CONTROLADORIA | PREFEITURA BELO HORIZONTE
GOVERNANDO PARA QUEM PRECISA

GUIA DE GERENCIAMENTO DE RISCOS APLICADO AO SETOR PÚBLICO

CTGM
Controladoria-Geral do Município de Belo Horizonte

SUTRANSP
Subcontroladoria de Transparência e Prevenção à Corrupção

DICC
Diretoria de Integridade, Prevenção e Combate à Corrupção

2021

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
- Carolina Cruz Quintão
- Daniela de Melo Vieira
- Fernanda de Lacerda Costa
- Gisele Leite Lima
- Manoel Tolentino Oliveira
- Márcia Cristina Garcia Pessoa
- Marcus Vinícius Araújo Murad
- Maurício Dias Batista Filho

Belo Horizonte, novembro de 2021

INTRODUÇÃO

As organizações existem para gerar valor, considerando os seus objetivos e os resultados percebidos pelos seus usuários e demais partes interessadas. No entanto, diversas situações adversas, desconhecidas ou incertas podem ocorrer durante seu caminho. Conhecer os problemas e riscos significativos e gerenciá-los aumentam as chances de atingimento dos propósitos organizacionais, além de favorecer uma governança responsável e transparente. O gerenciamento de riscos possibilita aos administradores tratar com eficácia essas incertezas de forma a aprimorar a capacidade de geração de valor à sociedade (COSO ERM).

O setor público apresenta aumento constante na complexidade da sua administração, em decorrência do número e diversidade de usuários, dos vários instrumentos normativos, das mudanças constantes das políticas públicas e das novas necessidades da sociedade. Gerenciar riscos de maneira estruturada se tornou uma necessidade de todos os agentes públicos com vista a realizar seus trabalhos de maneira mais fundamentada, profissional e com compromisso com os recursos e resultados gerados à população.

Visando maior objetividade na sua aplicação, esse Guia se propõe a apresentar o gerenciamento e a gestão de riscos de maneira focada nos objetivos institucionais, a partir de uma visão clara e intuitiva do porquê gerir riscos de maneira estruturada nos ambientes governamentais.

O gerenciamento de riscos aborda o processo de identificar, analisar, tratar e monitorar problemas e riscos, enquanto a gestão de riscos está direcionada à preparação do ambiente e da estrutura organizacional para a aplicação do gerenciamento de riscos.

A gestão e o gerenciamento de riscos devem ser aplicados considerando o ambiente e contexto de cada organização. Cada organização também tem um nível de maturidade de riscos. Algumas estão em um estágio mais avançado no gerenciamento e na cultura de riscos, enquanto outras se encontram em momento incipiente nesse tema. Independente das diferentes maturidades, todas podem e devem iniciar o gerenciamento de riscos e se favorecerem de uma ferramenta de governança importante para o suporte na tomada de decisão e na *accountability* pública. O importante é iniciar sua plataforma de gerir riscos e evoluir gradualmente, em um movimento de melhoria contínua.

"*Comece onde você está, use o que você tem e faça o que você puder*" (Arthur Ashe).

Gerir e gerenciar riscos é um processo estruturado, institucionalizado e evolutivo, que deve refletir o compromisso da alta administração na criação de uma cultura generalizada de riscos dentro da organização.

Para se modernizarem, as organizações necessitam de novos objetivos e, consequentemente, novos riscos. Riscos não devem ser temidos e sim gerenciados. Os gestores devem considerar o custo/benefício em assumir riscos, atuais ou potenciais.

No próximo tópico, serão apresentados os conceitos essenciais dos riscos, incluindo uma breve contextualização no ambiente organizacional. Na seção seguinte, será indicado o roteiro prático para o gerenciamento de riscos, que inclui a identificação, análise, tratamento e monitoramento. Posteriormente, será tratada da gestão de riscos, que aborda as providências preliminares para se incorporar o gerenciamento e a cultura de riscos no ambiente organizacional, incluindo apoio da alta administração, políticas e papeis.

