TRIBUNAL DE CONTAS DA UNIÃO

Referencial básico de GESTÃO DE RISCOS

República Federativa do Brasil
Tribunal de Contas da União

Ministros

Raimundo Carreiro (Presidente)
José Múcio Monteiro (Vice-presidente)
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Ana Arraes
Bruno Dantas
Vital do Rêgo

Ministros-Substitutos

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

Ministério Público junto ao TCU

Cristina Machado da Costa e Silva (Procuradora-Geral)
Lucas Rocha Furtado (Subprocurador-geral)
Paulo Soares Bugarin (Subprocurador-geral)
Marinus Eduardo De Vries Marsico (Procurador)
Júlio Marcelo de Oliveira (Procurador)
Sérgio Ricardo Costa Caribé (Procurador)
Rodrigo Medeiros de Lima (Procurador)
República Federativa do Brasil
Tribunal de Contas da União

TRIBUNAL DE CONTAS DA UNIÃO

Referencial básico de GESTÃO DE RISCOS

SEGECEX/COGER

ABRIL - 2018

TRIBUNAL DE CONTAS DA UNIÃO

RESPONSABILIDADE PELO CONTEÚDO
Tribunal de Contas da União
Coordenação-Geral de Controle Externo de Resultado de Políticas e Programas Públicos e Secretaria de Métodos e Suporte ao Controle Externo da Secretaria-Geral de Controle Externo.

Brasil. Tribunal de Contas da União.
Referencial básico de gestão de riscos / Tribunal de Contas da União. – Brasília : TCU, Secretaria Geral de Controle Externo (Segecex), 2018.
154 p. : il.
Inclui glossário com a definição dos principais termos utilizados.
1. Administração pública – governança. 2. Administração pública - eficiência. 3. Gestão de riscos. 4. Controle interno. I. Título.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa.

APRESENTAÇÃO

A sociedade anseia por uma administração pública ágil e eficiente, capaz de implementar políticas e programas de governo que entreguem o melhor valor para a população.

Todavia, não raras vezes essas expectativas são frustradas e, ao se analisarem as causas por trás das dificuldades da administração pública em corresponder a esses anseios, depara-se não apenas com restrições orçamentárias e deficiências de diferentes naturezas, mas principalmente com a baixa capacidade para lidar com riscos.

Diante desse cenário, a gestão e o controle da aplicação dos recursos públicos com base em risco têm sido recomendações recorrentes deste Tribunal, conquanto reconheça o fato de ser um desafio para a gestão das organizações públicas determinar o quanto de risco aceitar na busca do melhor valor para os cidadãos.

Apesar de não ser nova a discussão sobre a necessidade de gerenciar riscos no setor público, isso ainda é um paradigma a ser atingido. Persiste a necessidade não apenas de estruturas e processos, mas também de uma cultura de gerenciamento de riscos, a fim de contribuir para que a organização obtenha resultados com desempenho otimizado.

Um caminho para se atingir um elevado nível de compromisso com a governança de riscos e sua consideração na definição da estratégia e dos objetivos em todos os níveis da administração pública está claramente delineado na política de governança estabelecida no Decreto 9.203/2017, e também previsto no Projeto de Lei 9.163/2017, ambos construídos com a colaboração desta Corte de Contas.

Assim, é com satisfação que apresento o "Referencial Básico de Gestão de Riscos", com o objetivo de prover orientações técnicas aos responsáveis pela governança e gestão das organizações públicas.

Minha expectativa – e a dos demais integrantes do Tribunal de Contas da União – é que esta publicação seja útil na incorporação de boas práticas de gestão de riscos nas instituições, com vistas a ajudar os gestores a implementar o novo marco regulatório da governança pública.

Ministro RAIMUNDO CARREIRO
Presidente do TCU

SUMÁRIO

CAPÍTULO 1

FUNDAMENTOS DE GESTÃO DE RISCOS

CAPÍTULO 1
FUNDAMENTOS DE GESTÃO DE RISCOS

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

Os riscos existem independentemente da atenção que damos a eles. Seja na nossa vida cotidiana, seja no mundo corporativo, estamos imersos em ambiente repleto de riscos, oportunidades e ameaças que, se não gerenciados, podem comprometer o alcance de objetivos almejados.

A cada tomada de decisão, a cada movimento que executamos, ou deixamos de executar, alteramos a probabilidade de ocorrência de eventos futuros e, por conseguinte, ampliamos ou reduzimos o nível de riscos a que estamos expostos.

Na vida, existem pessoas com maior apetite a riscos, que se dispõem a aceitar maiores níveis de risco por avaliarem que os impactos positivos superam os negativos. No extremo oposto, há pessoas que não se sentem confortáveis com possíveis efeitos da incerteza sobre seus objetivos.

Desse modo, diante de um mesmo risco pessoas podem ter reações diferentes, a depender de sua maturidade e experiências pregressas, de sua capacidade de evitar, mitigar ou potencializar sua ocorrência, bem como de reduzir ou tolerar seu impacto.

Em geral, à medida que amadurecemos tomamos maior consciência do ambiente em que estamos inseridos, ficamos mais hábeis na identificação de vulnerabilidades (falhas ou fraquezas), mais aptos a identificar ameaças e oportunidades e, portanto, mais prontos a identificar eventos que podem impactar o alcance de nossos objetivos.

Ao analisarmos o ambiente em que estamos inseridos, e tendo em vista os objetivos estabelecidos, podemos decidir acerca de quais medidas ou controles internos podem ser adotados para tratar os potenciais riscos de sorte a mantê-los em níveis compatíveis com nosso apetite (aceitação) e tolerância (resiliência).

Considerando que não existe risco zero, é bom lembrar que restam, ao final da adoção das medidas mitigadoras, riscos residuais que precisam ser monitorados e mantidos dentro de limites compatíveis com os critérios de risco estabelecidos.

