TCE-RO

MANUAL DE GESTÃO DE RISCOS
DO TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

MANUAL DE GESTÃO DE RISCOS DO TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

APRESENTAÇÃO

No intuito de melhorar os controles e na busca pela excelência no exercício de suas competências, o Tribunal de Contas do Estado de Rondônia tem adotado estratégias que possibilitem maximizar a efetividade de suas ações, dentre as quais a implantação da Metodologia de Gerenciamento de Riscos.

A sistematização da gestão de riscos constitui estratégia que aumenta a capacidade da organização para lidar com incertezas, subsidia a tomada de decisão e contribui para o uso eficiente dos recursos, de modo a aumentar a probabilidade de a missão organizacional ser alcançada.

As melhores práticas internacionais recomendam a adoção de sistemas de gerenciamento de riscos associados a gestão da estratégia em três dimensões: missão, visão e valores centrais; objetivos estratégicos e de negócios; e desempenho organizacional. A perspectiva é de assegurar o alinhamento dos objetivos à missão, visão e valores; de avaliar as implicações dos objetivos e seus fatores subjacentes; e de avaliar os riscos associados aos objetivos.

O presente Manual integra o conjunto de instrumentos essenciais para a construção do Sistema de Gestão de Riscos do Tribunal de Contas do Estado de Rondônia - SGR/TCE-RO, o qual dará suporte para a concepção, implantação e melhoria contínua da gestão de riscos em todo o Tribunal.

Como primeira versão, simplificada, a expectativa é que este Manual proporcione as orientações básicas e necessárias para a adequada coordenação das atividades de gerenciamento de riscos e controles com o intuito de o Tribunal de Contas de Rondônia alcance patamares mais elevados de governança e gestão, alinhado ao objetivo estratégico de desenvolver a governança organizacional.

O desafio, a partir de agora, é introjetar nas pessoas a cultura de pensar as atividades a partir dos riscos e de imprimir em nossas ações a orientação para resultados.

SUMÁRIO

2. INTRODUÇÃO

A vida impõe riscos. Tudo e todos estão submetidos a inúmeras variáveis e eventos que podem comprometer seus objetivos, em maior ou menor grau de probabilidade e impacto. Essa mesma regra se impõe às organizações, sujeitas a uma série de fatores que podem comprometer suas diretrizes estratégicas.

Diante disso, e considerando o atual contexto global pós-moderno, que intensificou as inter-relações e multiplicou as variáveis, é essencial, como estratégia de sucesso, que as organizações passem a gerenciar os riscos de maneira integral e sistematizada, para reduzir as chances de fracasso e potencializar as oportunidades de sucesso.

Atento à essa exigência, que de maneira geral ainda engatinha no âmbito da Administração Pública, o Tribunal de Contas, sensível à necessidade de aprimoramento organizacional, está dando o primeiro passo em busca da excelência em seus processos de governança, por meio da implantação da gestão de riscos.

A gestão de riscos deve ser compreendida como instrumento central de tomada de decisão da alta administração, na medida em que oferece aos executivos informações sobre como reduzir a probabilidade e o impacto de ameaças e de como potencializar os resultados organizacionais.

A ideia de adotar um sistema de gestão de riscos é permitir, dentre inúmeros outros benefícios esperados[1], que a alta administração e os gestores sejam capazes, a partir do conhecimento dos riscos, de contribuir com a estratégia organizacional de maneira eficiente. Isto é, a Gestão de Riscos, muito mais do que um mero conjunto de procedimentos de controle, busca gerar valor à organização, contribuindo fundamentalmente para a realização de seus objetivos e metas de desempenho.

Este Manual de Gestão de Riscos, portanto, nasce com a proposta de estabelecer, de maneira prática, o passo-a-passo do gerenciamento de riscos no Tribunal de Contas do Estado de Rondônia.

[1] A implantação da Gestão de Riscos traz vários benefícios para a organização: a) preserva e aumenta o valor da organização, mediante a redução da probabilidade e/ou impacto de eventos de perda, combinada com a diminuição de custos de capital que resulta da menor percepção de risco por parte de financiadores e seguradoras e do mercado em geral; b) promove maior transparência, ao informar aos investidores e ao público em geral os riscos aos quais a organização está sujeita, as políticas adotadas para sua mitigação, bem como a eficácia das mesmas; c) melhora os padrões de governança, mediante a explicitação do perfil de riscos adotado, em consonância com o posicionamento dos acionistas e a cultura da organização, além de introduzir uma uniformidade conceitual em todos os níveis da organização, seu conselho de administração e acionistas.

2. REFERENCIAL TEÓRICO

O manual foi elaborado com base na análise de *frameworks* de aplicação internacional (COSO ERM, COSO GRC e ISO 31000/09), e, em especial, no Referencial Básico de Gestão de Riscos do Tribunal de Contas da União[2] e no Manual de Gestão de Integridade, Riscos e Controles Internos do Ministério do Planejamento[3].

2.1 Riscos

O gerenciamento de riscos consiste em um processo que busca gerenciar potenciais eventos que podem impactar o alcance dos objetivos organizacionais. Mas, afinal, o que é risco?

De acordo com a Política de Gestão de Riscos do TCERO, "risco é a possibilidade de que um evento afete negativamente a organização". Vale dizer, é tudo aquilo que de alguma maneira tenha potencial de afetar os resultados pretendidos pela organização.

