METODOLOGIA DE GESTÃO DE RISCOS DO MINISTÉRIO DO DESENVOLVIMENTO REGIONAL

Aprovada/alterada por:

Resolução CIGov nº 1, de __ de ____ de 2020

Ministro de Estado do Desenvolvimento Regional

Presidente do Comitê Interno de Governança

Rogério Simonetti Marinho

Secretário-Executivo

Claudio Xavier Seefelder Filho

Secretária Nacional de Mobilidade e Desenvolvimento Regional e Urbano

Tiago Pontes Queiroz

Secretário Nacional de Saneamento

Pedro Ronald Maranhão

Secretário Nacional de Proteção e Defesa Civil

Alexandre Lucas Alves

Secretário Nacional de Segurança Hídrica

Marcelo Pereira Borges

Secretário Nacional de Habitação

Alfredo Eduardo dos Santos

Sumário

Introdução

O esforço de integração e convergência interna do Ministério do Desenvolvimento Regional – MDR quanto à gestão de riscos envolve a compreensão das diferentes culturas, desafios, contextos e níveis de maturidade de seus órgãos e entidades.

De forma a estruturar esse esforço, o modelo de governança adotado pelo MDR contempla um processo contínuo, desenhado para identificar, responder e monitorar eventos que possam constranger os objetivos definidos ao Ministério, sob liderança da Diretoria de Gestão Estratégica e Coordenação Estrutural - DIGEC, em apoio ao Comitê Interno de Governança - CIGov.

Os conceitos, princípios, objetivos, diretrizes e responsabilidades no MDR na Gestão de Riscos estão dispostos na Política de Gestão de Riscos - PGR.

De forma geral, compreende-se que gerenciar é um processo de melhoria contínua de identificação, avaliação, administração e controle de potenciais eventos de riscos, sejam eles ameaças ou oportunidades. Esta gestão é importante na medida em que permite aos gestores e tomadores de decisão avaliar a factibilidade no alcance dos objetivos organizacionais, e assim decidir pela manutenção ou revisão de procedimentos para garantir o sucesso da organização. O desenvolvimento de uma gestão de riscos eficaz e eficiente, ao aumentar a probabilidade de atingimento dos objetivos do MDR, contribuirá ao cabo para uma condução mais eficiente das políticas públicas.

O processo de gestão de riscos definido nesta Metodologia está aderente às diretrizes definidas na Política de Gestão de Riscos do MDR, em seu artigo 6º, que define, no mínimo, as seguintes etapas:

I - Análise de ambiente e dos objetivos;

II - Identificação dos riscos;

III - Avaliação dos riscos;

IV - Resposta aos riscos;

V - Monitoramento e Comunicação.

Ao longo deste documento será detalhada cada uma destas etapas, com indicação de eventuais técnicas complementares, de forma a estruturar o método de gerenciamento de riscos.

Inicialmente, cumpre informar que para a implementação do gerenciamento de riscos será utilizado o sistema informatizado denominado Agatha para documentar as etapas da gestão de riscos – Agatha. Site: https://agatha.mdr.gov.br.

Análise do Ambiente e dos Objetivos

Esta etapa trata do levantamento e registro dos aspectos externos e internos essenciais ao alcance dos objetivos institucionais, permitindo a compreensão clara do ambiente em que a

organização se insere e identificar os fatores que podem influenciar a capacidade da organização de atingir os resultados planejados.

Essa etapa permite priorizar e facilitar a abordagem a partir do processo, projeto, programa, atividade ou iniciativa objeto do gerenciamento de riscos. Poderá ser realizada análise SWOT sobre os pontos fortes e fracos do ambiente interno[1], as oportunidades e ameaças do ambiente externo[2], e a identificação dos principais atores envolvidos no processo referente ao gerenciamento de riscos.

Deverá envolver também a definição dos critérios de risco, como limites de exposição e atribuições dos agentes envolvidos na avaliação e tratamento de riscos. Essas informações subsidiam todo o processo de gestão de riscos, inclusive a etapa de comunicação.

Identificação dos Riscos

A etapa de **identificação dos riscos** envolve o reconhecimento, descrição e registro do evento de risco, com a caracterização de suas prováveis causas e possíveis consequências, caso ocorra.

Nesta etapa, deverá ser desenvolvida uma lista de eventos de riscos que podem constranger os resultados e o alcance dos objetivos, afetando o valor público a ser entregue à sociedade.

Como fonte de informação para identificação dos riscos é desejável verificar também a existência de algum Acórdão ou Recomendação dos órgãos de controle (TCU e CGU), processos judiciais ou reclamações na Ouvidoria relacionados aos processos sob análise.

Para cada evento de risco identificado ao longo do processo de gerenciamento, é desejável especificar, explorar e ressaltar suas prováveis causas e possíveis consequências.

O risco não deve ser descrito simplesmente como o "não alcance" do objetivo. A descrição do risco deve prover *insights* sobre o que pode dar errado no processo.

Como apoio à coleta estruturada de informações, poderão ser utilizadas técnicas[3] como *Brainstorming*, Diagrama de *Ishikawa, Bow Tie*, entrevista com especialistas, e análise de cenários.

---

[1] Pode envolver aspectos como governança, estrutura organizacional, funções, responsabilidades, políticas, estratégias, capacidades, competência, alçadas, sistemas de informação, processos decisórios, cultura organizacional.

[2] Pode envolver aspectos no âmbito cultural, social, político, regulatório, financeiro, tecnológico, econômico, ambiental. Inicialmente, recomenda-se utilizar a Matriz SWOT: *strengths, weaknesses, opportunities and threats* (forças, fraquezas, oportunidades e ameaças).

[3] A norma ISO/IEC 31010:2009, por exemplo, traz um rol de técnicas mais amplo que pode ser consultado em apoio aos processos de identificação, análise e avaliação de riscos.

Figura 1 – Diagrama de Ishikawa

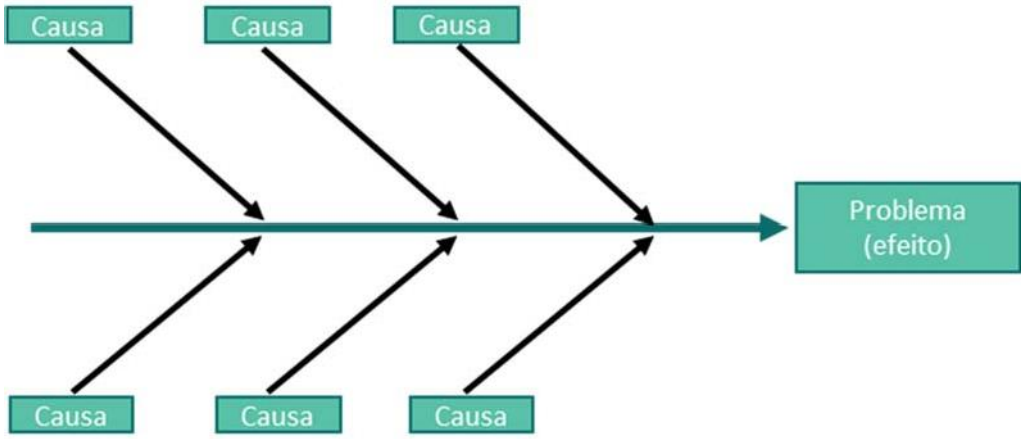
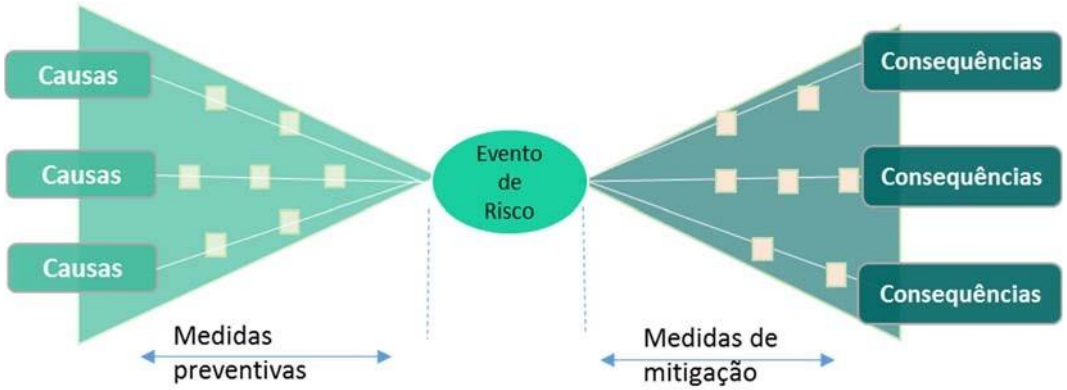


Figura 2 – *Bow Tie*



A sintaxe a seguir para descrição de aspectos envolvendo um evento de risco pode auxiliar na reflexão e desenvolvimento desta etapa:

Devido a **<CAUSA, FONTE>**, poderá acontecer **<EVENTO DE RISCO>**, o que poderá levar a **<IMPACTO, EFEITO, CONSEQUÊNCIA>**, constrangendo o **<OBJETIVO DO PROCESSO>**.