ROTEIRO BÁSICO PARA GESTÃO DE RISCOS

Cientes destes conceitos iniciais, convidamos você a refletir acerca de um empreendimento no qual esteja envolvido e a responder às seguintes questões:

1. Que empreendimento você deseja proteger ou ver bem-sucedido? Pode ser um projeto, um processo, um departamento, uma organização, uma política.

2. Quais são os objetivos desse empreendimento?

3. Que fatores (fraquezas, ameaças, erros, falhas...) podem afetar o alcance desses objetivos?

4. Que riscos podem se originar da ocorrência desses fatores?

5. Qual seria a probabilidade e o impacto da ocorrência de cada um desses riscos se nada tivesse sido feito para mitigá-los até o momento? Calcule o nível de risco inerente (probabilidade inicial x impacto inicial).

6. Qual é o seu apetite e a sua tolerância a risco? Qual nível de risco você considera aceitável?

7. Quais medidas mitigadoras já foram adotadas e que controles internos já estão implantados? Qual a eficácia dessas medidas e controles? Algum deles pode ser eliminado?

8. Que outras medidas mitigadoras e controles internos podem ser adotados para adequar o nível de risco ao apetite e à tolerância a risco?

9. Qual é a probabilidade e o impacto esperado da ocorrência desses riscos após a avaliação de eficácia e adequação das medidas mitigadoras e controles internos? Calcule o nível de risco residual (nível de risco inerente x risco de controle).

10. Com que frequência esses riscos devem ser monitorados?

11. Quem são os responsáveis por monitorar os riscos? Quem deve ser comunicado acerca desses? Com que frequência isso deve ser feito e por quais mecanismos?

Note que as questões supracitadas explicitam uma das possíveis formas de se gerenciar riscos. A literatura é rica em modelos, técnicas, ferramentas e estudos que podem, a depender da necessidade,

produzir análises mais simples ou robustas, mais genéricas ou específicas, mais gerais ou precisas. Cabe a cada pessoa e organização, à luz do seu contexto, escolher os modelos e instrumentos que melhor se adequem à sua necessidade. ■

CAPÍTULO 2

MODELOS DE GESTÃO DE RISCOS

CAPÍTULO 2
MODELOS DE GESTÃO DE RISCOS

Gestão de riscos consiste em um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. É o processo que visa conferir razoável segurança quanto ao alcance dos objetivos.

Para lidar com riscos e aumentar a chance de alcançar objetivos, as organizações adotam desde abordagens informais até abordagens altamente estruturadas e sistematizadas de gestão de riscos, dependendo de seu porte e da complexidade de suas operações.

Adotar padrões e boas práticas estabelecidos em modelos reconhecidos é uma maneira eficaz de estabelecer uma abordagem sistemática, oportuna e estruturada para a gestão de riscos, que contribua para a eficiência e a obtenção de resultados consistentes (ABNT, 2009), evitando que a organização seja aparelhada com uma coleção de instrumentos e procedimentos burocráticos, descoordenados, que podem levar à falsa impressão da existência de um sistema de gestão de riscos e controle efetivo, mas que, na prática, não garantem os benefícios desejados.

Este capítulo apresenta os principais modelos reconhecidos internacionalmente, que são utilizados pelas organizações para implementar a gestão de riscos de forma consistente e sistematizada.

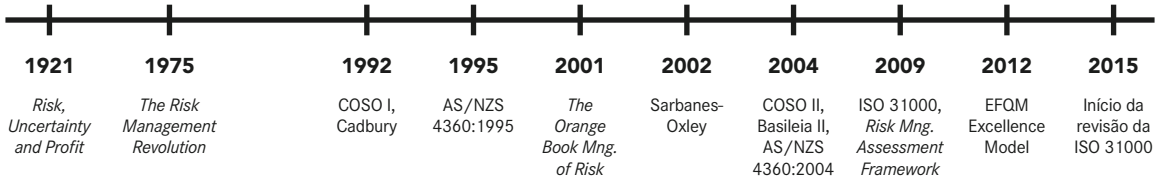
EVOLUÇÃO HISTÓRICA

Em termos históricos a gestão de riscos pode ser rastreada à época em que os primeiros chefes de clãs decidiram fortificar muralhas, realizar alianças com outras tribos e estocar provisões para o futuro.

Segundo Hubbard (2009), práticas relacionadas com a mitigação de riscos existiam na antiga Babilônia, a exemplo de indenizações em caso de perdas por roubos e inundações, ou a seleção, feita pelos primordiais banqueiros, de devedores com maior capacidade de honrar seus empréstimos.

No período recente, atribui-se a Frank Knight a publicação, em 1921, de obra (*Risk, Uncertainty and Profit*) que se tornou referência por estabelecer conceitos, definir princípios e introduzir alguma sistematização ao tema (FRASER; SIMKINS, 2010).

■ **Figura 1:** Linha do tempo



Cinquenta anos depois, em 1975, a revista Fortune publicou o artigo *The Risk Management Revolution*, um dos primeiros documentos a tratar o tema sob o enfoque corporativo e a atribuir à alta administração a responsabilidade por instituir políticas, supervisionar e coordenar as várias funções de riscos existentes em uma organização (FRASER; SIMKINS, 2010).

No início dos anos 90, as bases para o que conhecemos como gestão de risco foram estabelecidas, mediante a publicação de três documentos que se tornaram referência mundial no tema: o COSO I, o Cadbury e a AS/NZS 4360:1995.

O *guia Internal Control - Integrated Framework* (COSO I), publicado em 1992 pelo *Committee of Sponsoring Organizations of the Treadway Commission* – COSO, consolidou a ideia de gestão de risco corporativo e apresentou um conjunto de princípios e boas práticas de gestão e controle interno (COSO, 1992).