Segundo disposto no Referencial Básico de Gestão de Riscos do Tribunal de Contas da União:

> "Risco é o efeito da incerteza sobre objetivos estabelecidos. É a possibilidade de ocorrências de eventos que afetem a realização ou alcance dos objetivos, combinada com o impacto dessa ocorrência sobre os resultados pretendidos." (p. 8)

Nesse sentido, em síntese, risco é a probabilidade de ocorrência de um fato com potencial de impactar o alcance dos objetivos organizacionais.

2.2 Riscos e Controle Interno

De acordo com o *Committe of Sponsoring Organizations* (COSO), no referencial de Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO ERM), controle interno:

> "É um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de

[2] BRASIL. Tribunal de Contas da União. Referencial básico de gestão de riscos. Brasília, Secretaria Geral de Controle Externo, 2018. Disponível em: www.tcu.gov.br . Acessado em 16/04/2019.
[3] BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Manual de gestão de integridade, riscos e controles internos da gestão. Brasília, Assessoria Especial de Controle Interno, 2017. Disponível em: http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc . Acessado em 16/04/2019.

> afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos." (COSO ERM, 2004)

Controle interno é, portanto, um conjunto de processos, normas e estruturas que, de maneira integrada, busca conferir razoável segurança[4] ao alcance dos objetivos organizacionais.

Em síntese, gestão de riscos e controles internos voltam-se ao cumprimento dos objetivos organizacionais. São instrumentos que compõem a estrutura central da governança organizacional e devem funcionar de maneira sistêmica e integrada para que, de fato, a estratégia e os objetivos da organização sejam alcançados com segurança.

Para a Organização Internacional de Entidades de Fiscalização Superior (INTOSAI), a avaliação de riscos é um componente do controle interno, essencial para a seleção de atividades de controle, pois é o processo de identificação e análise dos riscos que determina as respostas apropriadas aos riscos organizacionais. (INTOSAI GOV 91000, p. 25)

Vale dizer, há clara inter-relação lógica entre o gerenciamento de riscos e a implantação de controles, na medida em que os controles internos são determinados a partir do processo de avaliação de riscos (identificação, análise e avaliação).

3. PROCESSO DE GESTÃO DE RISCOS

3.1 Visão Geral

O processo de gerenciamento de riscos, de acordo com o referencial COSO ERM, compõe-se de 8 (oito) etapas: ambiente interno, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta a riscos, atividades de controle, informação e comunicações e monitoramento.

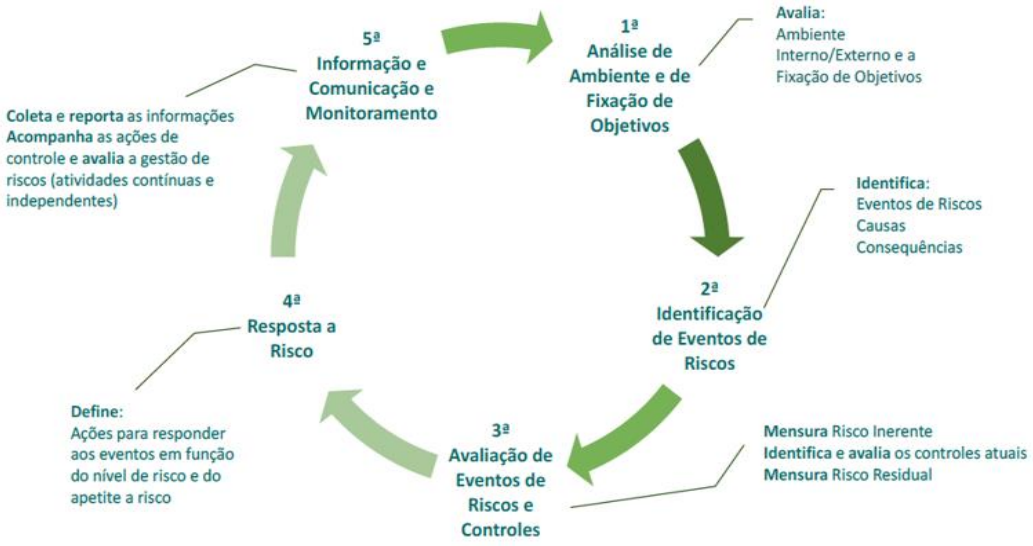
O gerenciamento de riscos, de acordo com o COSO ERM, é representado graficamente pelo cubo COSO:

[4] Segurança razoável equivale a um nível satisfatório de confiança considerando custo, benefício e riscos. (INTOSSAI GOV 9100, p. 8).

Figura 1 – Coso ERM, 2004

A estrutura do COSO ERM, com exceção de alguns detalhes conceituais, é a mesma do processo de gestão de riscos da ISO 31000/09, que, em síntese, compõem-se das etapas de estabelecimento do contexto (ambiente interno); identificação, análise e avaliação de riscos; seleção, implementação e monitoramento dos controles; e, comunicação dos riscos para os *stakeholders*.

Da mesma maneira, é a forma como o Ministério do Planejamento elaborou o ciclo de gerenciamento de riscos no âmbito da União, representada, em síntese, pelo gráfico abaixo:



3.2 Aplicação

O processo de gestão de riscos aplica-se a toda organização, a partir da compreensão do ambiente e dos objetivos.

Organização compreende toda a organização em si, ou apenas parte dela, podendo se restringir a um programa, projeto, processo de trabalho ou atividade operacional. Vale dizer, a gestão de riscos aplica-se em qualquer nível organizacional, do estratégico ao operacional.

Restringindo-se a processos, projetos ou atividades operacionais, o estabelecimento do contexto, além de compreender os objetivos da organização, também abrange os objetivos do objeto da gestão de riscos, de maneira que seja possível identificar os riscos específicos do processo, projeto ou atividade operacional em análise.