Já a classificação do evento de risco pode observar aspectos subdivididos em categorias, como:

- Estratégico: eventos de potencial impacto na missão, metas ou objetivos estratégicos da unidade/órgão;
- Operacional: eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e à eficiência dos processos organizacionais;

- Orçamentário: eventos que podem comprometer a capacidade da unidade de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;
- Reputação: eventos que podem comprometer a confiança da sociedade em relação à capacidade da unidade em cumprir sua missão institucional; interferem na imagem do órgão;
- Fiscal: eventos que podem afetar negativamente o equilíbrio das contas públicas;
- Conformidade: eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis;
- Social: eventos que podem comprometer o valor público esperado ou percebido pela sociedade em relação ao resultado da prestação de serviços públicos da instituição; e
- Integridade: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores preconizados pelo Ministério e a realização de seus objetivos.

Caso o evento de risco esteja associado a duas ou mais categorias de classificação, deverá ser escolhida a categoria que reflita o aspecto mais relevante quanto ao impacto que o evento de risco poderá trazer, caso se materialize.

Avaliação dos Riscos

A etapa de **avaliação dos riscos** visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimação da probabilidade de ocorrência, e do impacto destes eventos identificados como risco nos objetivos dos processos organizacionais.

Avaliação do risco inerente

Essa estimação pode ser feita com base em uma escala progressiva de cinco níveis (1 a 5), na forma:

- **Probabilidade**: muito baixa, baixa, média, alta, e muito alta; e
- **Impacto**: muito baixo, baixo, médio, alto, e muito alto.

A probabilidade escala-se em cinco níveis, com base em avaliação quantitativa ou qualitativa que utilizará o conhecimento técnico e experiências vivenciadas dos partícipes no processo a ser avaliado, e sempre que possível, será feita também uma avaliação quantitativa, com base nos dados estatísticos de eventos de riscos já materializados, por determinado período de tempo ou média histórica disponível. Nesse caso, é também possível o uso de técnicas de apoio à coleta estruturada de informações.

A avaliação da probabilidade utiliza da seguinte relação de aspecto avaliativo, frequência e valor do peso para apuração do risco:

- Muito baixa:

- Aspecto avaliativo: evento que pode ocorrer apenas em circunstâncias excepcionais
- Frequência observada/esperada: menor ou igual a 20%
- Peso na apuração do risco: 1 (um)

- Baixa:
  - Aspecto avaliativo: evento pode ocorrer em algum momento
  - Frequência observada/esperada: maior que 20% e menor ou igual a 40%
  - Peso na apuração do risco: 2 (dois)

- Média:
  - Aspecto avaliativo: evento deve ocorrer em algum momento
  - Frequência observada/esperada: maior que 40% e menor ou igual a 60%
  - Peso na apuração do risco: 3 (três)

- Alta:
  - Aspecto avaliativo: evento deve ocorrer na maioria das circunstâncias
  - Frequência observada/esperada: maior que 60% e menor ou igual a 80%
  - Peso na apuração do risco: 4 (quatro)

- Muito alta:
  - Aspecto avaliativo: evento com altíssima probabilidade de ocorrência
  - Frequência observada/esperada: maior que 80%
  - Peso na apuração do risco: 5 (cinco)

A avaliação de impacto utilizará os seguintes fatores de análise e pesos de distribuição caso o evento de risco ocorra:

- Orçamentário/Financeiro
  - Aspecto avaliativo: se evento de risco impacta na gestão orçamentária e financeira do MDR.
  - Peso na apuração do risco: 30% (trinta por cento).

- Resultados nas Políticas Públicas Setoriais
  - Aspecto avaliativo: se evento de risco impacta no atingimento dos resultados das estratégias setoriais expostas nas Políticas e Planos Nacionais de cada uma das políticas setoriais afetas ao MDR.
  - Peso na apuração do risco: 25% (vinte e cinco por cento).

- Resultados Organizacionais
  - Aspecto avaliativo: se evento de risco impacta no atingimento dos resultados definidos pelo próprio órgão em seus instrumentos de planejamento organizacional, tais como Planejamento Estratégico Institucional (PEI) e Plano Plurianual (PPA).
  - Peso de 20% (vinte por cento) no cálculo do impacto do evento de risco.

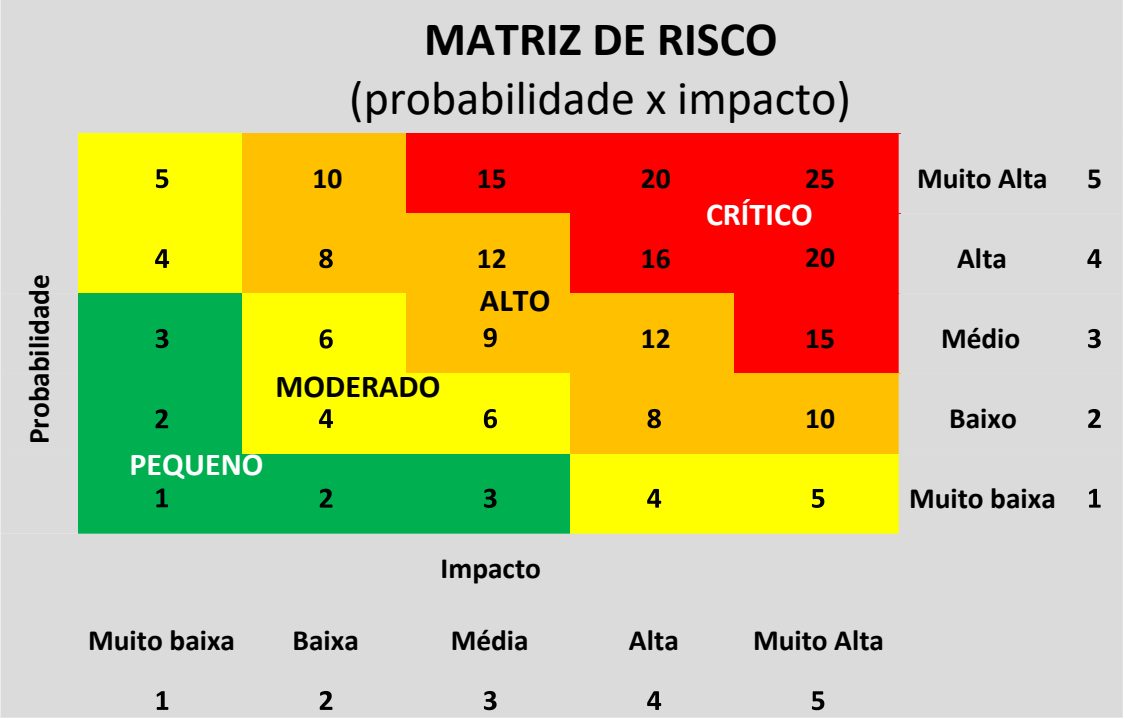
- Conformidade
  - Aspecto avaliativo: se evento de risco impacta nos atos normativos vigentes que regem o objeto (processo, projeto) da Gestão de Riscos, e medidas correlacionadas determinadas pelos órgãos de controle.
  - Peso na apuração do risco: 15% (quinze por cento).

- Imagem/Reputação

- Aspecto avaliativo: se evento de risco impacta nos aspectos de confiança da sociedade em relação à capacidade do MDR em cumprir sua missão institucional e que interferem na imagem do órgão.
- Peso na apuração do risco: 10% (dez por cento).

É desejável que a consistência das percepções de probabilidade e impacto seja sustentada pelo registro de **evidências**, como dados, documentos, relatórios, documentos SEI.

A conjunção da avaliação de probabilidade e impacto formam o resultado final da avaliação de risco agrupada em 4 (quatro) níveis, conforme **Matriz de Riscos** abaixo:



- **Nível Pequeno**: é possível conviver com o risco, mantendo as práticas e controles existentes;
- **Nível Moderado**: é possível promover ações que atenuem causas e/ou consequências;
- **Nível Alto**: é necessário a elaboração de plano de ação para evitar ou eliminar as causas e/ou consequências;
- **Nível Crítico**: é necessário a elaboração de plano de ação para evitar ou eliminar as causas e/ou consequências, bem como considerar a necessidade de mobilização imediata de recursos, materiais e pessoal capacitado, com vistas ao tratamento desse risco.