No mesmo ano, o relatório do Comitê Cadbury, do Reino Unido, atribui ao corpo governante superior das entidades a responsabilidade por definir a política de gestão de riscos, supervisionar o processo de gestão e assegurar que a organização entenda os riscos aos quais está exposta (CADBURY, 1992).

Em 1995, esforço conjunto das entidades padronizadoras *Standards Australia e Standards New Zealand* resulta na publicação do primeiro modelo padrão oficial para a gestão de riscos, a norma técnica *Risk Management Standard*, AS/NZS 4360:1995. Nos anos que se seguiram, normas técnicas semelhantes foram publicadas no Canadá, no Reino Unido e em outros países.

No início do Século XXI, houve a consolidação e disseminação de práticas de gestão de risco corporativo. Entre as publicações que se tornaram referências internacionais no tema estão: o *The Orange Book*, a lei Sarbanes-Oxley, o COSO-ERM, o Acordo de Basileia II, a AS/NZS 4360:2004 e a ISO 31000:2009.

O *The Orange Book - Management of Risk - Principles and Concepts*[1], produzido e publicado pelo *HM Treasury* Britânico, foi a principal referência do programa de gestão de riscos do governo do Reino Unido, iniciado em 2001. O modelo tem como vantagens, além de ser compatível com padrões internacionais de gestão de riscos, introduzir e tratar esse tema complexo de forma simples e abrangente.

Em 2002, um ano após o colapso da empresa Enron, decorrente de esquema gigantesco de ocultação e manipulação de dados contábeis e falhas em auditorias, os Estados Unidos aprovaram a chamada Lei Sarbanes-Oxley. Por meio dela, buscaram mitigar riscos, evitar a ocorrência de fraudes, proteger investidores e assegurar que as empresas que participam do mercado acionário norte-americano possuam estruturas e mecanismos adequados de governança (USA, 2002).

Em 2004, o COSO publicou o *Enterprise Risk Management - Integrated Framework* (conhecido como COSO-ERM ou COSO II), modelo de referência que estendeu o COSO I, tendo como foco a gestão de riscos corporativos.

No mesmo ano foi firmado o Acordo de Basileia II, aplicável a instituições bancárias em nível mundial, contendo requisitos específicos relacionados à gestão de riscos operacionais (BCBS, 2004). Ainda em 2004 foi lançada versão atualizada e expandida da norma AS/NZS 4360 (AUSTRÁLIA, 2004).

Em 2009 foi publicada a norma técnica ISO 31000 *Risk Management – Principles and Guidelines*, que provê princípios e boas práticas para um processo de gestão de riscos corporativos, aplicável a organizações de qualquer setor, atividade e tamanho (ABNT, 2009) e é hoje uma das principais referências mundiais no tema. O modelo preconizado na ISO 31000 aprimorou os conceitos, as diretrizes e as práticas recomendadas em normas técnicas de aplicação local que a precederam, como a AS/NZS 4360. A partir de 2015 iniciou-se o processo de revisão da ISO 31000 pelo Comitê Técnico da ISO ISO/TC 262/WG2.

1 Com base no Orange Book, o Ministério do Planejamento, Orçamento e Gestão produziu o Guia de Orientação para o Gerenciamento de Riscos, para apoiar o Modelo de Excelência do Sistema de Gestão Pública (GESPÚBLICA) e prover uma introdução ao tema gerenciamento de riscos (BRASIL, 2013).

MODELOS INTERNACIONAIS

A implantação e o aprimoramento da gestão de riscos em uma organização constituem um processo de aprendizagem, que começa com o desenvolvimento de consciência sobre a importância de gerenciar riscos e avança com a implementação de práticas e estruturas necessárias.

O ápice desse processo se dá quando a organização conta com uma abordagem sistêmica e consistente para gerenciar riscos e com uma cultura organizacional profundamente consciente dos princípios e práticas da gestão de riscos.

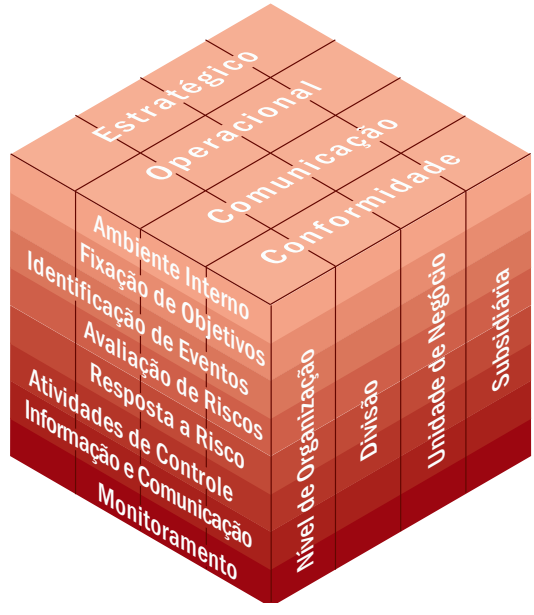
Para facilitar o alcance desses objetivos, sugere-se, sempre que possível, observar os modelos existentes, lembrando que a aplicação de um modelo deve considerar o princípio básico de que a gestão de riscos deve ser feita sob medida, alinhada com o contexto interno e externo da organização e com o seu perfil de risco (ABNT, 2009).

A seguir são apresentados quatro modelos de referência que devem ser estudados e conhecidos antes da institucionalização da gestão de risco no âmbito de uma organização, seja ela pública ou privada. São eles: (a) COSO II – Gerenciamento de Riscos Corporativos – Estrutura Integrada; (b) COSO GRC 2016 – Alinhando Risco com Estratégia e Desempenho; (c) ISO 31000 – Gestão de Riscos – Princípios e Diretrizes; e (d) *Orange Book e Risk Management Assessment Framework*.

Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO II)

Trata-se de modelo de gestão de riscos predominante no cenário corporativo internacional, especialmente na América do Norte, desenvolvido pela PricewaterhouseCoopers LLP, sob encomenda do COSO, com o propósito de fornecer estratégia de fácil utilização pelas organizações para avaliar e melhorar a gestão de riscos.

O modelo é apresentado na forma de matriz tridimensional (cubo), demonstrando uma visão integrada dos componentes que os gestores precisam adotar para gerenciar os riscos de modo eficaz, no contexto dos objetivos e da estrutura de cada organização.



■ **Figura 2:** Modelo de Gestão de Riscos previstos no COSO II.

Observe-se que a **face superior** do cubo apresenta as categorias de **objetivos** que são comuns a todas as organizações e que a gestão de riscos deve fornecer segurança razoável de seu alcance; a **face lateral esquerda** indica os **componentes** que devem estar presentes e funcionando de modo integrado à rotina da organização para que a gestão de riscos seja eficaz; e a **face lateral direita** representa a **estrutura organizacional**, os diversos níveis e/ou funções da organização, incluindo projetos, processos e demais atividades que concorrem para a realização dos seus objetivos.

Alinhando risco com estratégia e desempenho (COSO GRC)

Em junho de 2016, o COSO colocou em consulta pública uma revisão do modelo de 2004, adotando um novo título – "Alinhando Risco com Estratégia e Desempenho" – para destacar a importância da gestão de riscos na definição e na execução da estratégia e na gestão do desempenho organizacional. Com a incorporação dessa perspectiva, o modelo proporciona maior alinhamento às expectativas em torno das responsabilidades das instâncias de governança e da alta administração no cumprimento das suas obrigações de *accountability*.

O COSO GRC revisa e atualiza os componentes do COSO II, adota princípios, simplifica suas definições, enfatiza o papel da cultura e melhora o foco no valor, isto é, como as organizações criam, preservam e realizam valor, inserindo a gestão de riscos em três dimensões que são fundamentais à gestão de uma organização: (1) missão, visão e valores centrais; (2) objetivos estratégicos e de negócios; e (3) desempenho organizacional.

■ **Figura 3:** Modelo de gestão de riscos COSO GRC 2016 em consulta pública (COSO, 2016, tradução livre).

O modelo explora a gestão da estratégia e dos riscos corporativos a partir de três perspectivas diferentes, tornando mais claras as responsabilidades da governança e da alta administração no seu papel de supervisionar e no seu dever de se envolver no processo de gerenciamento do risco corporativo de modo efetivo. As perspectivas exploradas são: (a) a possibilidade de que os objetivos estratégicos e de negócios não se alinharem com a missão, a visão e os valores centrais da organização; (b) as implicações da estratégica escolhida; e (c) os riscos para a execução da estratégia.

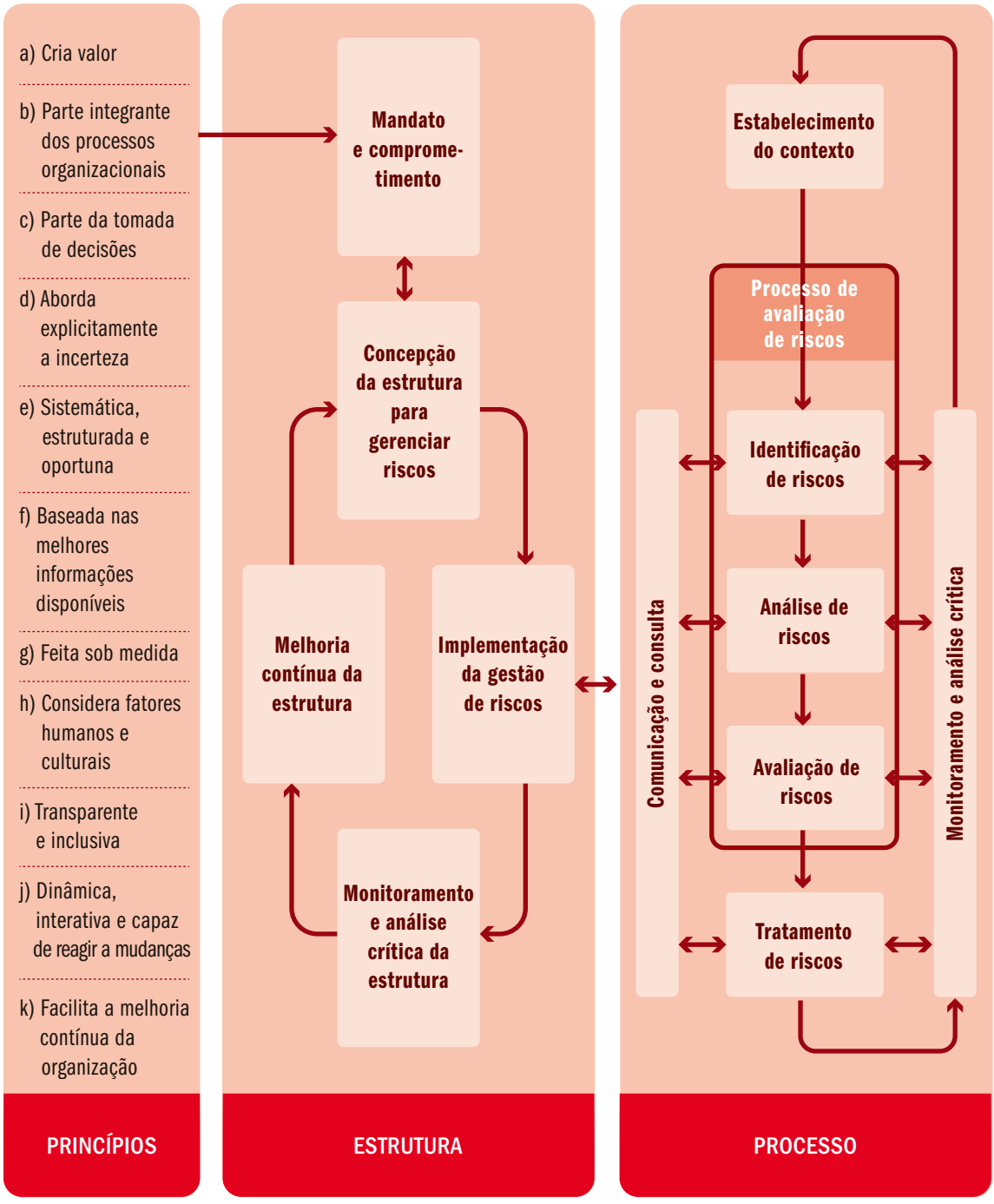
O novo modelo melhora o alinhamento da gestão de riscos com a gestão do desempenho, explorando como as práticas de gestão de riscos apoiam a identificação e avaliação de riscos que impactam o desempenho, elevando a necessidade de definir variações aceitáveis no desempenho, também denominadas tolerâncias a risco, em nível de princípio.