RISCO

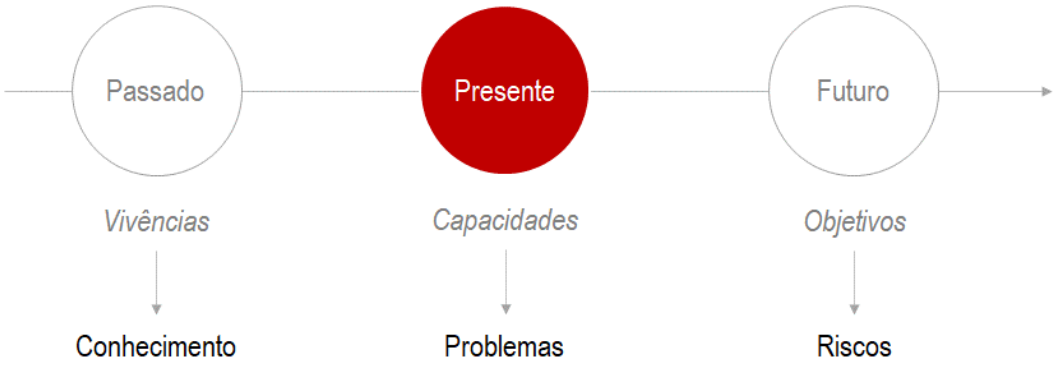
De maneira geral, podemos conceituar risco como qualquer circunstância (evento, desvio, omissão etc.), desconhecida ou incerta, que possa impactar o atingimento de objetivos[1].

Na administração pública, há objetivos de toda a ordem, como normativos a serem cumpridos, protocolos técnicos, objetivos estratégicos, metas do PPAG (Plano Plurianual de Ação Governamental) e da LOA (Lei Orçamentária Anual), programas, projetos, ações governamentais, plano de governo, princípios de governança pública, dentre outros. Entender e organizar esses objetivos e os obstáculos que se têm, ou pode ter, para cumpri-los é parte fundamental e até óbvia do trabalho.

Podemos considerar que esses obstáculos se traduzem em problemas atuais (adversidades nas capacidades organizacionais) e riscos futuros (ameaças que possam limitar o atingimento planejado dos objetivos), conforme a figura abaixo. De forma geral, podemos ter que os problemas (obstáculos atuais) são riscos que se materializaram e se tornaram reais.

Assim, ao abordar o gerenciamento de riscos, este Guia de Referência abrange tantos os riscos futuros quando os riscos já concretizados, que se tornaram problemas relevantes e impactantes nos objetivos organizacionais.

Figura 1 - Momentos organizacionais



Fonte: CTGM

Objetivos são sempre projetados no futuro. Mesmo que se tenha a intenção de que uma determinada situação continue como está, ainda assim, temos um objetivo (futuro) de mantê-la dessa forma.

Gerenciar riscos (que já se materializaram, ou ainda não) é aumentar as chances de se atingir objetivos; e esse gerenciamento também faz uso de conhecimentos e experiências

[1] *Há diversos conceitos em que o risco é definido como um desvio (risco é o efeito da incerteza nos objetivos – ISO 31.000, 2018), como uma chance de algo dar errado (risco é a possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos (COSO ERM, 2017) ou como um evento incerto (risco é um evento ou condição incerta que, se ocorrer, tem um efeito em pelo menos um objetivo do projeto (PMBOK 5 ed.). No entanto, o importante é tentarmos identificar quaisquer um desses fatores que possam influenciar nos objetivos.*

de situações e eventos passados da organização, que auxiliam na identificação de novas questões nocivas aos propósitos organizacionais.

Essas incertezas (futuras) podem ser tanto positivas, quanto negativas para os objetivos. No primeiro caso, são chamadas de oportunidades (riscos positivos), e, no segundo, ameaças (riscos negativos). O escopo deste guia contemplará apenas os riscos negativos, ou ameaças.

Apesar de terem um viés abstrato, já que são incertezas (futuras), os riscos organizacionais podem ser exprimidos pela combinação da sua chance de ocorrer (probabilidade) e por suas consequências diretas nos objetivos, caso ocorram (impactos). Essa combinação é chamada de **nível de risco** e é representada como:

Nível de Risco = Probabilidade x Impacto

Tanto a probabilidade, quanto o impacto podem fazer uso de escalas graduais para indicarem as suas intensidades no nível de risco. Podem ser usadas escalas de quaisquer quantidades de pontos (divisões). No entanto, sugerimos a escala de 5 pontos para reduzir a quantidade de "empates" nos níveis finais dos riscos. Dessa forma, haverá uma escala de 5 pontos para as probabilidades e outra de 5 pontos para os impactos.

Figura 2 - Escala de graduação das probabilidades e impactos

Fonte: CTGM

Há a possibilidade de usar teorias estatísticas e probabilísticos para mensurar as chances de ocorrência e os possíveis impactos nos objetivos, mas para nosso propósito, as escalas graduadas são mais comuns.

O gerenciamento de riscos deve trabalhar com um limite de nível de risco aceitável. Esse limite é denominado **apetite a riscos**, o qual indica 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 geração de valor aos usuários (COSO ERM)[2].