Avaliação do risco residual

Destaca-se que neste momento deve-se avaliar a eficácia dos controles[4] existentes a fim de aferir se o risco residual continua dentro do nível de risco aceitável ao processo em análise, a avaliação será notadamente quanto ao desenho e à operação dos controles existentes, na seguinte forma:

- **Desenho:** há procedimento de controle suficiente e formalizado?

a. Não há procedimento de controle;
b. há procedimentos de controle, mas insuficiente e não formalizado;
c. há procedimentos de controle formalizado, mas insuficientes;
d. há procedimentos de controle suficientes, mas não formalizados; ou
e. há procedimentos de controle suficientes e formalizados.

- **Operação**: há procedimento de controle sendo executado? Há evidências de sua execução?

a. Não há procedimento de controle;
b. há procedimentos de controle, mas não são executados;
c. há procedimentos de controle, mas parcialmente executados;
d. há procedimentos de controle executados, mas não evidenciados; e
e. há procedimentos de controle executados de forma evidenciável.

Orienta-se que todo o processo de Gestão de Riscos observe os controles sob a ótica de **custo e benefício**, de forma a otimizar a alocação de recursos, e permitir maior alcance do valor público gerado. De forma geral, o custo de um controle não deve superar seu benefício gerado ou esperado.

Resposta aos Riscos

A resposta aos riscos é a etapa em que, a cada risco identificado e avaliado, poderá ser elaborada e proposta uma ou mais medidas (respostas ao risco) para sua mitigação, na forma de Plano de Tratamento.

Há quatro possíveis tipos de respostas quanto aos riscos identificados:

- Evitar: não iniciar, ou descontinuar a atividade que origina o risco;
- Aceitar: deixar a atividade como está, não adotando qualquer medida;
- Reduzir: desenvolver ações para mitigar o risco, ou seja, remover suas fontes, ou reduzir a probabilidade e/ou o impacto do risco; e
- Compartilhar: distribuir parte do risco para outros atores (terceiros).

[4] Controle é a medida que mantém e/ou modifica o risco, e pode estar relacionado a qualquer processo, política, dispositivo, prática, inciativa, entre outras condições e/ou ações, relacionadas ao objeto da Gestão de Riscos.

As respostas deverão observar os limites de exposição a riscos definidos pelo Ministério do Desenvolvimento Regional, todos os riscos com nível de criticidade apurado superior ao nível definido, deverão preferencialmente ser instituídos controles e/ou ações mitigadoras com o objetivo de reduzi-lo ou compartilha-lo até sua conformidade com o limite de exposição aceitável pelo Ministério.

Os controles propostos podem ser avaliados quanto a:

Tipo:

- Preventivo: tem como objetivo prevenir a materialização do evento de risco (ex: verificação da credencial das pessoas, antes de entrarem no prédio do ministério); ou
- Corretivo: tem como objetivo mitigar falha que já ocorreu, apurada após o processamento inicial ter ocorrido (ex: identificação, pela vigilância, das pessoas que estão no prédio, mas sem credencial).

Natureza:

- Manual: controle realizado por pessoa (ex: conferência de assinatura);
- Automático: controle processados por sistema, sem intervenção humana relevante (ex: senha de e-mail); ou
- Híbrido: controle que mescla atividades manuais e automáticas.

Frequência: anual, semestral, bimestral, mensal, diária.

A implementação dos controles pode considerar ainda aspectos como:

- Os custos e esforços (diretos ou de oportunidade) de implementação envolvidos, bem como os benefícios decorrentes;
- Os requisitos legais, normativos e regulatórios;
- Os responsáveis por aprovar e implementar as ações (as funções devem ser segregadas);
- Recursos necessários.

Monitoramento e Comunicação

O **monitoramento** é a etapa contínua em que as instâncias envolvidas com Gestão de Riscos interagem. Abrange a coleta e a disseminação de informações e iniciativas, a fim de assegurar a compreensão suficiente a todos os agentes envolvidos dos riscos existentes em cada decisão.

É importante que as informações apresentadas nos meios de monitoramento possuam qualidade contextual e de representação como base nos critérios a seguir:

- Relevância: a informação deve ser útil para o objetivo do trabalho;
- Integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;

- Adequação: volume de informação adequado e suficiente;
- Concisão: informação deve ser apresentada de forma compacta;
- Consistência: as informações apresentadas devem ser compatíveis;
- Clareza: informação deve ser facilmente compreensível; e
- Padronização: informação deve ser apresentada no padrão aceitável.

O acesso a informações confiáveis, íntegras e tempestivas é vital para a eficiência da gestão visando facilitar o alcance dos objetivos de cada processo. Para isso, o fluxo das comunicações deve permitir que as informações fluam em todas as direções, com a divulgação tempestiva e adequada das informações às partes interessadas.

Assim, devem ser observados aspectos como alçadas dos agentes e, quanto às informações, a gradual convergência para promover a relevância, integralidade, adequação, concisão, consistência, clareza e padronização.

O MDR deverá assegurar que os controles permaneçam eficazes e que ambiente de controle se mantenha efetivo ao longo do tempo.

> *O gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo. As respostas a risco que se mostravam eficazes anteriormente podem tornar-se inócuas; as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou os objetivos podem mudar. (...) Diante dessas mudanças, a administração necessita determinar se o funcionamento do gerenciamento de riscos corporativos permanece eficaz. (COSO ERM)*

Cabe destacar que a implementação de atividades relacionadas à gestão de risco e controles, por si só, não é suficiente a assegurar que os objetivos dos processos sejam alcançados. O estabelecimento de limites de atuação de cada área/servidor, bem como a clareza das suas responsabilidades são essenciais para que cada um dos participantes saiba como seu cargo se encaixa na estrutura corporativa de gestão de riscos e controles. As instâncias e as competências de cada uma estão definidas na Política de Gestão de Riscos do MDR.

ANEXOS:

A. Referencial Teórico;
B. Glossário;

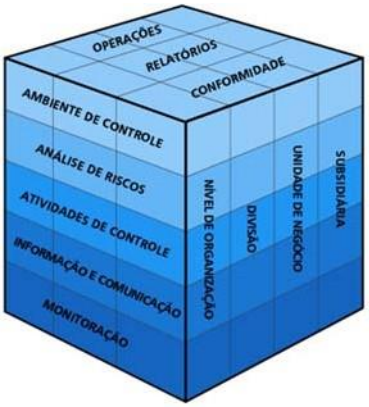
ANEXO A – Referencial Teórico

Apresentam-se neste anexo as estruturas de gerenciamento de riscos mundialmente reconhecidas e que têm sido base para a implementação da gestão de riscos na maior parte das organizações em todo o mundo. A maioria dessas normas apresentam mais semelhanças que diferenças e são aplicáveis a qualquer tipo de organização, devendo ser adaptadas às suas características, atividades e cultura.

COSO I e COSO GRC/COSO II

O Coso (*The Committee of Sponsoring Organizations of the Treadway Commission* – Comitê das Organizações Patrocinadoras) é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros por meio da ética, efetividade dos controles internos e governança corporativa. Criada em 1985, sua origem está relacionada a um grande número de escândalos financeiros, na década de 70, nos Estados Unidos, que colocaram em dúvida a confiabilidade dos relatórios corporativos. Em 1992, o Coso publicou um trabalho denominado Controle Interno: um modelo integrado (COSO I), revisado em 2013.

O COSO I tornou-se referência por auxiliar as organizações a avaliar e aperfeiçoar seus sistemas de controle interno, sendo essa estrutura incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos (TCU, 2009).