O modelo revisado reduz de oito para cinco os componentes da gestão de riscos: (1) governança e cultura; (2) estratégia e definição de objetivos; (3) desempenho; (4) revisão e correção; e (5) informação, comunicação e reporte.

Associados aos componentes, foram adotados vinte princípios de gestão de riscos, que representam as práticas que podem ser aplicáveis de diferentes maneiras por diferentes organizações, independentemente de tamanho ou setor, cuja implementação permitirá que a governança e a administração tenham uma expectativa razoável de que a organização entende e é capaz de gerenciar os riscos associados com a estratégia e os objetivos de negócio, em um nível aceitável.

Gestão de Riscos – Princípios e Diretrizes (ISO 31000)

A ISO 31000 fornece princípios e diretrizes para gerenciar qualquer tipo de risco em toda ou em parte de qualquer tipo de organização. Trata-se de uma norma geral, independentemente de indústria, setor ou área e não concorre com outras normas sobre gestão de riscos em áreas específicas. Busca servir como um guia mestre em matéria de gestão de riscos e harmonizar os processos de gestão de riscos, fornecendo uma abordagem comum, que pode ser aplicada a uma ampla gama de atividades, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos (ABNT, 2009).



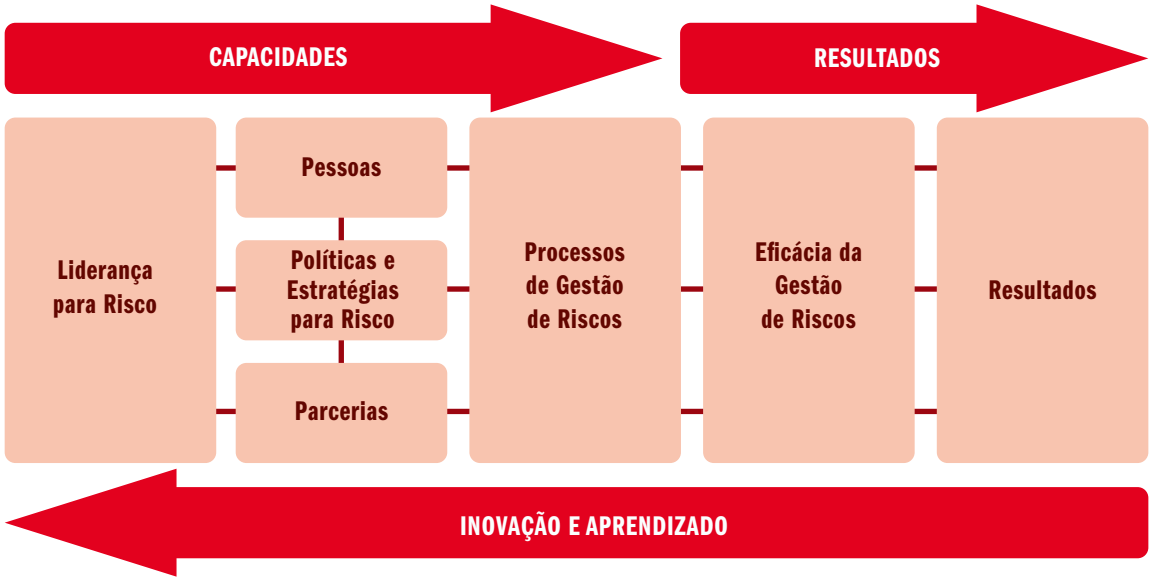
■ **Figura 4:** Relação entre princípios, estrutura e processo de gestão de risco (ABNT, 2009).

A norma ISO 31000 está estruturada em três partes fundamentais inter-relacionadas: os princípios, a estrutura e o processo de gestão de riscos. Uma contribuição fundamental da ISO 31000 é o processo de gestão de riscos, cujo propósito é fornecer uma abordagem comum para a aplicação sistemática de políticas, procedimentos e práticas de gestão de riscos.

Orange Book e Risk Management Assessment Framework

O *The Orange Book Management of Risk - Principles and Concepts*, produzido e publicado pelo HM Treasury Britânico, foi a principal referência do programa de gestão de riscos do governo do Reino Unido, iniciado em 2001. O modelo tem como vantagens, além de ser compatível com padrões internacionais de gestão de riscos, como COSO e ISO 31000, apresentar uma introdução ao tema gestão de riscos, tratando um assunto complexo de forma abrangente e simples.