Para os casos de problemas, ou seja, riscos materializados, já se tem a certeza de sua ocorrência, é um fato. Para esses casos, usaremos o grau mais intenso na escada das probabilidades; ou seja, 5.

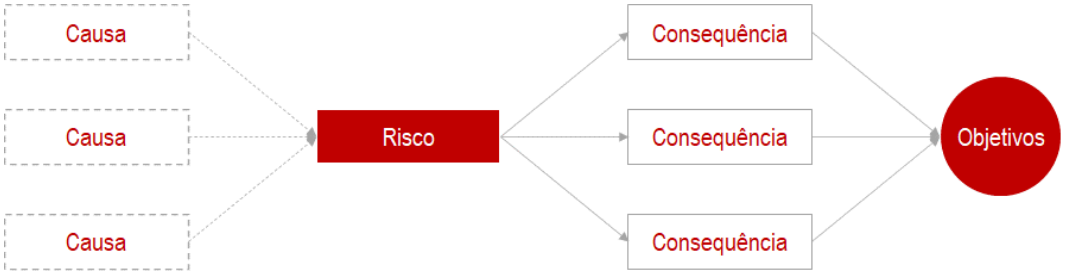
Riscos também podem ter probabilidade 5 e isso acaba por generalizar esse grau tanto para situações certas (problemas) quanto incertas (riscos). Esse viés não prejudica o processo de gerenciamento de riscos (e problemas), pois haverá uma outra informação para distinguir essas duas situações.

[2] *Há terminologias que diferem apetite a riscos e tolerância a riscos. Esse Guia tratará esses conceitos como sinônimos.*

Outra característica dos riscos e problemas é que normalmente eles têm uma ou mais **causas** e pode gerar uma ou mais **consequências** negativas nos objetivos. Esses elementos são chamados de **componentes** do risco.

A disposição dos componentes pode ser representada em uma estrutura denominada *bow-tie* (gravata borboleta), como apresentado abaixo.

Figura 3 - Componentes do risco



Fonte: CTGM.

Basicamente, esses são os conceitos básicos que envolvem riscos e que são necessários para o gerenciamento proposto nesse Guia. A seguir, será apresentado o processo de gerenciamento de riscos e a gestão de riscos, que são providências e ações preliminares ao gerenciamento para preparar a organização para a adoção, efetivação e integração do gerenciamento de riscos na governança da administração pública.

GERENCIAMENTO DE RISCOS

O gerenciamento de riscos representa as etapas para identificar, analisar e tratar os riscos e problemas organizacionais. Além de incluir as ações de monitoramento e de melhoria contínua do processo.

Figura 4 - Etapas do gerenciamento de riscos

Fonte: CTGM

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. O gerenciamento de riscos é melhorado continuamente por meio de aprendizado e experiências (ISO 31000).

O gerenciamento 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 todas as etapas podem e realmente influenciam as demais (COSO ERM).

A seguir, as etapas serão detalhadas para melhor compreensão das atividades que envolvem o processo de gerenciamento de riscos.

Etapa 1 - Identificação

Objetivos da etapa:
- Descobrir problemas e riscos que possam afetar significativamente os objetivos organizacionais

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

> *Na identificação, podem surgir inúmeras questões que se caracterizam como problema ou risco, mas, sugere-se que sejam relatadas aquelas que possam impactar os objetivos de maneira relevante e que tenham chances razoáveis para ocorrer.*

A identificação pode ser realizada de diversas formas. Uma das mais adequadas e rápidas é a reflexão (reuniões, entrevistas, questionários, *brainstorming* etc.), em conjunto com pessoas que conheçam o histórico, as experiências e também a rotina do trabalho, suas vulnerabilidades, inseguranças, inconformidades, dentre outras debilidades. Além dessas reflexões, outras técnicas são apresentadas a seguir:

- **Análise SWOT** - Análise dos ambientes internos e externos da organização, buscando identificar problemas e 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 da cadeia de valor[3] e do fluxo dos processos, procurando encontrar situações de vulnerabilidades, inseguranças ou instabilidades. A análise de cenário pode ser aplicada em um nível mais superficial, ao avaliar os elementos organizacionais mentalmente, ou então utilizar mapeamentos e diagramas 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)

[3] *A cadeia de valor10 enfatiza a captura de processos e atividades que adicionam valor ao serviço ou produto entregue ao cidadão e à sociedade. 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 valor11 (BPM CBOK, 2013).*

Etapa 2 - Análise

Objetivos da etapa:

- Entender as causas, eventos e consequências dos riscos
- Priorizar os riscos a partir dos seus níveis, que são obtidos pela multiplicação de cada grau de probabilidade e de impacto

Após a identificação dos principais problemas e riscos, eles devem ser analisados, buscando-se conhecê-los de forma mais detalhada. Aqui, serão definidos os componentes (causas e consequências) e os níveis dos riscos (probabilidade x impacto).