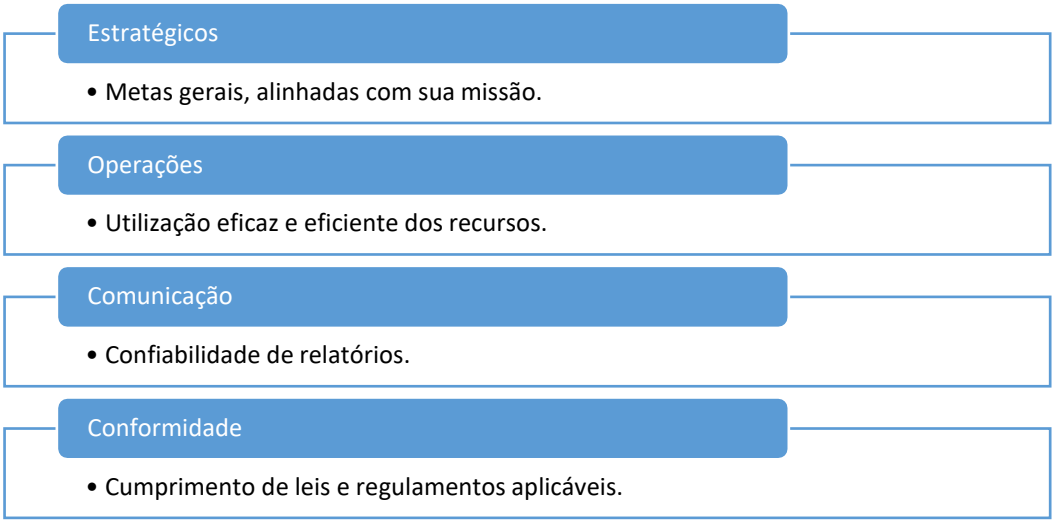
Fonte: COSO

Em 2004, a intensificação da preocupação com riscos, a partir da crise ocorrida no início dos anos 2000, quando foram descobertas manipulações contábeis em diversas empresas, tais como Enron, Worldcom, Xerox, Parmalat (Itália), dentre outras, fez com que o COSO divulgasse o trabalho ***Enterprise Risk Management – Integrated Framework*** (Gerenciamento de Riscos Corporativos – Estrutura Integrada), também conhecido como COSO ERM, COSO GRC ou COSO II, com um foco mais voltado para o gerenciamento de riscos corporativos, tendo definido esse termo como:

> *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 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 (2004)*

De acordo com o COSO GRC, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização.

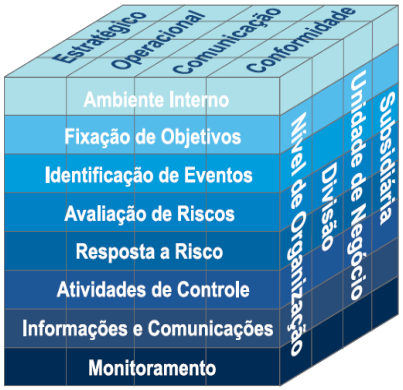
Essa estrutura de gerenciamento de riscos é orientada a fim de alcançar os objetivos de uma organização e são classificados em **quatro categorias**:



Um avanço da estrutura do COSO GRC em relação ao COSO I, que tinha como enfoque os controles internos de uma organização, é justamente a categoria de objetivos estratégicos.

A lógica por trás dessa inclusão é que, em se tratando de atingimento de objetivos de uma organização, de nada adiantaria as operações serem eficientes, os relatórios confiáveis e leis e regulamentos serem cumpridos, se não há uma estratégia a ser alcançada, ou seja, se a organização não sabe onde quer chegar.

A figura a seguir ficou conhecida como Cubo do Coso. A dimensão superior apresenta os objetivos que devem ser objeto do gerenciamento de risco, conforme abordado anteriormente. Já a dimensão lateral representa os níveis da organização por onde perpassam a gestão de riscos. Por fim, a dimensão frontal apresenta os oito componentes do gerenciamento de riscos, que serão abordados de forma sucinta a seguir, representando o que é necessário fazer, de forma integrada, para atingir os objetivos elencados na face superior.



Fonte: COSO (2004)

Ambiente interno

O ambiente interno é moldado pela história e cultura da organização e, por sua vez, molda, de maneira explícita ou não, a cultura de gestão dos riscos da organização e a forma como eles são encarados e gerenciados (tom da organização), influenciando a consciência de controle das pessoas (TCU, 2009).

Segundo o COSO GRC, esse componente fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, sendo o alicerce para os demais. Integridade, valores éticos e competência dos colaboradores (funcionários, servidores, etc.) são alguns dos fatores que compõem o Ambiente Interno. Além deles, a forma como a gestão delega autoridade e responsabilidades, define seu apetite a riscos, bem como posiciona sua estrutura de governança e define as políticas e práticas de recursos humanos também fazem parte desse componente.

Fixação de objetivos

A estrutura do COSO GRC requer que todos os níveis da organização tenham objetivos fixados e comunicados (estratégicos, operacionais, comunicação e conformidade), antes da identificação dos eventos que possam influenciar em seu atingimento.

Os objetivos estratégicos devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos. Tais objetivos são metas de nível geral, alinhadas com a missão/visão da organização e fornecendo-lhe apoio. Devem refletir como a alta administração escolheu uma forma de gerar valor para as partes interessadas que, na esfera pública em última instância, é a sociedade.

Identificação de eventos

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer.

Podem ser positivos ou negativos, sendo que a estrutura do COSO GRC denomina os eventos negativos como riscos, enquanto os positivos são chamados de oportunidades.

Por meio da identificação de eventos, pode-se planejar o tratamento adequado para as oportunidades e para os riscos, devendo ser entendidos como parte de um contexto, e não de forma isolada, já que muitas vezes um risco que parece trazer grande impacto pode ser minimizado pela existência conjunta de uma oportunidade.

Após a identificação de eventos, a organização atua sobre os riscos, avaliando-os e determinando a forma de tratamento para cada evento identificado e qual o tipo de resposta a ser dada a esse risco.

Avaliação de Riscos

Os eventos identificados no componente anterior, externos e internos, devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. Essa avaliação é justificada para que a administração desenvolva estratégias para dar resposta aos riscos, ou seja, como os riscos serão administrados, de modo a diminuir a probabilidade de ocorrência e/ou a magnitude do impacto.

Os riscos devem ser avaliados quanto a sua condição de inerentes e residuais. Entende-se por risco inerente aquele que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Já o risco residual é aquele que ainda permanece após a resposta da administração (COSO, 2004).

Resposta a riscos

Para cada risco identificado será prevista uma resposta. A escolha dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco e pode ser de 4 tipos: evitar, aceitar, compartilhar ou reduzir. A administração deve obter uma visão dos riscos em toda organização e desenvolver ações concretas para manter o nível de riscos residuais alinhado aos níveis de tolerância e apetite a riscos da organização.

De acordo com o COSO (2004), “Evitar” sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. “Reduzir” ou “Compartilhar” reduzem o risco residual a um nível compatível com as tolerâncias desejadas ao risco, enquanto “Aceitar” indica que o risco inerente já esteja dentro das tolerâncias ao risco.

Ao analisar as respostas, a administração poderá considerar eventos e tendências anteriores, e o potencial de situações futuras (COSO, 2004).

É importante que se tenha consciência que sempre existirá algum nível de risco residual, não somente porque os recursos são limitados, mas também em decorrência da incerteza e das limitações inerentes a todas as atividades de uma organização.

Atividades de controle

Segundo o COSO GRC, ao selecionar as respostas aos riscos, a administração identifica as atividades de controle necessárias para assegurar que estas sejam executadas de forma adequada e oportuna.

Essas atividades contribuem para assegurar que os objetivos sejam alcançados, que as diretrizes administrativas sejam cumpridas e que as ações necessárias para gerenciar os riscos com vistas ao atingimento dos objetivos da entidade estejam sendo implementadas.

Ao selecionar as atividades de controle, a administração deve levar em consideração a forma como essas atividades se relacionam entre si. Há situações em que uma única atividade de controle aborda diversas respostas a riscos. Em outras, diversas atividades de controle são necessárias para dar resposta a apenas um risco. E, ainda, há aquelas situações em que a administração poderá constatar que as atividades de controle existentes são suficientes para assegurar a execução eficaz das novas respostas a riscos (COSO, 2004).

Informação e Comunicação

Esse componente abrange informações e sistemas de comunicação, permitindo que as pessoas da organização coletem e troquem informações necessárias para conduzir, gerenciar e controlar suas operações. É importante que toda a informação relevante, relacionada aos objetivos – riscos - controles, sejam capturadas tempestivamente e comunicadas por toda a organização.

A organização também deve possuir mecanismos para coletar informações do ambiente externo que possam afetá-la, e deve transmitir externamente aquelas que sejam relevantes aos *stakeholders*, inclusive à sociedade, que, no caso das organizações públicas, pode ser considerada a principal parte interessada.

A comunicação deverá ser oportuna e adequada, além de abordar aspectos financeiros, econômicos, operacionais e estratégicos. Deve ser entendida como um canal que movimenta as informações em todas as direções – dos superiores aos subordinados, e vice-versa – pois determinados assuntos são mais bem visualizados pelos integrantes dos níveis mais subordinados (COSO, 2004). A habilidade da administração de tomar decisões apropriadas é afetada pela qualidade da informação, que deve ser útil, isto é, apropriada, tempestiva, atual e precisa.