Em 2009, oito anos após a edição do Orange Book, o governo britânico divulgou o *Risk Management Assessment Framework: a Tool for Departments* (UK, 2009), uma ferramenta para aferir a gestão de riscos nas organizações governamentais daquele país e identificar oportunidades de melhoria, a qual deriva de um modelo de excelência de gestão consolidado e utilizado por mais de trinta mil organizações, principalmente na Europa – *The EFQM Excellence Model* (EFQM, 2012). A ferramenta é estruturada em sete componentes, podendo ser utilizada tanto por auditores como ser autoaplicada pelos gestores.



■ **Figura 5:** Modelo de avaliação da gestão de riscos do Reino Unido (REINO UNIDO, 2009).

Esse modelo foi selecionado para integrar a base conceitual do modelo de avaliação da maturidade em gestão de riscos que se verá adiante, por ter sido desenvolvido especificamente para organizações públicas e por incorporar o componente denominado parcerias[2], considerado relevante para as características do setor público. ■

2 Quando o ente público se vale de outros agentes para alcançar seus objetivos e resultados pretendidos (BRASIL, 2013).

CAPÍTULO 3

PROCESSO DE GESTÃO DE RISCOS

CAPÍTULO 3
PROCESSO DE GESTÃO DE RISCOS

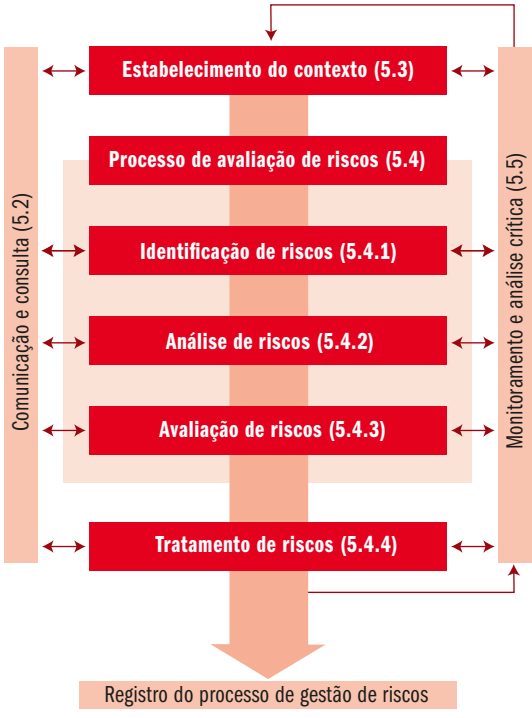
Este capítulo descreve o processo de gestão de riscos com fundamento na norma ISO 31000. Observe-se que as etapas do processo de gestão de riscos são basicamente as mesmas nos diversos modelos citados neste referencial, com algumas variações terminológicas (por exemplo, o COSO II denomina "resposta a risco" o que a ISO 31000 chama de "tratamento de riscos").

O processo de gestão de riscos envolve a identificação, a análise e a avaliação de riscos, a seleção e a implementação de respostas aos riscos avaliados, o monitoramento de riscos e controles, e a comunicação sobre riscos com partes interessadas, internas e externas. Esse processo é aplicado a uma ampla gama das atividades da organização, em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura de gestão de riscos da entidade.

Ressalte-se que a documentação das atividades realizadas durante o processo de gestão de riscos constitui importante instrumento de *accountability*[3], além de facilitar a comunicação com as partes interessadas. Por essa razão, na descrição de cada etapa do processo, indicamos alguns tipos de documentos e informações essenciais que convém armazenar como parte do registro de riscos.

Considerando que a proposta da ISO 31000 é harmonizar os processos de gestão de riscos entre os diversos modelos, fornecendo uma abordagem comum para aplicação em ampla gama de atividades, utilizaremos o modelo desta norma para descrever o processo de gestão de riscos, que compreende as atividades descritas nas subseções 5.2 a 5.6 da norma ABNT NBR ISO 31000:2009.

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



■ **Figura 6:** Processo de gestão de riscos da ISO 31000 (adaptado de ABNT, 2009).

COMUNICAÇÃO E CONSULTA

Durante todas as etapas ou atividades da aplicação do processo de gestão de riscos deve haver comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para: (a) auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração; (b) auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização; e (c) garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos.

Convém que seja desenvolvido um plano de comunicação e realizada consulta interna e externa para apoiar essa atividade, seja por meio de documento formal ou de lista de verificação.

ESTABELECIMENTO DO CONTEXTO

O estabelecimento do contexto envolve o entendimento da organização, dos objetivos e do ambiente, inclusive do controle interno, no qual os objetivos são perseguidos, com o fim de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização para atingir seus objetivos, bem como fornecer parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas.

Contexto é o ambiente no qual a organização busca atingir os seus objetivos. Os objetivos são a essência da definição do contexto, pois a gestão de riscos ocorre no contexto dos objetivos da organização.

O conceito de organização aqui pode se referir a toda entidade ou parte dela, a um processo, como o planejamento estratégico, ou a projetos, processos de trabalho, operações, funções, decisões, produtos, serviços e ativos (ABNT, 2009). Assim, caso a gestão de risco seja aplicada a processo, projeto ou

atividade, os objetivos do processo, do projeto ou da atividade devem ser considerados no contexto dos objetivos da organização como um todo, de modo a assegurar que os riscos significativos do objeto da gestão de riscos sejam identificados.

Um dos primeiros passos da atividade de estabelecimento do contexto é identificar os fatores do ambiente, interno e externo, no qual a organização persegue seus objetivos. Não menos importante é a identificação das partes interessadas, bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, pois essas partes interessadas devem ser incluídas em cada etapa ou ciclo do processo de gestão de riscos, por meio do processo de comunicação e consulta, abordado no tópico anterior.