As causas são os pontos focais de tratamento para mitigação dos riscos, de forma que as ações sejam efetivas e não incorram em medidas paliativas e temporárias.

Uma sugestão para a distribuição dos componentes (causa ⇨ risco/problema ⇨ consequência) é utilizar a seguinte **sintaxe** para posicionamento desses elementos:

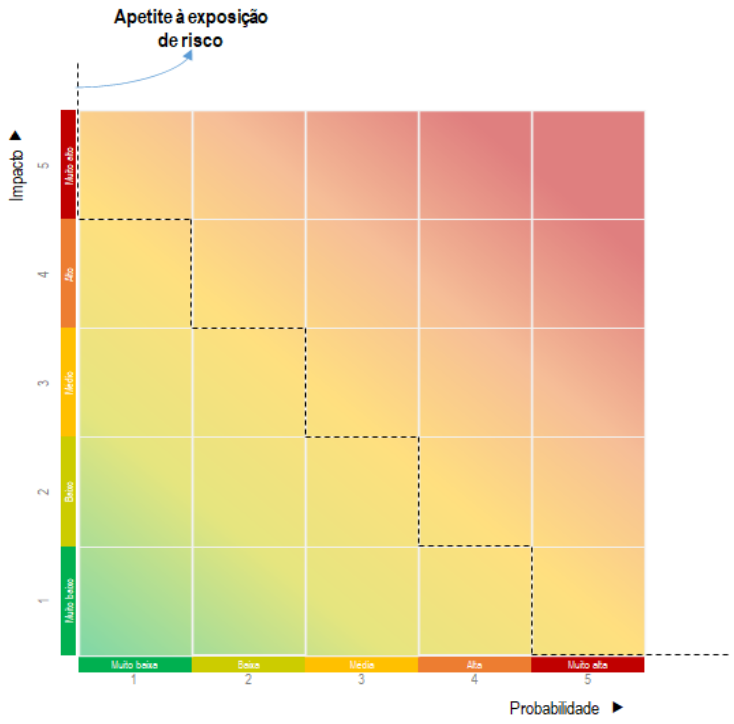
Devido às <CAUSAS>, poderá acontecer <DESCRIÇÃO DO RISCO>, o que poderá levar a <DESCRIÇÃO DAS CONSEQUÊNCIAS>, impactando no <OBJETIVO >

Fonte: ENAP (2018).

Os problemas e riscos devem ser ordenados de forma decrescente (maiores níveis em primeiro) para que essa lista retrate a priorização, *a priori*, dos riscos a serem tratados.

Cada risco, após atribuídos, suas probabilidades e impactos pode ser projetado em uma **matriz de risco**, ou matriz de calor, para melhor exame da sua disposição em um plano que possibilite a comparação entre si.

Figura 5 - Matriz de riscos



Fonte: CTGM

A matriz de riscos tem o propósito de apresentar o arranjo dos riscos conforme suas probabilidades e impactos e a região de plotagem representa uma graduação de gravidade do risco indo do vermelho (mais grave) para o verde (menos grave). Na figura acima, também é evidenciado um traço, que representa um hipotético apetite a riscos (hipotético pois cada organização define a sua, sem, necessariamente, ter os limites mostrados na figura).

Na próxima etapa, os níveis de risco serão avaliados. Aqueles que estiverem acima do apetite a riscos previamente estabelecido, deverão ter um tratamento definido, ou uma justificativa plausível para uma eventual decisão contrária.

Etapa 3 - Tratamento

Objetivos da etapa:
- Verificar os riscos acima do apetite (limite de nível tolerável)
- Atribuir as respostas aos riscos acima do apetite
- Definir o plano de ação com as medidas a serem tomadas para aprimorar os controles, responsáveis por essas medidas e estimativas de prazos e custos

Na etapa passada, os riscos foram "dissecados" em causas e consequências, para se entender o fluxo de desdobramentos que possam impactar os objetivos; e em probabilidade e impacto, para se definir o nível de cada risco, a fim de ordená-los e priorizá-los conforme esses níveis.

Aqui, será utilizado um "corte" que representa o apetite ao risco. O apetite a riscos é um limite de aceitação de riscos e pode ser configurado conforme a necessidade da organização; podendo ser um índice geral ou se cada área ou atividade terá um apetite específico, por exemplo. Os riscos posicionados acima dessa fronteira deverão ter respostas que indicarão se haverá controles para a sua mitigação, ou uma justificativa em caso de outra decisão que não seja a implementação ou aprimoramentos de controles internos para sua mitigação.