Monitoramento

Monitorar diz respeito a avaliar, certificar e revisar a estrutura de gestão de riscos e controles internos para saber se estão sendo efetivos ou não. Tem, portanto, o objetivo de avaliar a qualidade da gestão de risco e dos controles internos ao longo do tempo, buscando assegurar que estes funcionam como previsto e que são modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos (TCU, 2009).

O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno pode “reagir” de forma dinâmica, ajustando-se conforme as condições o determinem. O monitoramento pode ser realizado por meio de:

As atividades contínuas são incorporadas as demais atividades normais da organização e as avaliações independentes, realizadas por auditores internos e ou externos, garantem a eficácia do gerenciamento dos riscos ao longo do tempo. Modernamente também são utilizadas as autoavaliações, processo que pode ter um grande auxílio dos auditores.

O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a frequência das avaliações independentes dependerão basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento.

Diferentemente das atividades de controle, que são concebidas para dar cumprimento aos processos e políticas da organização e visam tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de melhorias (BRASIL, 2017).

COSO 2017 – Integração com Estratégia e Desempenho

Em 2017 ocorreu a revisão do Coso ERM: *Enterprise Risk Management: Integrating with Strategy and Performance* (COSO, 2017), que estabelece que o gerenciamento de riscos corporativos "não é uma função ou departamento. É a cultura, os recursos e as práticas que as organizações integram com a estratégia definida e executada, com o objetivo de gerenciar o risco na criação, preservação e valorização (tradução livre).

De maneira geral, o novo modelo passa a integrar o gerenciamento de riscos com outros processos da organização, tais como governança, definição da estratégia, definição dos objetivos e gestão do desempenho. O novo modelo explora a gestão da estratégia e dos riscos a partir de três perspectivas, quais sejam:

- ✓ Possibilidade de os objetivos estratégicos e de negócios não se alinharem com a missão, a visão e os valores fundamentais da organização.
- ✓ As implicações da estratégica escolhida.
- ✓ Os riscos na execução da estratégia.

Fonte: COSO (2017)

Um ponto importante atualizado no documento é o refinamento entre apetite a riscos e tolerância a riscos, agora com enfoque na variação aceitável do desempenho.

A primeira parte da publicação oferece uma perspectiva dos conceitos atuais e em desenvolvimento e aplicações do gerenciamento de riscos corporativos. A segunda parte da publicação apresenta 20 princípios organizados em 5 componentes inter-relacionados: Governança e cultura, Estratégia e definição de objetivos, Performance, Monitoramento do desempenho e revisão; e finalmente Informação, comunicação e divulgação.

Aderir a estes princípios pode conferir a organização uma razoável expectativa de que ela entende e se esforça para gerenciar os riscos associados à sua estratégia e objetivos de negócios.

Fonte: COSO Enterprise Risk Management – Integrating with Strategy and Performance (COSO, 2017 - tradução livre).

a) Governança e Cultura (fornece a base para os demais componentes)

1. Exercita a Supervisão de Riscos pelo Conselho - O conselho de administração supervisiona a estratégia e executa responsabilidades de governança para apoiar a gestão na consecução da estratégia e dos objetivos de negócios.

2. Estabelece Estruturas Operacionais - A organização estabelece estruturas operacionais na busca de objetivos estratégicos e de negócios.

3. Define Cultura Desejada - A organização define os comportamentos desejados que caracterizam a cultura desejada pela entidade.

4. Demonstra Compromisso com Valores Fundamentais - A organização demonstra compromisso com os valores fundamentais da entidade.

5. Atrai, Desenvolve e Mantém Indivíduos Capazes - A organização está empenhada em construir capital humano em alinhamento com a estratégia e os objetivos de negócios.

b) Estratégia e Definição de Objetivos

6. Analisa o Contexto de Negócio - A organização considera os potenciais efeitos do contexto dos negócios no perfil de risco.

7. Define o Apetite ao Risco - A organização define o apetite a riscos no contexto de criação, preservação e realização de valor.

8. Avalia Estratégias Alternativas - A organização avalia estratégias alternativas e potencial impacto sobre o perfil de risco.

9. Elabora Objetivos de Negócios - A organização considera o risco ao estabelecer os objetivos de negócios em vários níveis que alinham e apoiam a estratégia.

c) Desempenho

10. Identifica Riscos - A organização identifica o risco que afeta o desempenho da estratégia e dos objetivos de negócios.

11. Avalia a Severidade do Risco - A organização avalia a gravidade do risco.

12. Prioriza Riscos - A organização prioriza os riscos como base para a seleção das respostas aos riscos.

13. Implementa Respostas a Riscos - A organização identifica e seleciona respostas a riscos.

14. Desenvolve Visão de *Portfolio* - A organização desenvolve e avalia uma visão de portfólio de risco.

d) Revisão

15. Avalia Mudanças Substanciais - A organização identifica e avalia mudanças que podem afetar substancialmente a estratégia e os objetivos de negócios.

16. Revê Riscos e Desempenho - A organização revê o desempenho da entidade e considera o risco.

17. Persegue a Melhoria no Gerenciamento de Riscos Corporativos - A organização busca a melhoria do gerenciamento de riscos corporativos.

e) Informação, Comunicação e Divulgação

18. Aproveita a Informação e a Tecnologia - A organização aproveita os sistemas de tecnologia da informação da entidade para apoiar a gestão de riscos corporativos.

19. Comunica Informações de Risco - A organização usa canais de comunicação para suportar o gerenciamento de riscos corporativos.

20. Reporta sobre Risco, Cultura e Desempenho - A organização informa sobre risco, cultura e desempenho em vários níveis e em toda a entidade.

ISO 31000

A ABNT NBR **ISO 31000** foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos, sendo uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 31000:2018, preparada pelo *Technical Commitee risk management*, conforme ISO/IEC *Guide* 21-1:2005.

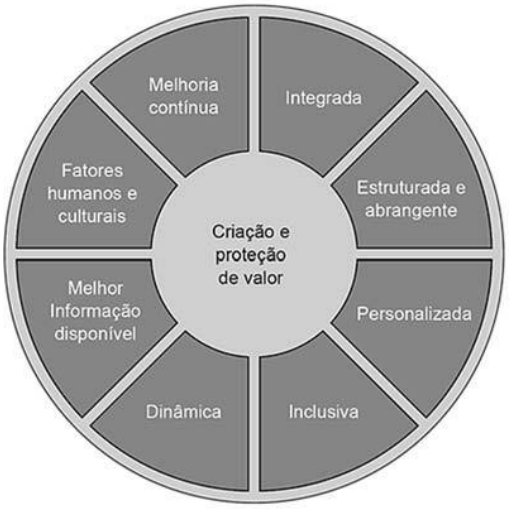
A ISO 31000 foi atualizada em 2018, sendo a ISO 31010:2009 (traduzida para o português em 2012 – ABNT NBR ISSO/IEC 31010:2012) ainda permanece em vigor, com previsão para sua atualização agora no ano de 2019.

A ISO 31000 tem talvez a mais simples definição de riscos dentre todas as outras normas e estruturas de gestão de riscos. Segundo ela, risco é o “efeito da incerteza nos objetivos”. Esse efeito é um desvio em relação ao esperado, podendo ser positivo ou negativo.

Essa é uma das diferenças entre essa norma e o COSO GRC, já que este considera risco apenas como algo negativo, chamando de oportunidade quando o evento é positivo.

Segundo essa norma o propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos.

Os princípios, descritos na Figura a seguir, são a base para gerenciar riscos e convém que sejam considerados quando se estabelecerem a estrutura e os processos de gestão de riscos da organização. Convém que estes princípios possibilitem uma organização a gerenciar os efeitos da incerteza nos seus objetivos.



Fonte: ABNT NBR ISO 31000

a) Integrada

A gestão de riscos é parte integrante de todas as atividades organizacionais.

b) Estruturada e abrangente

Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis.

c) Personalizada

A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos.

d) Inclusiva

O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada.

e) Dinâmica

Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna.

f) Melhor informação disponível

As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes.

g) Fatores humanos e culturais

O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio.

h) Melhoria contínua

A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da Alta Direção.

O desenvolvimento da estrutura engloba integração, concepção, implementação, avaliação e melhoria da gestão de riscos através da organização. A Figura a seguir ilustra os componentes de uma estrutura.

Fonte: ABNT NBR ISO 31000

Convém que a organização avalie suas práticas e processos existentes de gestão de riscos, avalie quaisquer lacunas e aborde estas lacunas no âmbito da estrutura.

Convém que os componentes da estrutura e o modo como funcionam em conjunto sejam personalizados para as necessidades da organização.

Liderança e comprometimento

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que a gestão de riscos esteja integrada em todas as atividades da organização.