3.3 Etapas

Para realizar a gestão de riscos de quaisquer objetos, as seguintes etapas devem ser seguidas:

a) estabelecimento do contexto;
b) identificação dos riscos;
c) análise dos riscos;
d) avaliação dos riscos;
e) tratamento dos riscos;
f) comunicação e consulta com partes interessadas;
g) monitoramento;
h) melhoria contínua.

O processo de gestão de riscos pode ser visualizado na figura abaixo.

Figura 1: Processo de Gestão de Riscos (ISO 31000 – Adaptado)

Cada uma das etapas da gestão de riscos exige procedimentos específicos. Em razão disso, no detalhamento de cada etapa serão descritas as informações que deverão ser produzidas e as maneiras como elas poderão ser documentadas. Ressalte-se que a documentação é parte essencial no gerenciamento de riscos para cumprimento da

accountability[5], como forma de demonstrar como os recursos e objetivos foram geridos e controlados.

3.3.1 Estabelecimento do contexto

Contexto é o ambiente no qual a organização opera para alcançar seus objetivos. Estabelecer o contexto, portanto, consiste em compreender, de maneira abrangente, a própria organização (ambiente interno) e o ambiente em que atua (ambiente externo) para identificar os fatores que podem impactar a capacidade da organização em atingir seus objetivos.

Na prática, essa etapa está relacionada à análise: dos recursos humanos (valores éticos, integridade, competências, etc.), das lideranças (*tone of the top* – atitudes e ações do Conselho de Administração), da estrutura de gestão e governança, da cultura (valores, controles informais, estilo operacional da gestão, etc.) e das partes interessadas (identificar, verificar expectativas, etc.). Além disso, nesta etapa também se verifica: se os objetivos foram definidos e comunicados para todos os níveis da organização e se os objetivos estão adequadamente alinhados à estratégia organizacional.

Em síntese, o estabelecimento do contexto deve seguir os seguintes passos:
a) identificar quais objetivos ou resultados devem ser alcançados;
b) identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;
c) identificar as pessoas envolvidas nesses processos e especialistas na área;
d) mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, *stakeholders* etc.), por meio da análise SWOT; e,
e) analisar as partes interessadas a partir de seus interesses e capacidade de interferência no alcance dos objetivos, por meio da matriz de análise de *stakeholder*.

É importante ressaltar que a base para o gerenciamento de riscos são os processos de trabalho, motivo pelo qual é essencial que a cadeia de valor esteja estruturada e que os processos estejam mapeados.

[5] Obrigação que têm as pessoas, físicas ou jurídicas, públicas ou privadas, às quais se tenha confiado recursos públicos, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a sociedade e a quem lhes delegou essas responsabilidades sobre o cumprimento de objetivos e metas e o desempenho alcançado na gestão dos recursos públicos. É, ainda, obrigação imposta a uma pessoa ou entidade auditada de demonstrar que administrou ou controlou os recursos que lhe foram confiados em conformidade com os termos segundo os quais eles lhe foram entregues (Normas de Auditoria do TCU).

Caso o processo não esteja mapeado, recomenda-se a utilização do diagrama de escopo para identificação das informações gerais do processo (insumos, atividades, produtos, colaboradores, recursos, fornecedores e clientes), com base na ferramenta abaixo:

DIAGRAMA DE ESCOPO

Nome do processo:	Setor responsável:
Objetivo:	

Leis, normas, políticas e padrões

Fornecedores	Insumos	PROCESSO (principais atividades)	Produtos	Clientes/Destinatários
		Evento inicial:		
		Evento final:		

Colaboradores	Recursos

Como preencher Diagrama de Escopo de Processo? Selecione o um grupo de pessoas que tenham conhecimento e/ou trabalhem com o processo e possam contribuir com a qualidade das discussões. O grupo pode contar com pessoas que executam atividades, bem como com fornecedores, clientes, especialistas e outras partes do processo. Preencha os campos conforme as seguintes orientações:

a) Nome do processo: nome pelo qual o processo é conhecido na organização.

b) Setor responsável: nome do setor que responde pelo processo. Pode ser acompanhado da sigla.

c) Objetivo: redigir o objetivo de forma completa, explicitando, sempre que possível, dimensões de qualidade, prazo, escopo e custo. Objetivos devem ser específicos, mensuráveis ou observáveis, alcançáveis, relevantes e com prazo determinado, de maneira que possam ser compreendidos prontamente pelas pessoas que estão trabalhando para alcançá-los.

d) Leis, normas, políticas e padrões: indicar o regramento que deve ser observado na execução do processo.

e) Insumos: indicar os principais insumos utilizados pelo processo. Podem ser bens, serviços ou informações.

f) Fornecedores: indicar quem fornece os insumos para o processo.

g) Principais atividades: listar as principais atividades que compõem o processo, destacando os eventos que delimitam o processo (evento inicial e evento final).

h) Produtos: indicar os principais produtos gerados pelo processo. Podem ser bens, serviços ou informações.

i) Clientes/destinatários: indicar quem recebe os produtos gerados pelo processo.

j) Colaboradores: indicar nome dos colaboradores ou classes de colaboradores que atuam na gestão e execução do processo (comissionados, servidores, estagiários, terceirizados).

k) Recursos: indicar principais recursos materiais, tecnológicos e financeiros que sustentam a execução do processo.