A documentação desta etapa do processo de gestão de riscos é normalmente feita por meio de: (a) relato conciso dos objetivos organizacionais e dos fatores críticos de sucesso para o alcance destes, bem como uma análise dos fatores dos ambientes interno e externo, mediante uma análise SWOT, por exemplo; (b) análise das partes interessadas e seus interesses, com o uso de ferramentas tais como análise de *stakeholder*, matriz RECI (RACI *matrix* ou *chart*, em inglês) e matriz de responsabilidades; e (c) conjunto de critérios mais importantes para analisar e avaliar os níveis de risco: escalas de probabilidade; escalas de consequências ou impactos; como será determinado se o nível de risco é tolerável ou aceitável e se novas ações de tratamento são necessárias, isto é, diretrizes para priorização e tratamento de riscos.

IDENTIFICAÇÃO DE RISCOS

A identificação de riscos é o processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido e apoiando-se na comunicação e consulta com as partes interessadas internas e externas (ABNT, 2009). O objetivo é produzir uma lista abrangente de riscos, incluindo fontes e eventos de risco que possam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto.

Em muitos casos, a identificação de riscos em múltiplos níveis é útil e eficiente. Em etapa inicial ou preliminar, pode-se adotar uma abordagem de identificação de riscos *top-down*, que vai do geral para o específico. Primeiro, identificam-se riscos em um nível geral ou superior como ponto de partida para se estabelecer prioridades para, em segundo momento, identificarem-se e analisarem-se riscos em nível específico e/ou mais detalhado. Pode-se, por exemplo, primeiramente identificar riscos aos objetivos estratégicos e, posteriormente, riscos que afetam processos prioritários.

A identificação de riscos pode basear-se em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, assim como em necessidades das partes interessa-

das. Convém que pessoas com conhecimento adequado sejam envolvidas na identificação de riscos e que a organização utilize ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, às suas capacidades e aos riscos enfrentados (ABNT, 2009). Envolver a equipe também ajuda a criar a responsabilidade em relação ao processo de gestão de riscos e o comprometimento em relação ao tratamento dos riscos.

A documentação dessa etapa geralmente inclui: (a) o escopo do processo, projeto ou atividade coberto pela identificação; (b) os participantes do processo de identificação dos riscos; (c) a abordagem ou o método utilizado para identificação dos riscos e as fontes de informação consultadas; e (d) descrição de cada risco, pelo menos com a fonte de risco, as causas, o evento e as consequências.

ANÁLISE DE RISCOS

A análise de riscos é o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos (ABNT, 2009).

O risco é uma função tanto da probabilidade como da medida das consequências. Desse modo, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos:

Risco = *f*unção (Probabilidade e Impacto)

O resultado final desse processo será o de atribuir a cada risco identificado uma classificação, tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco, expressas em termos tangíveis ou intangíveis.

Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas, e ser mais ou menos detalhada (ABNT, 2009). O método e o nível de detalhamento da análise podem ser influenciados pelos objetivos, pela natureza do risco, pela disponibilidade de informações e de recursos.

Métodos qualitativos definem o impacto, a probabilidade e o nível de risco por qualificadores como "alto", "médio" e "baixo", com base na percepção das pessoas.

Métodos semiquantitativos usam escalas numéricas previamente convencionadas para mensurar a consequência e a probabilidade, os quais são combinados, por meio de uma fórmula, para produzir o nível de risco. A escala pode ser linear, logarítmica ou de outro tipo. As fórmulas também podem variar de acordo com a necessidade e o contexto.

Métodos quantitativos estimam valores para as consequências e suas probabilidades a partir de valores práticos e calculam o nível de risco a partir de unidades específicas definidas no desenvolvimento do contexto.

Observe-se que a análise quantitativa necessita de dados factuais e, devido à falta dessas informações ou ao grau de esforço exigido, poderá não ser sempre possível ou desejável. Nesses casos, de acordo com a norma NBR ISO/IEC 31010, a utilização de um método qualitativo ou semiquantitativo, baseado na opinião de especialistas, pode ser suficiente e eficaz (ABNT, 2012).

Em análises qualitativas e semiquantitativas, considerando que a lógica subjacente seja que o nível de risco é proporcional tanto à probabilidade como ao impacto, a função 'Risco' será essencialmente um produto dessas variáveis.

Risco = Probabilidade X Impacto

Contudo, essa relação simples pode não refletir relações não lineares, sendo necessário, assim, incluir um fator de ponderação para um dos componentes (probabilidade ou impacto), de modo a atingir a escala relativa necessária entre eles. Além disso, um operador exponencial pode ser necessário para um ou ambos os componentes, como no exemplo a seguir.

Risco = (Probabilidade)^x x (Impacto x fator de ponderação)^y

Em sua forma qualitativa mais elementar, a relação entre os riscos e os seus componentes pode ser ilustrada por meio de uma matriz simples, como a que segue:

■ **Figura 7:** Matriz de riscos simples

A análise qualitativa é geralmente utilizada para realizar uma avaliação inicial de riscos em um nível geral ou superior de modo a estabelecer prioridades para identificação e análise de riscos em nível específico e/ou mais detalhado, bem como quando não se exige precisão quantitativa ou ainda quando dados numéricos, tempo e recursos não estão disponíveis.

Análises semiquantitativas geralmente utilizam escalas, como as exemplificadas a seguir, para estabelecer um entendimento comum das classificações de probabilidades e impactos. Ressalte-se que, em situações reais, essas escalas são construídas de modo compatível com o contexto e os objetivos específicos da atividade objeto da gestão de riscos.

■ **Quadro 1:** Exemplo de Escala de Probabilidades (BRASIL, 2012, adaptado).