Integração

A integração da gestão de riscos apoia-se em uma compreensão das estruturas e do contexto organizacional. Estruturas diferem, dependendo do propósito, metas e complexidade da organização. O risco é gerenciado em todas as partes da estrutura da organização. Todos na organização têm responsabilidade por gerenciar riscos.

Integrar a gestão de riscos em uma organização é um processo dinâmico e iterativo, e convém que seja personalizado para as necessidades e cultura da organização.

Convém que a gestão de riscos seja uma parte, e não separada, do propósito organizacional, governança, liderança e comprometimento, estratégia, objetivos e operações.

Concepção

Entendendo a organização e seu contexto

Ao conceber a estrutura para gerenciar riscos, convém que a organização examine e entenda seus contextos externo e interno.

Articulando o comprometimento com a gestão de riscos

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, demonstrem e articulem o seu comprometimento contínuo com a gestão de riscos por meio de uma política, uma declaração ou outras formas que claramente transmitam os objetivos e o comprometimento com a gestão de riscos de uma organização.

Convém que o comprometimento com a gestão de riscos seja comunicado na organização e às partes interessadas, como apropriado.

Atribuindo papéis organizacionais, autoridades, responsabilidades e responsabilizações

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que as autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização.

Alocando recursos

Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem a alocação de recursos apropriados para a gestão de riscos. Convém que a organização considere as capacidades e restrições dos recursos existentes.

Estabelecendo comunicação e consulta

Convém que a organização estabeleça uma abordagem aprovada para comunicação e consulta para apoiar a estrutura e facilitar a aplicação eficaz da gestão de riscos. Comunicação envolve compartilhar informação com públicos-alvo. A consulta também envolve o fornecimento de retorno pelos participantes, com a expectativa de que isto contribuirá para as decisões e sua formulação ou outras atividades. Convém que os métodos e conteúdo da comunicação e consulta reflitam as expectativas das partes interessadas, onde for pertinente.

Convém que a comunicação e a consulta sejam oportunas e assegurem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, e que o retorno seja fornecido e as melhorias sejam implementadas.

Implementação

Convém que a organização implemente a estrutura de gestão de riscos por meio de:

- desenvolvimento de um plano apropriado, incluindo prazos e recursos;
- identificação de onde, quando e como diferentes tipos de decisões são tomadas pela organização, e por quem;
- modificação dos processos de tomada de decisão aplicáveis, onde necessário;
- garantia de que os arranjos da organização para gerenciar riscos sejam claramente compreendidos e praticados.

A implementação bem-sucedida da estrutura requer o engajamento e a conscientização das partes interessadas. Isso permite que as organizações abordem explicitamente a incerteza na tomada de decisão, enquanto também asseguram que qualquer incerteza nova ou posterior possa ser levada em consideração à medida que ela surja.

Adequadamente concebida e implementada, a estrutura de gestão de riscos assegurará que o processo de gestão de riscos é parte de todas as atividades da organização, incluindo a tomada de decisão, e que as mudanças nos contextos externo e interno serão adequadamente capturadas.

Avaliação

Para avaliar a eficácia da estrutura de gestão de riscos, convém que a organização:

- mensure periodicamente o desempenho da estrutura de gestão de riscos em relação ao seu propósito, planos de implementação, indicadores e comportamento esperado;
- determine se permanece adequada para apoiar o alcance dos objetivos da organização.

Melhoria

Adaptação

Convém que a organização monitore e adapte continuamente a estrutura de gestão de riscos para abordar as mudanças externas e internas. Ao fazer isso, a organização pode melhorar seu valor.

Melhoria contínua

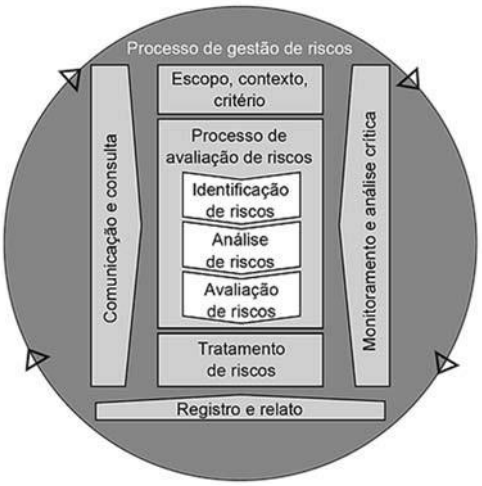
Convém que organização melhore continuamente a adequação, suficiência e eficácia da estrutura de gestão de riscos e a forma como o processo de gestão de riscos é integrado.

À medida que lacunas ou oportunidades de melhoria pertinentes são identificadas, convém que a organização desenvolva planos e tarefas e os atribua àqueles responsabilizados pela implementação.

Uma vez implementadas, convém que estas melhorias contribuam para o aprimoramento da gestão de riscos.

Processo

O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos. Este processo é ilustrado na Figura a seguir:



Fonte: ABNT NBR ISO 31000

Convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas ou de projetos.

Comunicação e consulta

O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas. A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão. Convém que uma coordenação estreita entre as duas facilite a troca de informações factuais, oportunas, pertinentes, precisas e compreensíveis, levando em consideração a confidencialidade e integridade da informação, bem como os direitos de privacidade dos indivíduos.

Convém que ocorram comunicação e consulta com partes interessadas apropriadas externas e internas, no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos.

Escopo, contexto e critérios

O propósito do estabelecimento do escopo, contexto e critérios é personalizar o processo de gestão de riscos, permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

Escopo, contexto e critérios envolvem a definição do escopo do processo, a compreensão dos contextos externo e interno.

Definindo o escopo

Convém que a organização defina o escopo de suas atividades de gestão de riscos.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis (por exemplo, estratégico, operacional, programa, projeto ou outras atividades), é importante ser claro sobre o escopo em consideração, os objetivos pertinentes a serem considerados e o seu alinhamento aos objetivos organizacionais.

Contextos externo e interno

Os contextos externo e interno são o ambiente no qual a organização procura definir e alcançar seus objetivos.

Convém que o contexto do processo de 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 riscos é aplicado.

Definindo critérios de risco

Convém que a organização especifique a quantidade e o tipo de risco que podem ou não assumir em relação aos objetivos. Convém também que estabeleça critérios para avaliar a significância do risco e para apoiar os processos de tomada de decisão. Convém que os critérios de risco sejam alinhados à estrutura de gestão de riscos e sejam personalizados para o propósito específico e o escopo da atividade em consideração. Convém que os critérios de risco reflitam os valores, objetivos e recursos da organização e sejam consistentes com as políticas e declarações sobre gestão de riscos. Convém que os critérios de risco sejam estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas.

Embora convenha que os critérios de risco sejam estabelecidos no início do processo de avaliação de riscos, eles são dinâmicos; e convém que sejam continuamente analisados criticamente e alterados, se necessário.

Processo de avaliação de riscos

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos.

Convém que o processo de avaliação de riscos seja conduzido de forma sistemática, iterativa e colaborativa, com base no conhecimento e nos pontos de vista das partes interessadas. Convém que use a melhor informação disponível, complementada por investigação adicional, como necessário.

Identificação de riscos

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Informações pertinentes, apropriadas e atualizadas são importantes na identificação de riscos.

A organização pode usar uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos. Convém que os seguintes fatores e o relacionamento entre estes fatores sejam considerados:

- fontes tangíveis e intangíveis de risco;
- causas e eventos;
- ameaças e oportunidades;
- vulnerabilidades e capacidades;
- mudanças nos contextos externo e interno;
- indicadores de riscos emergentes;
- natureza e valor dos ativos e recursos;
- consequências e seus impactos nos objetivos;
- limitações de conhecimento e de confiabilidade da informação;
- fatores temporais;
- vieses, hipóteses e crenças dos envolvidos.

Convém que a organização identifique os riscos, independentemente de suas fontes estarem ou não sob seu controle. Convém considerar que pode haver mais de um tipo de resultado, o que pode resultar em uma variedade de consequências tangíveis ou intangíveis.

Análise de riscos

O propósito da análise de riscos é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

A análise de riscos pode ser realizada com vários graus de detalhamento e complexidade, dependendo do propósito da análise, da disponibilidade e confiabilidade da informação, e dos recursos disponíveis.

As técnicas de análise podem ser qualitativas, quantitativas ou uma combinação destas, dependendo das circunstâncias e do uso pretendido.

Convém que a análise de riscos considere fatores como:

- a probabilidade de eventos e consequências;
- a natureza e magnitude das consequências;
- complexidade e conectividade;
- fatores temporais e volatilidade;
- a eficácia dos controles existentes;
- sensibilidade e níveis de confiança.