Além disso, é de se destacar que a efetividade do gerenciamento de riscos passa pela adequada definição do objeto de controle com foco nos processos de maior relevância. Assim, é importante para definição do escopo do gerenciamento de riscos a aplicação do *Analytic Hierarchy Process* – ferramenta que auxilia na identificação de prioridades.

3.3.2 Identificação dos Riscos

É o processo que compreende reconhecer e descrever os riscos relacionados aos objetivos, com base na análise do contexto. A finalidade dessa etapa é produzir uma lista abrangente de todos os riscos, por meio de consultas internas e externas, dados históricos e análises teóricas.

A identificação dos riscos deve seguir os seguintes passos:

a) identificar com clareza o(s) objetivo(s)/resultado(s) do processo, projeto ou atividade;
b) envolver as pessoas necessárias para identificação dos riscos;
c) definir as dinâmicas e estruturar as ferramentas e processos que serão utilizados para identificar os riscos;
d) listar, para cada objetivo/resultado, os eventos que possam vir a ter impacto negativo no alcance do objetivo/resultado;
e) descrever as causas dos riscos e a maneira como impactam o objetivo/resultado a eles associados; e,
f) classificar os riscos quanto à abrangência (setorial, intersetorial ou institucional) e à categoria (operacional, estratégico, integridade, imagem, etc).

A identificação dos riscos deve ser realizada em oficinas de trabalho por meio de técnicas que permitam levantar, de maneira abrangente, todos os riscos (*Brainstorming*, *Delphi*, entrevistas estruturadas, visitas técnicas, etc.). Feita a identificação, é necessário detalhar as causas e consequências dos riscos por meio de técnicas apropriadas (*Bow-Tie*, Diagrama de *Ishikawa*, etc.).

Algumas perguntas podem facilitar a identificação dos riscos, dentre as quais:

a) o que pode atrapalhar o alcance do objetivo/resultado?
b) o que pode afetar os fatores de sucesso necessários para alcance do objetivo/resultado?
c) existe algum problema relacionado à infraestrutura, pessoal, processo, norma ou tecnologia que pode comprometer o objetivo/resultado?
d) qual é a causa (e a causa da causa) do evento de risco identificado?

Convém ressaltar que os riscos devem ser identificados por um grupo de pessoas com conhecimento adequado e capacidade de análise sistêmica da área e do funcionamento organizacional, a partir da seguinte estrutura:

Devido a **<CAUSA/FONTE>**, poderá acontecer **<DESCRIÇÃO DO EVENTO DE RISCO>**, o que poderá levar a **<DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS>** impactando no/na **<OBJETIVO DE PROCESSO >**.

Ao descrever o evento de risco propriamente dito, cuidado com os seguintes erros recorrentes:

a) Evite descrever o evento de risco como a ausência de um controle. Exemplo: “falta de segregação de funções” (errado). A necessidade de um controle (solução) pressupõe um risco associado (problema).

b) Evite descrever o risco como o não atingimento do objetivo do processo de trabalho ou atividade. Exemplo: “não entregar 90% dos relatórios no prazo” (errado). Riscos devem ser eventos que podem impedir que o objetivo seja alcançado.

c) Evite descrever o evento de risco como problema ou situação existente. A gestão de risco deve orientar-se para o futuro. Exemplo: “servidores não capacitados”. Avalie se o problema não seria a causa de um evento futuro e incerto (risco) que afetará os objetivos da operação analisada.

A elaboração de uma matriz SWOT pode auxiliar a identificação de riscos. Franquezas e Ameaças podem ser fontes de riscos negativos e oportunidades podem resultar em riscos positivos.

Note-se que a análise do risco deve estar sempre associada ao objetivo do processo, o que pressupõe haver clareza da finalidade do processo analisado e de seu impacto na estratégia organizacional.

3.3.3 Análise dos Riscos

Analisar risco é um processo de compreender a natureza do risco, dimensionando o impacto e a probabilidade de sua ocorrência para subsidiar a tomada de decisão. O resultado da análise serve, essencialmente, para classificar os riscos de maneira que se permita identificar quais são os mais relevantes para a organização, quais precisam ser priorizados e quais são as estratégias de respostas a serem adotadas.

A avaliação dos riscos deve seguir os seguintes passos:

a) avaliar o impacto do risco sobre o objetivo/resultado – o impacto mede o potencial comprometimento do objetivo/resultado (p.ex.: um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto);
b) avaliar a probabilidade de ocorrência do risco (p.ex.: um evento cuja ocorrência seja quase certa de acontecer é um evento de alta probabilidade);
c) definir o nível do risco com base na matriz probabilidade e impacto.

A matriz define o nível de riscos a partir da combinação das escalas de probabilidade e de impacto, avaliados a partir da percepção das pessoas, com base nos critérios qualificadores abaixo:

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE	PESO
MUITO BAIXA	Improvável. Não há histórico conhecido de ocorrência.	1
BAIXA	Rara. Embora haja histórico conhecido de sua ocorrência na gestão e operação da atividade, o evento é raro (1 vez a cada 2 anos)	2
MÉDIA	Possível. Histórico de ocorrência e/ou a análise de cenário sugere que o evento deve ocorrer (até 1 vez ao ano)	3
ALTA	Provável. Histórico de ocorrência e/ou a análise de cenário sugere que o evento deve ocorrer (entre 2 a 5 vezes ao ano)	4
MUITO ALTA	Histórico de ocorrência e/ou a análise de cenário sugere que o evento deve ocorrer (mais de 5 vezes ao ano)	5

