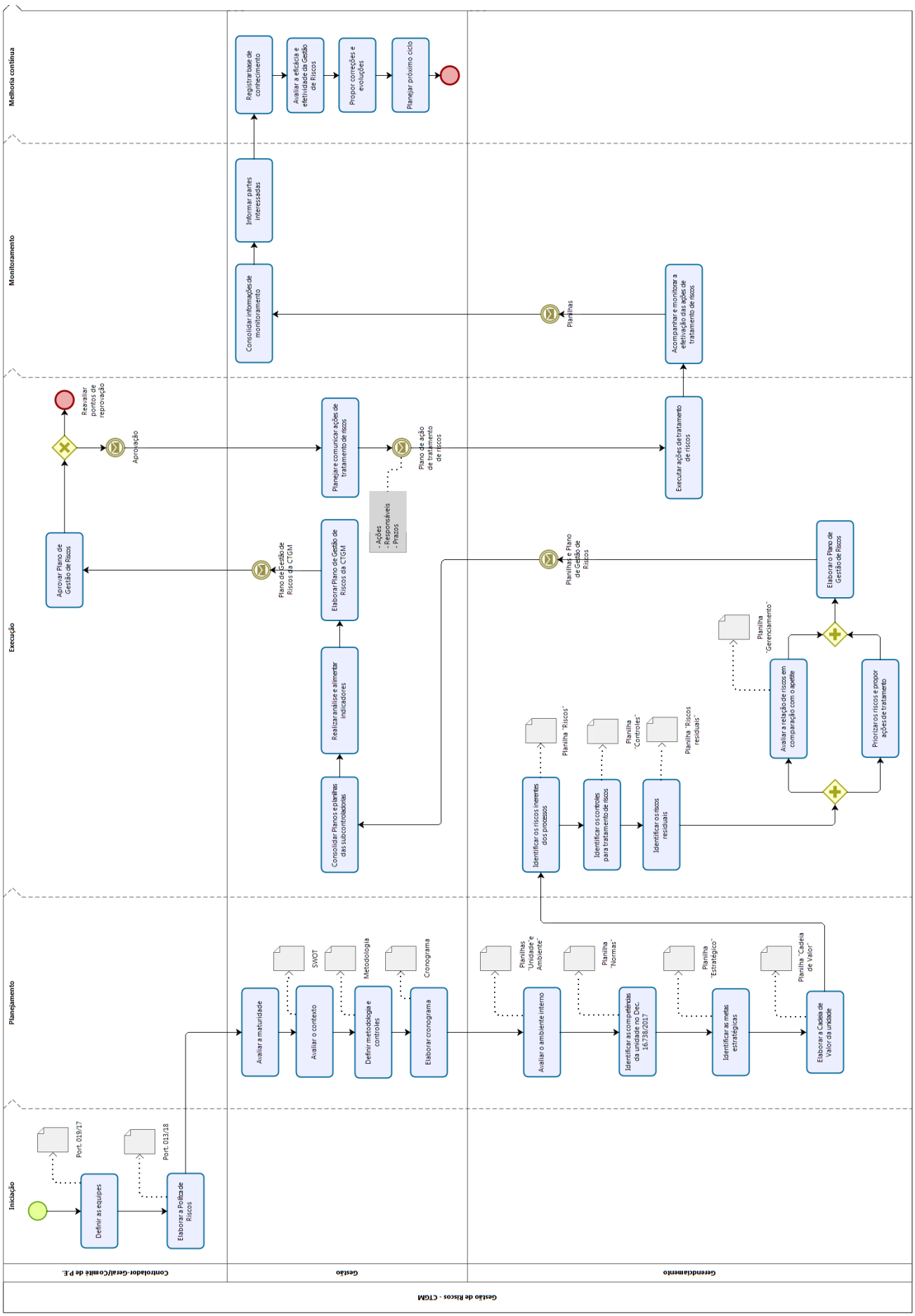


Figura 17 - Fluxo integrado da GR-CTGM