A análise de riscos pode ser influenciada por qualquer divergência de opiniões, vieses, percepções do risco e julgamentos. Influências adicionais são a qualidade da informação utilizada, as hipóteses e as exclusões feitas, quaisquer limitações das técnicas e como elas são executadas.

Convém que estas influências sejam consideradas, documentadas e comunicadas aos tomadores de decisão.

Avaliação de riscos

O propósito da avaliação de riscos é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de:

- fazer mais nada;
- considerar as opções de tratamento de riscos;
- realizar análises adicionais para melhor compreender o risco;
- manter os controles existentes;
- reconsiderar os objetivos.

Convém que as decisões levem em consideração o contexto mais amplo e as consequências reais e percebidas para as partes interessadas externas e internas.

Convém que o resultado da avaliação de riscos seja registrado, comunicado e então validado nos níveis apropriados da organização.

Tratamento de riscos

O propósito do tratamento de riscos é selecionar e implementar opções para abordar riscos.

O tratamento de riscos envolve um processo iterativo de:

- formular e selecionar opções para tratamento do risco;
- planejar e implementar o tratamento do risco;

- avaliar a eficácia deste tratamento;
- decidir se o risco remanescente é aceitável;
- se não for aceitável, realizar tratamento adicional.

Seleção de opções de tratamento de riscos

Selecionar a(s) opção(ões) mais apropriada(s) de tratamento de riscos envolve balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou apropriadas em todas as circunstâncias.

A justificativa para o tratamento de riscos é mais ampla do que apenas considerações econômicas, e convém que leve em consideração todas as obrigações da organização, compromissos voluntários e pontos de vista das partes interessadas. Convém que a seleção de opções de tratamento de riscos seja feita de acordo com os objetivos da organização, critérios de risco e recursos disponíveis.

Ao selecionar opções de tratamento de riscos, convém que a organização considere os valores, percepções e potencial envolvimento das partes interessadas, e as formas mais apropriadas para com elas se comunicar e consultar. Embora igualmente eficazes, alguns tratamentos de riscos podem ser mais aceitáveis para algumas partes interessadas do que para outras.

Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos, para assegurar que as diferentes formas de tratamento se tornem e permaneçam eficazes.

O tratamento de riscos também pode introduzir novos riscos que precisem ser gerenciados.

Se não houver opções de tratamento disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, convém que este seja registrado e mantido sob análise crítica contínua.

Convém que os tomadores de decisão e outras partes interessadas estejam conscientes da natureza e extensão do risco remanescente após o tratamento de riscos. Convém que o risco remanescente seja documentado e submetido a monitoramento, análise crítica e, onde apropriado, tratamento adicional.

Preparando e implementando planos de tratamento de riscos

O propósito dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos

envolvidos, e o progresso em relação ao plano possa ser monitorado. Convém que o plano de tratamento identifique claramente a ordem em que o tratamento de riscos será implementado.

Convém que os planos de tratamento sejam integrados nos planos e processos de gestão da organização, em consulta com as partes interessadas apropriadas.

Monitoramento e análise crítica

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

Convém que monitoramento e análise crítica ocorram em todos os estágios do processo. Monitoramento e análise crítica incluem planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno.

Convém que os resultados do monitoramento e análise crítica sejam incorporados em todas as atividades de gestão de desempenho, medição e relatos da organização.

Registro e relato

Convém que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados. O registro e o relato visam:

- comunicar atividades e resultados de gestão de riscos em toda a organização;
- fornecer informações para a tomada de decisão;
- melhorar as atividades de gestão de riscos;
- auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

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

O relato é parte integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a Alta Direção e os órgãos de supervisão a cumprirem suas responsabilidades.

Orange Book

O documento ***The Orange Book Management of Risk - Principles and Concepts*** (Gerenciamento de Riscos – Princípios e Conceitos) foi produzido e publicado pelo *HM Treasury* do

Governo Britânico (UK, 2004), sendo amplamente utilizado como a principal referência do Programa de Gerenciamento de Riscos do Governo do Reino Unido, iniciado em 2001. O modelo foi atualizado em 2004 e tem como vantagens, além de ser compatível com padrões internacionais de gerenciamento de riscos, como COSO GRC e ISO 31000.

Segundo o documento, mais importante que uma organização seguir qualquer norma ou estrutura de risco em particular é sua habilidade em demonstrar que os riscos são gerenciados, com suas particularidades e de uma maneira que efetivamente suporta a entrega de seus objetivos (UK, 2004). O modelo de gerenciamento de riscos do Orange Book é ilustrado a seguir:

Fonte: UK (2004 – tradução livre)

A gestão do risco não é um processo linear, mas o equilíbrio de uma série de elementos entrelaçados que interagem uns com os outros e que devem estar em equilíbrio para que a gestão de risco seja efetiva.

Além disso, os riscos específicos não podem ser abordados isoladamente um do outro, pois a gestão de um risco pode ter impacto em outro, e podem ser desenvolvidas ações efetivas que controlem mais de um risco simultaneamente (Ibidem, 2004).

Nenhuma organização é inteiramente autônoma, apresentando uma série de interdependências com outras organizações. O modelo chama essas interdependências de "empresa / organização estendida" e impactam a gestão de risco da organização, dando origem a certos riscos adicionais que precisam ser gerenciados.

O modelo funciona em um ambiente em que o apetite de risco tenha sido definido e esse conceito perpassa toda sua estrutura. Ele divide o processo central de gerenciamento de risco

em elementos (identificação, avaliação, resposta e monitoramento) para fins ilustrativos, em consonância com o que vimos em outras estruturas de riscos. Além disso, o modelo ilustra como o processo central de gerenciamento de riscos não é algo isolado, mas que ocorre em um contexto.

O Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos do GesPública, afirma que uma das vantagens do Orange Book é tratar riscos de forma simples, sendo que estes devem ser gerenciados em três níveis: estratégico, de programas e de projetos e atividades. A organização deve ser capaz de gerenciar riscos em todos eles.

Nível Estratégico

É neste nível onde se dá o contrato político do Governo com a sociedade e é estabelecida a coerência do seu programa de Governo. Decisões neste nível envolvem a formulação dos objetivos estratégicos e as prioridades para a alocação de recursos públicos em alinhamento com as políticas públicas.

Nível Programa

Neste nível encontram-se as decisões de implementação e gerenciamento de programas temáticos previstos no nível estratégico, através dos quais são executadas as políticas e as ações prioritárias de Governo. Ocorre a transformação da estratégia em ações.

Nível Projetos e Atividades

Neste nível encontram-se os projetos que contribuirão para o atingimento dos objetivos dos Programas, e as atividades relativas aos processos finalísticos. As lideranças em todos os níveis da organização devem estar conscientes, capacitadas e motivadas com relação à relevância do gerenciamento de riscos nos três níveis, que são interdependentes.

O Modelo das Três Linhas de Defesa

Embora não seja um documento que traga uma proposta de estrutura ao gerenciamento de riscos em uma organização, opta-se por apresentar o modelo das Três Linhas de Defesa nesse anexo por ser uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais de cada um dentro de uma organização, sendo aplicável a qualquer órgão ou entidade – não importando o seu tamanho ou a sua complexidade – ainda que não exista uma estrutura ou sistema formal de gestão de riscos.

O modelo apresenta um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, tendo sido amplamente difundido a

partir da Declaração de Posicionamento do Instituto de Auditores Internos - IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles (IIA, 2013), base para essa parte do capítulo.

No modelo de Três Linhas de Defesa, o gestor é a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa e a avaliação independente é a terceira. Cada uma dessas três "linhas" desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

Embora os órgãos de governança e a alta administração não sejam considerados dentre as três "linhas" desse modelo, nenhuma discussão sobre sistemas de gerenciamento de riscos estaria completa sem considerar, em primeiro lugar, os papéis essenciais dos órgãos de governança (conselho de administração e órgãos equivalentes) e da alta administração. Os órgãos de governança e a alta administração são as principais partes interessadas atendidas pelas "linhas" e são as partes em melhor posição para ajudar a garantir que o modelo de Três Linhas de Defesa seja aplicado aos processos de gerenciamento de riscos e controle da organização.

Fonte: Declaração de Posicionamento IIA (2013)

1ª Linha de Defesa: Gestão Operacional

Como primeira linha de defesa, os gerentes operacionais gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

Se pensarmos em uma organização do setor público, essa primeira linha de defesa é aquela realizada por cada agente público no exercício de suas atividades.

Segundo o IIA (2013), a gerência operacional é responsável por manter controles internos eficazes e por conduzir procedimentos de riscos e controle diariamente.