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS	PESO
INSIGNIFICANTE	Mínimo. O impacto sobre os objetivos (estratégicos, operacionais, de informação/comunicação, conformidade) é mínimo	1
BAIXO	Pequeno. Pouco afera os objetivos (estratégicos, operacionais, de informação/comunicação, conformidade)	3
MÉDIO	Moderado. Dificulta o alcance dos objetivos (estratégicos, operacionais, de informação/comunicação, conformidade) e causa impacto moderado no custo, prazo e qualidade, porém recuperável	6
ALTO	Significativo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação, conformidade), de difícil reversão, em termos de custo, qualidade e prazo.	10
CATASTRÓFICO	Catastrófico impacto nos objetivos (estratégicos, operacionais, de informação/comunicação, conformidade), de forma irreversível	20

Os critérios qualificadores de probabilidade e impacto compõem a matriz de risco, que indica o nível do risco avaliado, subdividido em 4 (quatro) classificações: baixo (verde), médio (amarelo), alto (vermelho) e catastrófico (vermelho escuro).

Para definir o nível dos riscos, utiliza-se a matriz abaixo.

IMPACTO						
	CATASTRÓFICO (20)	20	40	60	80	100
	ALTO (10)	10	20	30	40	50
	MÉDIO (6)	6	12	18	24	30
	BAIXO (3)	3	6	9	12	15
	INSIGNIFICANTE (1)	1	2	3	4	5
		MUITO BAIXA (1)	BAIXA (2)	MÉDIA (3)	ALTA (4)	MUITO ALTA (5)
		PROBABILIDADE				

A atribuição de peso a cada uma das escalas tem a finalidade de classificar os eventos de risco por ordem de prioridade, de acordo com o produto resultante das escalas. Dessa maneira, o gestor identifica de maneira objetiva quais são os riscos mais críticos, nas hipóteses em que identificados mais de um evento de risco.

A análise inicial do risco – o risco inerente – não considera eventuais medidas de controle que já existam para reduzir a probabilidade ou mitigar o impacto, considera, apenas, o risco identificado em si, sem qualquer tratamento.

Caso o risco inerente identificado seja significativo, é necessário avaliar se já existe medida de resposta e, a partir dela, reavaliar o evento para identificar o "risco residual".

A avaliação da medida de resposta para tratar o risco inerente deve seguir 4 (quatro) requisitos, escalonados em 5 (cinco) níveis, que indicam a maturidade do controle: 1. Documentação (indica se o controle e seu procedimento de revisão foram definidos e descritos); 2. Pessoas (indica se as pessoas são comunicadas, orientadas e treinadas para executar e melhorar o controle); 3. Supervisão (indica se o controle é supervisionado pela hierarquia superior ou alguém designado); 4. Evidenciação (indica se existem evidências que permitem verificar como o controle foi executado e supervisionado e descobrir falhas).

A tabela abaixo traz os critérios e os respectivos graus de maturidade:

Critérios para avaliar a maturidade do controle

	1	2	3	4	5
DOCUMENTA-ÇÃO	Controle não foi definido.	Controle definido, mas não descrito (informal).	Controle definido e descrito de forma clara.	Controle institucionalizado por ato normativo	Controle e seu procedimento de revisão e melhoria definidos e descritos.
PESSOAS	Pessoas controlam se e como desejam. Não recebem orientação nem treinamento.	Pessoas comunicadas sobre o controle a executar.	Pessoas orientadas e treinadas para executar o controle.	Pessoas treinadas para avaliar o controle e propor ou implementar melhorias.	Pessoas preparadas para implementar melhorias no controle sem interrupção do processo.
SUPERVISÃO	Não há supervisão	Supervisão é ocasional.	Supervisão regular pela hierarquia superior ou por servidor ou grupo designado.		Monitoramento em tempo real.
EVIDENCIAÇÃO	Não há evidências que permitem identificar se e como o controle foi executado.		Existem evidências, mas obtenção é trabalhosa.	Existem evidências acessíveis que permitem verificar como o controle foi executado e supervisionado e descobrir falhas.	

Além dos critérios acima, também deve ser considerada a capacidade de mitigação do controle, o que compreende analisar em que medida o tratamento tem sido capaz de mitigar o risco.

O resultado dessa avaliação deve indicar o nível de eficácia do controle analisado, de acordo com a tabela abaixo:

Eficácia do controle

Nível do controle	Eficácia*
Forte	80%**
Satisfatório	60%
Mediano	40%
Fraco	20%
Inexistente ou inoperante	0%

* Percentual de eventos de risco que o controle é capaz de mitigar.
** Nenhum controle fornece segurança absoluta.

O percentual de eficácia deve ser considerado para o cálculo do risco residual, que será o produto da multiplicação do risco inerente com a eficácia do controle. A tabela abaixo exemplifica:

Calculando o risco residual - exemplos

Proba-bilidade	Impacto	Risco inerente	Nível do controle	Eficácia	Risco residual
Alta (8)	Moderado (5)	Alto (40)	Forte	80%	Baixo (8)
Moderada (5)	Muito alto (10)	Alto (50)	Forte	80%	Moderado (10)
Alta (8)	Alto (8)	Alto (64)	Satisfatório	60%	Moderado (25)
Baixa (2)	Moderado (5)	Moderado (10)	Mediano	40%	Baixo (6)
Baixa (2)	Alto (8)	Moderado (16)	Fraco	20%	Moderado (13)
Muito elevada (10)	Alto (8)	Extremo (80)	Inexistente ou inoperante	0%	Extremo (50)