A finalidade é que ocorram tratamentos de riscos até que seus níveis fiquem dentro do apetite (abaixo do limite aceitável).

De forma mais detalhada, as respostas ao risco acima do apetite são:

1. **Mitigar** - A mitigação ocorrerá em casos de intervenções nas probabilidades e/ou nos impactos mediante a implantação ou aprimoramento ou criação 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. Determinados riscos podem já estar em processo de mitigação. Nesse caso, basta indicar o andamento no plano de ação e o progresso dessas frentes de trabalho.
2. **Transferir** - 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, concessões públicas, acompanhantes em internações hospitalares etc.
3. **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).
4. **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.

Comumente parte significativa dos tratamentos de riscos não envolvem custos adicionais, necessitando, ao invés disso, planejamento e execução.

Com exceção de "aceitar", as demais respostas a riscos demandam um plano de ações para as medidas de tratamento de cada risco acima do apetite. Basicamente esse plano deve conter:

- **Medidas de tratamento** – criação de novos controles ou melhoria de controles internos já existentes que visem a redução da probabilidade e/ou impacto dos efeitos dos riscos, caso se materializem.
- **Responsável** – Pessoa que irá conduzir e responder pelas medidas de tratamento. Sugere-se que uma única pessoa seja definida como responsável, mesmo que haja mais pessoas atuando no tratamento.
- **Prazo** – Data prevista para término das implementações das medidas de tratamento. Sugere-se que seja uma data específica (dia, mês e ano).
- **Custo** – Previsão de gastos extras demandados pelas medidas de tratamento. Aqui devem ser considerados os custos que não já façam parte dos gastos usuais da organização (custeio).
    - O custo deve ser estimado em uma escala de 1 a 5, onde 1-sem custos adicionais; 2-baixo; 3-médio; 4-alto e 5-indefinido (há altos custos, mas sem estimativa de sua magnitude).

Para eventuais casos de materialização de riscos que possam trazer danos passíveis de custos para as suas correções, recuperações ou indenizações, a organização deve prover, além do plano de ações para tratamento de riscos, um **plano de contingência**, o que pode incluir medidas de redução de danos ou fundos destinados para esse fim. O plano de contingência inclui providências previamente definidas para os casos de materialização dos riscos que necessitem de remediação ou correção dos possíveis danos.

Etapa 4 - Monitoramento

Objetivos da etapa:

- Verificar se as medidas do plano de ação (controles) estão surtindo efeitos esperados
- Corrigir ou revisar a medidas do plano de ação, se necessário
- Identificar novos riscos
- Registrar e implementar melhorias continuadas no processo de gerenciamento de riscos

Dentre uma de suas finalidades, a etapa de monitoramento busca avaliar se os efeitos dos controles definidos para o tratamento dos riscos estão sendo eficazes de forma a mitigar a probabilidade e/ou o impacto das ameaças. Além disso, o monitoramento também deve observar a descoberta de novos problemas e riscos relevantes, para serem inseridos no gerenciamento e as oportunidades e sugestões de aprimoramento continuado no processo de gerenciamento de riscos, visando a melhoria das etapas, das experiências em riscos pelos atores, das comunicações entre os envolvidos e no maior suporte à tomada de decisões pelo corpo diretivo.

A partir do monitoramento, o gerenciamento de riscos inicia um fluxo contínuo das etapas, revisitando-as de forma a fazer com que o processo seja internalizado, ampliado e aperfeiçoado na organização.

GESTÃO DE RISCOS

O gerenciamento de riscos estruturado deve ser aplicado gradualmente por todos os gestores (e servidores) da organização. O incentivo, a preparação do ambiente, da estrutura e da metodologia a ser aplicada, além das pessoas-chave que conduzirão o processo devem fazer parte de um momento anterior ao gerenciamento, denominado **gestão de riscos**.

A gestão de riscos inclui a política de riscos da organização, seu apetite à exposição aos riscos e todos os recursos necessários ao gerenciamento estruturado e institucionalizado dos problemas e riscos.

Espera-se que todos recebam 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.

Apoio da alta administração

Comprometimento e acompanhamento

De antemão, a alta administração deve se conscientizar da importância do gerenciamento de riscos e fomentar, de forma efetiva, a sua implementação em todos os níveis organizacionais. O apoio da alta administração é, assim, condição necessária ao êxito do processo. O apoio não deve ocorrer apenas nas fases iniciais do gerenciamento de riscos. Ao invés disso, o acompanhamento constante para que a cultura de riscos seja institucionalizada e que agregue valor à governança é fundamental para que os resultados desse instrumento sejam úteis e perceptíveis pelo corpo diretivo.