Essa gerência identifica, avalia, controla e mitiga os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos. Por meio de uma estrutura de responsabilidades em cascata, os gerentes do nível médio desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução, por parte de seus funcionários, desses procedimentos. Trazendo isso para uma linguagem mais adequada ao setor público, é como se os coordenadores, chefes de divisão, gerentes de projeto, ou qualquer cargo semelhante tivessem essa responsabilidade.

Segundo a Instrução Normativa CGU nº 3/2017, a primeira linha de defesa é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos destinados a garantir que as atividades sejam realizadas de acordo com as metas e objetivos da organização.

A primeira linha de defesa contempla os controles primários, que devem ser instituídos e mantidos pelos gestores responsáveis pela implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio.

2ª Linha de Defesa: Funções de gerenciamento de riscos e conformidade

As instâncias de segunda linha de defesa estão situadas ao nível da gestão e objetivam assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada.

Segundo o IIA (2013), as funções específicas variam nos diversos tipos de organizações, mas funções típicas dessa segunda linha de defesa incluem uma:

- Função (e/ou comitê) de gerenciamento de riscos que facilite e monitore a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional e auxilie os proprietários dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização.
- Função de conformidade que monitore diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis. Nesse quesito, a função separada reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade.
- Função de controladoria que monitore os riscos financeiros e questões de reporte financeiro.

Essas instâncias são destinadas a apoiar o desenvolvimento dos controles internos e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da

primeira linha de defesa, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento.

Como exemplo, no Poder Executivo Federal, os Assessores e Assessorias Especiais de Controle Interno - AECI nos Ministérios integram a segunda linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações.

3ª Linha de Defesa: Auditoria Interna

Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização. Esse alto nível de independência não está disponível na segunda linha de defesa.

A auditoria interna provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle.

Na Administração Pública Federal, considerando que os órgãos não possuem auditoria interna em sua estrutura, o responsável por essa 3ª linha de defesa é o Ministério da Transparência e Controladoria-Geral da União – CGU, que é considerada a auditoria interna do Poder Executivo Federal.

Segundo **o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal**, a terceira linha de defesa presta serviços de avaliação e de consultoria com base nos pressupostos de autonomia técnica e de objetividade, devendo ser desempenhada com o propósito de contribuir para o aprimoramento das políticas públicas e a atuação das organizações que as gerenciam. Os destinatários desses serviços são a Alta Administração, os gestores das organizações e entidades públicas federais e a sociedade.

Por fim, especificamente em relação aos riscos, essa linha de defesa deve (Deloitte, 2014):

- Executar testes independentes e avaliar se a estrutura de apetite de risco, políticas de risco, procedimentos de risco e controles relacionados estão funcionando como previsto.
- Fornecer avaliação à administração quanto à qualidade e eficácia do programa de gerenciamento de riscos, incluindo apetite a riscos.

ANEXO B – GLOSSÁRIO

Accountability – obrigação dos agentes e das organizações que gerenciam recursos públicos de assumir integralmente as responsabilidades por suas decisões e pela prestação de contas de sua atuação de forma voluntária, inclusive sobre as consequências de seus atos e omissões (IN CGU Nº 3, 09 de junho de 2017).

Análise de riscos – compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia (ABNT, 2018).

Apetite a risco – quantidade de risco em nível amplo que uma organização está disposta a aceitar na busca de seus objetivos (INTOSAI, 2007). Quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir (ABNT, 2009a).

Avaliação de risco – envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional.

Controles (Sistema de Controle) – processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos (Decreto Nº 9.203/2017).

Controles Detectivos – são controles desenhados para detectar erros (intencionais e não-intencionais) que já ocorreram, seu enfoque é “a posteriori”.

Controles internos da gestão – conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que na consecução da missão da entidade os seguintes objetivos gerais serão alcançados: (i) execução ordenada, ética, econômica, eficiente e eficaz das operações; (ii) cumprimento das obrigações de *accountability*; (iii) cumprimento das leis e regulamentos aplicáveis; e (iv) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.

Controles Preventivos – são controles desenhados para prevenir a ocorrência de erros (intencionais e não-intencionais), seu enfoque é “a priori”.

Ética – refere-se aos princípios morais, sendo pré-requisito e suporte para a confiança pública.

Evento – um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a implementação da estratégia e a realização de objetivos de modo negativo, positivo ou ambos (INTOSAI, 2007). Eventos com impacto negativo representam riscos. Eventos com impacto

positivo representam oportunidades; ocorrência ou mudança em um conjunto específico de circunstâncias, podendo consistir em alguma coisa não acontecer. A expressão “eventos potenciais” é muitas vezes utilizada para caracterizar riscos (ABNT, 2009).

Fraude – ato ou omissão intencional concebido por um ou mais indivíduos, responsáveis pela governança, empregados ou terceiros, para obter vantagem ilícita, em prejuízo alheio, caracterizado pela desonestidade, dissimulação ou quebra de confiança (IN CGU Nº 3, 09 de junho de 2017 e NBC T 11 - IT - 03 - fraude e erro).

Gestão de Riscos – conjunto de princípios, estruturas, alçadas, processos e atividades coordenados para dirigir e controlar uma organização no que se refere a riscos.

Governança Pública – conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (Decreto nº 9.203/2017).

Impacto – efeito resultante da ocorrência do evento de risco.

Indicadores – “medidas, de ordem quantitativa ou qualitativa, dotada de significado particular e utilizada para organizar e captar as informações relevantes dos elementos que compõem o objeto da observação. É um recurso metodológico que informa empiricamente sobre a evolução do aspecto observado” (Brasil, 2010, p. 21).

Indicadores-chaves de desempenho – número, percentagem ou razão que mede um aspecto do desempenho na realização de objetivos estratégicos e operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização, com o objetivo de comparar esta medida com metas preestabelecidas (TCU, 2010).

Indicadores-chaves de risco – número, percentagem ou razão estabelecido para monitorar as variações no desempenho em relação à meta para o cumprimento de objetivos estratégicos e operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização (TCU, 2010).

Risco à Integridade – *efeito da incerteza relacionado a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores e padrões preconizados pela Instituição e a realização de seus objetivos.*

Matriz de risco – matriz gráfica que exprime o conjunto de combinações de probabilidade e impacto de riscos para classificar os níveis de risco.

Medidas de contingência – ações previamente planejadas que devem ser executadas caso um ou mais riscos se concretizem visando mitigar os impactos.

Monitoramento – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. Monitoramento pode ser aplicado a riscos, a controles, à estrutura de gestão de riscos e ao processo de gestão de riscos.

Nível de risco – magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências [impacto] e de suas probabilidades (ABNT, 2009).

Política de gestão de riscos – documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis em todos os níveis, dentre outros aspectos (ABNT, 2009).

Primeira Linha de Defesa – responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos destinados a garantir que as atividades sejam realizadas de acordo com as metas e objetivos da organização; contempla os controles primários, que devem ser instituídos e mantidos pelos gestores responsáveis pela implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio (IN CGU Nº 3, 09 de junho de 2017).

Probabilidade – medida da possibilidade de ocorrência de um evento de risco.

Respostas a risco – opões e ações gerenciais para tratamento de riscos. Inclui evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco porque o risco está além do apetite a risco da organização e outra resposta não é aplicável; transferir o risco a outra parte ou compartilhar o risco com outra parte; aceitar o risco por uma escolha consciente; ou mitigar o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências (INTOSAI, 2007).

Risco – possibilidade de um evento ocorrer e afetar adversamente a realização de objetivos (COSO GRC, 2004); efeito da incerteza nos objetivos (ABNT, 2018); possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade (IN CGU Nº 3, 09 de junho de 2017).

Risco inerente – risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto (IN CONJ. CGU/MP Nº 001, 10 de maio de 2016).

Risco residual – risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (IN CONJ. CGU/MP Nº 001, 10 de maio de 2016).

Segunda Linha de Defesa – Situada ao nível da gestão e objetivam assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada. Destinadas a apoiar o desenvolvimento dos controles internos da gestão e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da primeira linha de defesa, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento (IN CGU Nº 3, 09 de junho de 2017).

Terceira Linha de Defesa – representada pela atividade de auditoria interna governamental, que presta serviços de avaliação e de consultoria com base nos pressupostos de autonomia técnica e de objetividade (IN CGU Nº 3/2017).

Tolerância a Risco - representa a variação aceitável em desempenho, intimamente ligada com apetite a risco.

Valor público – produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos (Decreto Nº 9.203/2017).