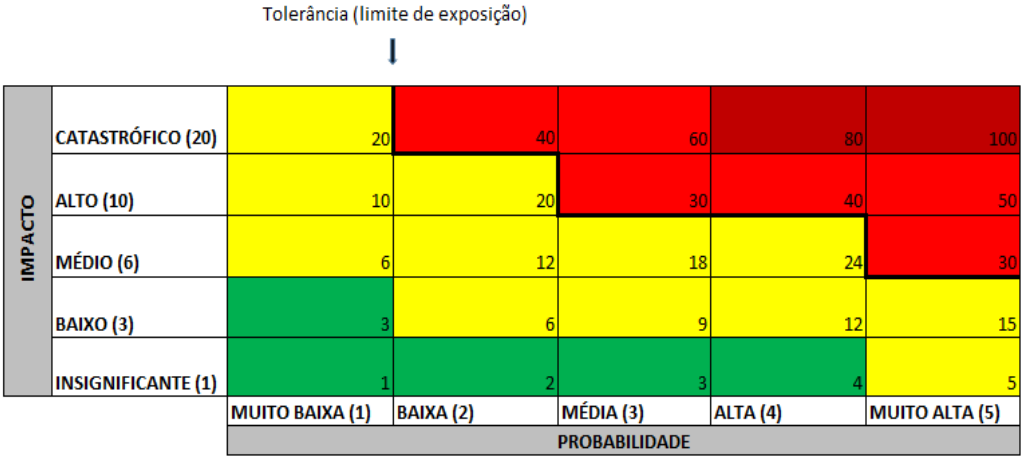
Se o risco residual ainda for significativo, mesmo após a análise do controle, passa-se, então, a etapa de avaliação dos riscos.

3.3.4 Avaliação dos Riscos

A avaliação do risco envolve a comparação do nível do risco identificado com o limite aceitável de exposição a riscos organizacional (Declaração de Apetite e Tolerância a Riscos), a fim de determinar quais decisões deverão ser tomadas.

Na prática, o limite de exposição a riscos indica o nível de risco aceitável e acima do qual é desejável o tratamento do risco, ou, até mesmo as hipóteses em que a execução do processo deverá ser evitada.

A imagem abaixo ajuda a visualizar o limite de exposição:



Nesta etapa, busca-se avaliar se os eventos de risco analisados estão dentro dos limites aceitáveis definidos pela Alta Administração e, consequentemente, se precisam ser tratados e como devem ser priorizados.

A avaliação dos riscos deve seguir, em geral, os seguintes passos:

a) identificar, na matriz probabilidade e impacto, os riscos cujos níveis estão acima do limite de exposição a risco (faixa vermelha da matriz);
b) identificar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a organização e encaminhar para decisão da Presidência;
c) os riscos cujos níveis se encontrem na faixa verde, deverão ser aceitos sem qualquer tratamento e monitorados a cada 6 (seis) meses pelo gestor;
d) os riscos cujos níveis se encontrem na faixa amarela, deverão, em regra, ser tratados (transferidos, compartilhados, mitigados ou prevenidos), se verificado bom custo-benefício pelo gestor, especialmente em se tratando de riscos de natureza financeira, à imagem ou à integridade organizacional;
e) os riscos que se encontrem na faixa vermelha, avaliar se deverão ser evitados (descontinuar o processo) ou tratados e encaminhar para decisão da Presidência; e
f) os riscos que se encontrem na faixa escura, avaliar, com máxima urgência, se devem ser evitados ou tratados e encaminhar para decisão da Presidência e ratificação pelo CSA.

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao gestor, diante da lista de riscos ordenados por nível de risco, decidir, de maneira justificada, quais merecerão ações de tratamento, de acordo com a relação custo-benefício.

3.3.5 Tratamento dos Riscos

Compreende o planejamento e a realização de ações para reduzir ou adequar o nível do risco identificado aos limites aceitos pela organização. O nível do risco pode ser modificado por meio de medidas que mitiguem (reduzam o impacto), transfiram, compartilhem ou previnam (reduzam a probabilidade) os riscos. Essas medidas de tratamento, na prática, correspondem a implantação de novos controles ou adequação dos já existentes.

O tratamento dos riscos deve seguir os seguintes passos:

a) identificar medidas de resposta ao risco (relacionar diversas opções de resposta);
b) avaliar a viabilidade da implantação das medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento);
c) decidir quais serão implementadas, balanceando o esforço de implementação e os benefícios decorrentes do controle;
d) elaborar plano de implementação das medidas para inclusão nos planos institucionais.

Assim como na etapa de identificação de riscos, esta fase de definição das medidas de resposta ao risco deve ser realizada em oficinas de trabalho com a participação de pessoas que conheçam bem o objeto de gestão de riscos, por meio de técnicas que permitam levantar, de maneira abrangente, todos os riscos (*Brainstorming*, *Delphi*, entrevistas estruturadas, visitas técnicas, etc).

São dicas que facilitam a identificação de medidas de resposta ao risco:

a) responder às seguintes perguntas-chave: que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco? Que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado? É possível adotar medidas para transferir o risco?

b) considerar as fontes e causas dos riscos – a princípio, as medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência, ou também podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize, ou uma combinação das duas abordagens;

c) na decisão quanto à implantação das medidas de resposta ao risco, considerar a quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível do risco gerado pela medida. As medidas mitigadoras podem envolver, por exemplo, a adoção de controles, o redesenho de processos, a realocação de pessoas, a realização de ações de

capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, entre outros.

A documentação desta etapa consiste no registro da descrição da medida (o que e como será realizada), do tipo de controle (aceitação, transferência, prevenção ou mitigação), e do objetivo e do resultado esperado a partir da implementação do tratamento.