Alinhamento com o corpo diretivo

Toda a cadeia de comando da organização deve estar envolvida no movimento para se empregar o gerenciamento de riscos na organização. Iniciativas para capacitações, oficinas, orientações e estimulação constante devem ser empregadas para que o gerenciamento de riscos possa cobrir todo o ambiente organizacional possível.

Promoção do gerenciamento de riscos na tomada de decisões

Os resultados do gerenciamento de riscos devem ser usados como parâmetro na tomada de decisões em todos os níveis da organização. Gradativamente, eles se revelarão mais úteis e serão uma espécie de bússola que orientará os gestores nas análises de cenário e na escolha das melhores alternativas, considerando as circunstâncias de cada momento. Nesse sentido, o gerenciamento de riscos dá suporte ao *accountability* público (prestação de contas) e à governança transparente, responsável e participativa.

Estrutura

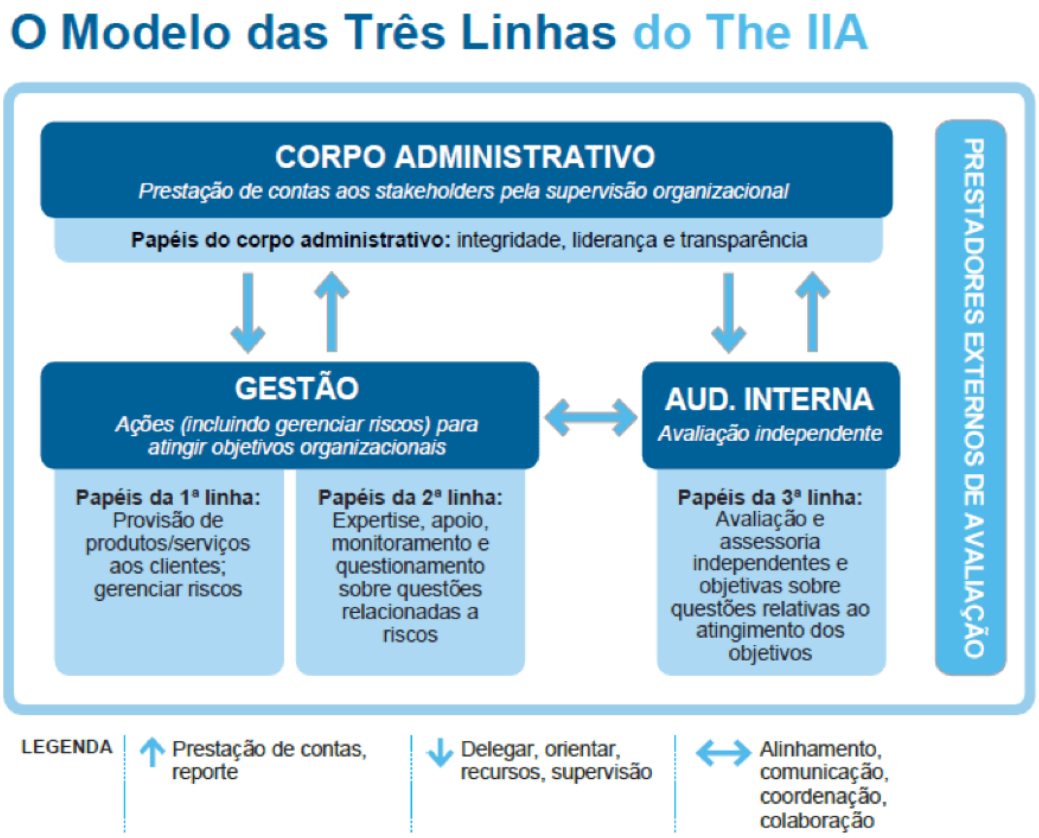
Equipe de referência em gerenciamento de riscos

Antes de iniciar o gerenciamento de riscos, sugere-se que sejam designados servidores para organizar e desenvolver a metodologia de processo na organização. Além disso, essa equipe pode trabalhar na intermediação das consolidações de dados e reportes de relatórios e informações.

As três linhas da gestão de riscos

O gerenciamento de riscos, como já dito anteriormente, envolve as etapas de manejo dos problemas e riscos organizacionais. Esse processo pode e deve ser adotado em todos os níveis organizacionais a partir de uma metodologia padronizada, capaz de empregar uma mesma linguagem, modelo e política de riscos. Para melhor organizar esse arranjo, é proposto o modelo das três linhas desenvolvido pelo The Institute of Internal Auditors (The IIA).

Figura 6 - O modelo das três linhas da gestão de riscos



Fonte: IIA (2020)

O modelo das três linhas propõe que o gerenciamento de riscos seja realizado pela primeira linha, enquanto a segunda linha daria suporte a esse processo. A terceira linha é representada pela auditoria interna para que se tenha avaliação e assessoria independente, quando necessário.

Todas as linhas devem reportar informações ao corpo diretivo (alta administração e demais gestores), que devem conduzir a governança organizacional com integridade, liderança e transparência[4].

Diretrizes

Política de gestão de riscos

Documento formal que deve ser publicado pela organização contendo principais definições de gestão e gerenciamento de riscos utilizadas na instituição, diretrizes, prazos de implementação do gerenciamento de riscos, estrutura, delegações, produtos esperados dentre outras informações pertinentes às orientações de como o gerenciamento de riscos deve ser estruturado e institucionalizado.

Apetite a riscos

A gestão de riscos deve disponibilizar, a partir de decisão da alta administração, qual o apetite a riscos a ser usado no gerenciamento de riscos. Esse parâmetro é importante pois é o limite julgado pertinente para os riscos terem planos de ação para o seu tratamento de mitigação.

Plano e fundos de contingência

Espera-se que os riscos sejam gerenciados e controlados de forma a não gerarem danos à organização, às pessoas ou a outros ativos. No entanto, nem sempre esse gerenciamento consegue cobrir todos os casos, seja devido à falta da descoberta de problemas e riscos, a erros de estimativas ou em razão da relação custo-benefício. Para esses casos em que os riscos se concretizem e gerem danos que devam ser corrigidos ou atenuados, quando possível, pode ser definido um plano de contingência e criado fundo de recursos para essas remediações. Essa decisão deve ser tomada pela alta administração e divulgada na gestão de riscos.

Metodologia

A metodologia de gerenciamento de riscos exprime, principalmente, o *modus operandi* para que os gestores possam contar com métodos, padrões e controles para identificar, analisar, tratar, monitorar e divulgar os problemas e riscos. Há padrões disponíveis como o COSO ERM, ISO 31.000, PMBOK, Orange Book, dentre outros que buscam orientar a gestão e gerenciamento de riscos. No entanto, essas fontes devem ser adaptadas de acordo com as realidades e necessidades de cada organização.

A metodologia também deve dispor de orientações para a elaboração do **Plano de Gestão de Riscos**, que é o documento que consolida as informações resultantes do gerenciamento de riscos como sendo o principal meio de comunicação do gerenciamento com o corpo diretivo e a organização como um todo.

Convém que a metodologia disponha de aferições periódicas da **maturidade da gestão de riscos** da organização visando acompanhar a evolução do processo de gerenciamento e de abrangência da cultura de riscos.

---

[4] *Para maiores informações sobre a nova versão (2020) do modelo das três linhas, consultar: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf*

REFERÊNCIAS

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.

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.

Implementando a gestão de riscos no setor público (módulo 3). Escola Nacional de Administração Pública (ENAP). Disponível em: *https://repositorio.enap.gov.br/bitstream/1/4090/1/ Modulo%203-Ciclo%20de%20 Gerenciamento%20de%20Riscos.pdf*. Brasília, 2018.

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.

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

Metodologia de gestão de riscos da CTGM. Controladoria-Geral do Município de Belo Horizonte. 2018.

Modelo das Três Linhas do The IIA. The Instutute of Internal Auditors. 2020

Orange Book. Governo do Reino Unido. Disponível em https://www.gov.uk/government/publications/orange-book

Risco. Tribunal Regional do Trabalho do Paraná (TRT4). Disponível em https://www.trt9.jus.br/pds/index.htm