3.3.6 Monitoramento

O monitoramento compreende a verificação do desempenho da medida de controle adotada, a fase da execução do controle (planejamento, execução e concluído) e a situação atualizada (no prazo ou atrasada), além de outras informações gerenciais básicas, dentre as quais: a área e o profissional responsável, quando se inicia e termina a medida de controle e o resultado obtido após a implementação do tratamento.

A finalidade desta etapa é produzir informação confiável e tempestiva para a gestão dos riscos da organização, de maneira que decisões possam ser tomadas em tempo para que os objetivos organizacionais não sejam comprometidos por riscos não gerenciados.

O monitoramento tem três dimensões:

a) o funcionamento do Sistema de Gestão de Riscos do TCE-RO (avaliar em que medida o sistema funciona e o que deve ser aperfeiçoado);
b) a implementação e os resultados do tratamento de riscos (avaliar se as medidas de controle implementadas funcionam e quais precisam ser aperfeiçoadas ou substituídas);
c) a evolução do nível dos riscos que não mereceram tratamento por parte do gestor (avaliar se outros riscos precisam ser tratados).

O monitoramento do funcionamento do Sistema de Gestão de Riscos está a cargo do Conselho Superior de Administração (CSA) e da Alta Administração do Tribunal de Contas do Estado de Rondônia.

As ações de monitoramento dos riscos estão a cargo do gestor de riscos, cabendo à Presidência, ao CAAD e aos Secretários a supervisão, sem prejuízo da Corregedoria poder avaliar o adequado funcionamento desta etapa e recomendar melhorias no sistema e nos instrumentos de gestão.

Caso deficiências ou vulnerabilidades sejam identificadas nas medidas de tratamento dos riscos, os gestores deverão reavaliar os controles e comunicar à CAAD, com as devidas justificativas.

Além disso, cabe aos gestores de risco detectar mudanças no contexto e promover as revisões necessárias tanto sobre os tratamentos realizados quanto sobre os riscos emergentes, de maneira a assegurar eficiência e efetividade aos controles.

É importante ressaltar que as atividades de monitoramento e as análises críticas devem assegurar que os riscos e as medidas de controle sejam atualizadas.

3.3.7 Comunicação

Refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos.

Comunicar riscos é fornecer as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados pelo risco. Em outras palavras, comunicar é dar ciência da existência e do tratamento dos riscos para as pessoas que tenham interesse, que podem ser impactadas, que atuam ou podem influenciar na gestão do risco, ou mesmo, que dependem das informações para tomada de decisão.

Podemos dividir esse fluxo de comunicação em duas direções: vertical e horizontal. A comunicação vertical ocorre no sentido da base para a cúpula ou vice-versa, proporcionando aos destinatários, dentro de suas respectivas competências e poderes, informação indispensável à tomada de decisão.

Por sua vez, a comunicação horizontal é importante para que os riscos de um processo que envolva diferentes unidades sejam conhecidos igualmente por todos para solução integrada do risco.

Nessa fase, algumas informações produzidas nas etapas de identificação, análise, avaliação e definição do tratamento são essenciais, dentre as quais sobre: nível, categoria; abrangência; e resultado do controle, pois a partir delas o fluxo de informação e comunicação seguem caminhos distintos, como se vê a seguir.

Algumas premissas ajudam na compreensão dessa etapa:

a) os riscos baixos (verde) apenas serão monitorados nos ciclos semestrais de avaliação e não serão controlados pela 2ª linha;
b) os riscos altos (vermelho) deverão ser reportados à Presidência, a quem caberá decidir sobre a medida de controle sugerida pela 1º linha;
c) os riscos catastróficos (escuro) deverão ser levados ao CSA para ciência e ratificação;
d) os riscos multisetorias e/ou institucionais deverão ser compartilhados entre os setores envolvidos para definição das diretrizes gerenciais.

Em síntese, a etapa de comunicação é essencial para que as informações sejam compartilhadas dentro da organização para as pessoas certas, da maneira certa e no tempo certo, entre as instâncias de execução, supervisão e decisão nas três linhas de defesa, de acordo com a Política de Gestão de Riscos do Tribunal de Contas de Rondônia.

3.3.8 Melhoria contínua

Compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento. A melhoria contínua pode ser entendida em duas dimensões: uma relativa ao próprio Sistema de Gestão de Riscos do TCE-RO, a cargo da Alta Administração; e outra relacionada aos resultados do monitoramento sobre a efetividade do tratamento do risco, a cargo dos gestores de risco.

4. RESPONSABILIDADES-CHAVE DO PROCESSO

As responsabilidades de todos os agentes envolvidos no processo de gerenciamento de riscos estão definidas na Política de Gestão de Riscos do Tribunal de Contas de Rondônia. Aqui serão destacadas apenas algumas funções-chave essenciais para a rotina de gestão de riscos.

4.1 Gestor de Riscos

O gestor deverá gerenciar os riscos da unidade sob sua responsabilidade, considerando as seguintes dimensões:

a) riscos como subsídio para tomada de decisão quanto à inclusão ou não de ações em planos institucionais;
b) riscos referentes a ações e metas previstas nos respectivos planos institucionais;
c) riscos relacionados às entregas que cabem à unidade, conforme previsto no rol de suas atribuições e competências;
d) riscos que comprometam o funcionamento da unidade.

Sob a ótica do processo de planejamento, na definição de estratégias e ações, deverão ser considerados os riscos como parte do processo decisório para sua inclusão ou não no plano.