ROTEIRO PARA GESTÃO E GERENCIAMENTO DE RISCOS

GESTÃO	Apoio da alta administração		**Comprometimento e acompanhamento** Sem o apoio, comprometimento e acompanhamento da alta administração o gerenciamento de riscos terá seus efeitos reduzidos significativamente. **Alinhamento com corpo diretivo** Todos os gestores devem atuar para colocar o gerenciamento de riscos em prática e buscar aprimoramento contínuo. **Promoção do gerenciamento para a tomada de decisões** O gerenciamento de riscos deve ser adotado como uma ferramenta para análise de alternativas.
	Estrutura		**Equipe de referência em gerenciamento de riscos** Escolha de pessoas para organizar, definir a metodologia, disseminar, consolidar, realizar comunicação com o corpo diretivo e serem referências para dúvidas e orientações sobre o processo de gerenciamento de riscos. **Linhas de defesa** As linhas de defesa procuram organizar as funções e comunicações no gerenciamento de riscos. A primeira linha representa a aplicação prática do gerenciamento de riscos em todos os setores da organização. A segunda linha dá apoio à primeira mediante opiniões e orientações especializadas. A terceira linha procura avaliações e pareceres isentos da auditoria interna. Todas elas devem manter comunicação entre si, bem como com os demais níveis administrativos.
	Diretrizes		**Política de gestão de riscos** Documento formal e amplamente divulgado na organização com as diretrizes básicas da gestão e do gerenciamento de riscos, além do compromisso da alta administração. **Definir o apetite a riscos** Nível a partir do qual, todos os riscos deverão ter um tratamento ou justificativa plausível para o contrário. **Definir se haverá plano e fundos de contingência** Definição se haverá recursos extras destinados a correções e indenizações, para os casos de materialização de riscos que envolvam danos elegíveis de responsabilizações legais **Metodologia** Manual com a forma que a organização deverá gerenciar seus riscos, considerando sua área de atuação, temas críticos e públicos-alvo.
GERENCIAMENTO	Identificação	1	Realizar atividades para **descobrir problemas e riscos** relevantes e capazes de prejudicar o atingimento dos objetivos organizacionais. Para levantamento dos riscos de integridade, é disponibilizado modelo específico. Lançar todos os problemas e riscos identificados e relevantes na planilha. Modelo "MODELO 1 - Identificação de riscos de integridade" Planilha, colunas "Data da identificação" e "Risco/Problema"
	Análise	2	Analisar os problemas e riscos, buscando apontar suas **causas e consequências** diretas nos objetivos organizacionais. Lançar as causas e consequências respectivas na planilha, para cada problema e risco. Planilha, colunas "Causas" e "Consequências"
		3	Estimar os **graus de probabilidade e de impacto** dos problemas e riscos. Os graus de probabilidade e impacto variam de 1-muito baixo(a) a 5-muito alto(a). Lançar os graus de probabilidade e de impacto na planilha, para cada problema e risco. Planilha, colunas "Probabilidade" e "Impacto"
	Tratamento	4	Definir as **respostas** aos problemas e riscos. Caso eles estiverem acima do apetite definido previamente, os riscos devem ter tratamento de mitigação. Se a resposta ao risco for atípica, justificar. Indicar o tipo de resposta (tipo de tratamento), para cada problema e risco. Planilha, colunas "Resposta"
		6	Elaborar o **plano de ações** para tratamento dos riscos com a definição das medidas de tratamento, responsáveis, prazos e custos estimados, para cada problema e risco. Planilha, colunas "Medidas de tratamento", "Responsável", "Prazo" e "Custo"
		7	Se definido na gestão de riscos, elaborar o **plano de contingência**, para cada problema e risco. Planilha, coluna "Medidas de contingência"
	Monitoramento	8	Periodicamente, realizar a **aferição dos efeitos dos novos controles** (tratamentos), para cada problema e risco. Planilha, coluna "Monitoramento"
		9	O monitoramento também deve estar atento à identificação de **novos riscos** para que sejam lançados na planilha.
		10	O monitoramento também deve estar atento às **oportunidades de melhoria** no processo de gerenciamento de riscos e sugerir a implementação desses aprimoramentos.

GESTÃO

Apoio da alta administração

- Comprometimento e acompanhamento
- Alinhamento com corpo diretivo
- Promoção do gerenciamento para a tomada de decisões

Estrutura

- Equipe de referência em gerenciamento de riscos
- Linhas de defesa

Diretrizes

- Política de gestão de riscos
- Apetite a riscos
- Plano e fundo para contingência
- Metodologia

GERENCIAMENTO

Identificação

1. **Descobrimento dos problemas e riscos**
   - *Modelo "MODELO 1 - Identificação de riscos de integridade"*
   - *Planilha, colunas "Data da identificação" e "Risco/Problema"*

Análise

2. **Causas e consequências dos problemas e riscos identificados**
   - *Planilha, colunas "Causas" e "Consequências"*
3. **Graus de probabilidade e de impacto de cada risco identificado**
   - *Planilha, colunas "Probabilidade" e "Impacto"*

Tratamento

4. **Seleção dos riscos acima do apetite**
5. **Definição da resposta a cada risco acima do apetite**
   - *Planilha, colunas "Resposta"*
6. **Plano de ação**
   - *Planilha, colunas "Medidas de tratamento", "Responsável", "Prazo" e "Custo"*
7. **Plano de contingência**
   - *Planilha, coluna "Medidas de contingência"*

Monitoramento

8. **Efeitos dos novos controles nos problemas e riscos**
   - *Planilha, coluna "Monitoramento"*
9. **Manutenção e novos riscos**
10. **Melhoria contínua**