Depois de definidas as ações que farão parte do plano da unidade, as respectivas medidas mitigadoras para esses riscos também farão parte do plano.

A identificação dos riscos da unidade, das estratégias e das ações será realizada de acordo com a metodologia de planejamento do Tribunal.

Se o dirigente da unidade identificar algum risco que possa ser caracterizado como risco-chave para o TCE-RO, a partir de critérios pré-definidos, deverá informar à CAAD e ao titular da respectiva unidade básica.

4.2 Gestor da Área

Espera-se que o gestor da área supervisione os riscos setoriais e atue como patrocinador da gestão de riscos. A atuação do gestor da área é fundamental para que a cultura de *accountability*, transparência e controles seja internalizada por sua equipe, visando a produção de informações indispensáveis para a gestão do setor e assegurar razoável segurança ao alcance dos objetivos da área. Isso inclui, dentre outras ações, o acompanhamento da evolução da gestão de riscos nas unidades e das medidas de tratamento adotadas pelos gestores dos riscos.

4.3 CAAD

A CAAD definirá, em conjunto com os gestores de riscos, critérios para priorização dos processos que deverão ser objeto de gestão de riscos, considerando a transversalidade e o impacto desses processos nos objetivos estratégicos do Tribunal.

A partir dos processos priorizados, a CAAD e os responsáveis pelo processo definirão a equipe que irá participar do processo de identificação dos riscos e das medidas mitigadoras (quantidade, perfil, lotação etc.).

A gestão dos riscos em processos de trabalho deverá seguir as etapas descritas neste Manual.

Possíveis riscos-chave, identificados a partir de critérios definidos previamente, deverão ser informados ao dirigente da unidade ou da unidade básica, conforme o caso, e à CAAD.

Os riscos-chave deverão ser monitorados pela CAAD e acompanhados pelo Gestor da Área.

4.4 Corregedoria

A Corregedoria realizará trabalhos de avaliação do Sistema de Gestão de Riscos por amostragem para verificar a adoção das boas práticas exigidas, cabendo-lhe reportar ao Conselho Superior de Administração os achados relevantes.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR ISO 31000: Gestão de Riscos: Princípios e Diretrizes. Rio de Janeiro, 2009.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Manual de gestão de integridade, riscos e controles internos da gestão. Brasília, Assessoria Especial de Controle Interno, 2017. Disponível em: http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc . Acessado em 16/04/2019.

_____._____. Método de Priorização de Processos. Brasília, 2017. Disponível em . Acesso em: fevereiro 2018.

_____. _____ e Controladoria-Geral da União. Instrução Normativa Conjunta Nº 1, de 10 de REFERÊNCIAS Tribunal de Contas da União | 81 maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, 2016. Disponível em . Acesso em: maio 2016.

_____. Tribunal de Contas da União. Referencial básico de gestão de riscos. Brasília, Secretaria Geral de Controle Externo, 2018. Disponível em: www.tcu.gov.br . Acessado em 16/04/2019.

_____. _____. Referencial básico de governança aplicável a órgãos e entidades da administração pública. Versão 2. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2014. Disponível em: . Acesso em: março, 2017.

CADBURY, A. *Report of the Committee on the financial aspects of corporate governance*. Londres: *Gee and Company Ltd*, 1992. Disponível em: . Acesso em: maio, 2016.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA - IBGC. Guia de Orientação para Gerenciamento de Riscos Corporativos (2007).

INTERNATIONAL FEDERATION OF ACCOUNTANTS - IFAC. Governance in the public sector: a governing body perspective. International public sector study nº 13, 2001.

INTOSAI (International Organization of Supreme Audit Institutions). Subcomitê de Normas de Controle Interno. Diretrizes para Normas de Controle Interno do Setor Público – Informações Adicionais sobre Gestão de Risco nas Entidades. INTOSAI GOV 9130. Viena, 2007. Tradução: Antonio Alves de Carvalho Neto. Brasília, 2013.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT - OCDE. Avaliação da OCDE sobre o sistema de integridade da Administração Pública Federal Brasileira: Gerenciando riscos por uma administração pública mais íntegra. Sumário Executivo. OCDE, 2011.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. Controle Interno: Estrutura Integrada: Sumário Executivo e Estrutura. Tradução: PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2013.

_____. Gerenciamento de Riscos Corporativos: Estrutura Integrada: Sumário Executivo e Estrutura (COSO GRC, 2004). Tradução: REFERÊNCIAS Tribunal de Contas da União | 83 PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2007.

GLOSSÁRIO

Gestor setorial de gestão de riscos: pessoa ou unidade responsável por coordenar ações e promover a execução do SGR/TCE-RO no âmbito da unidade básica a que se vincula, prover informações à unidade central, bem como apoiar os dirigentes e os gestores de riscos no desempenho das competências.

Evento: um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.

Gestão de riscos: atividades coordenadas para dirigir e controlar a organização no que se refere a riscos e oportunidades.

Gestor de risco: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco.

Nível do risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e seu impacto nos objetivos.

Objeto de gestão de riscos (objeto de gestão): qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos do TCE-RO.

Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos.

Risco: possibilidade de que um evento afete negativamente o alcance de objetivos.

Risco-chave: risco que, em função do impacto potencial ao TCE-RO, deve ser conhecido pela alta administração.

Sistema de Gestão de Riscos do Tribunal de Contas do Estado de Rondônia (SGR/TCE-RO): consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, a implementação, o monitoramento e a melhoria contínua da gestão de riscos na organização e compreende, entre outros: política, estruturas organizacionais, planos, relacionamentos, responsabilidades, atividades, processos e recursos.