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	PESO
Muito baixa	**Improvável.** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	**1**
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	**5**
Alta	**Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	**8**
Muito alta	**Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	**10**

■ **Quadro 2:** Exemplo de Escala de Consequências (BRASIL, 2012, adaptado).

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA	PESO
Muito baixo	**Mínimo** impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	**Pequeno** impacto nos objetivos (idem).	2
Médio	**Moderado** impacto nos objetivos (idem), porém recuperável.	5
Alto	**Significativo** impacto nos objetivos (idem), de difícil reversão.	8
Muito alto	**Catastrófico** impacto nos objetivos (idem), de forma irreversível.	10

Nível de risco inerente

O **nível de risco inerente** (NRI) é o nível de risco antes da consideração das respostas que a Administração adota para reduzir a probabilidade do evento ou os seus impactos nos objetivos, incluindo controles internos. Resulta da combinação da probabilidade com o impacto (no nosso exemplo, por meio de multiplicação).

A política de gestão de riscos da organização geralmente estabelece diretrizes (classes, faixas ou categorias) para classificar os níveis de risco resultantes do processo de análise, sejam inerentes ou residuais, de modo consistente com os limites de exposição aceitáveis pela organização.

■ **Quadro 3:** Exemplo de escala de classificação de risco (elaboração própria).

RB (Risco Baixo)	**RM** (Risco Médio)	**RA** (Risco Alto)	**RE** (Risco Extremo)
0 – 9,99	**10 – 39,99**	**40 – 79,99**	**80 – 100**

Os resultados das combinações de probabilidade e impacto, classificados de acordo com a escala de níveis de risco, podem ser expressos em uma matriz, como a exemplificada adiante.

■ **Quadro 4:** Exemplo de matriz de riscos (BRASIL, 2012, adaptado).

MATRIZ DE RISCOS

IMPACTO						
	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

Segue-se um exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos inerentes (NRI) de alguns riscos identificados, de acordo com o método apresentado.

■ **Quadro 5:** Exemplo de registro de riscos parcial com níveis de risco inerente calculados (BRASIL, 2012, adaptado).

RISCOS IDENTIFICADOS	PROBABILIDADE		IMPACTO		NÍVEL DE RISCO INERENTE (NRI)
Risco 1 – Descrição do risco 1	Alta	8	Muito Alto	10	80 RE (Extremo)
Risco 2 – Descrição do risco 2	Média	5	Alto	8	40 RA (Alto)
Risco 3 – Descrição do risco 3	Baixa	2	Médio	5	10 RM (Médio)
Risco *n* – Descrição do risco *n*	Muito Baixa	1	Médio	5	5 RB (Baixo)

Nível de risco residual

A análise de riscos só se completa quando as ações que a gestão adota para respondê-los são também avaliadas, chegando-se ao **nível de risco residual**, o risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles internos e outras ações. Formas de resposta a riscos podem variar entre aceitar, reduzir, evitar ou compartilhar o risco, incluindo o estabelecimento de atividades de controle para assegurar que as respostas definidas sejam efetivamente aplicadas.

As **atividades de controle** são as ações estabelecidas por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela Administração para mitigar os riscos à realização dos objetivos (COSO, 2013). As atividades de controle também são geralmente referidas como controles internos.

Uma forma de avaliar o efeito dos controles internos na mitigação de riscos consiste em estimar a eficácia de cada controle e deter-

minar um **nível de confiança** (NC), mediante análise dos atributos do desenho e da implementação do controle, conforme exemplo ilustrativo apresentado a seguir.

■ **Quadro 6:** Exemplo de escala para avaliação de controles (adaptado de DANTAS et al, 2010; AVALOS, 2009, adaptado).

NÍVEL DE CONFIANÇA (NC)	AVALIAÇÃO DO DESENHO E IMPLEMENTAÇÃO DOS CONTROLES (ATRIBUTOS DO CONTROLE)	RISCO DE CONTROLE (RC)
Inexistente NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto **1,0**
Fraco NC = 20% (0,2)	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Alto **0,8**
Mediano NC = 40% (0,4)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	Médio **0,6**
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo **0,4**
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	Muito Baixo **0,2**

Observe-se, no exemplo apresentado, que o controle mais bem avaliado recebeu um NC = 80% (0,8). Isso se deve ao fato de que controles têm limitações que lhe são inerentes, como a possibilidade de se tornarem ineficazes pela ação de conluio, de contorno efetuado pela própria Administração ou simplesmente de falhar por erro humano na sua aplicação. Logo, não importa quão efetivo seja o desenho e a implementação de um controle, ele só poderá fornecer uma segurança razoável, nunca absoluta, quanto ao cumprimento dos objetivos para os quais foi concebido. Portanto, nunca se pode atribuir 100% de confiança a um controle.

Uma vez determinado o nível de confiança (NC), pode-se determinar o **risco de controle** (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de

eventos que possam afetar adversamente a realização de objetivos. O RC é definido como complementar ao NC:

Risco de controle = 1 – Nível de confiança

Pela fórmula é possível deduzir que quanto mais eficaz for o projeto e a implementação dos controles, ou seja, quanto maior for o NC, menor será o RC e vice-versa, porém este nunca será "zero", uma vez que aquele nunca poderá ser 100%.

Uma vez estabelecido o RC, é possível estimar o **nível de risco residual** (NRR) que permanece depois de considerado o efeito das respostas adotadas pela gestão. Para isso, deduz-se do nível de risco inerente (NRI) o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo RC, utilizando a seguinte fórmula.

Nível de risco residual = Nível de risco inerente x Risco de controle

Segue-se um exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos residuais (NRR) de alguns riscos identificados, de acordo com o método apresentado, sendo que o valor do NRR foi arredondado para o número inteiro mais próximo.

■ **Quadro 7:** Exemplo de registro de riscos parcial com níveis de risco residual calculados (BRASIL, 2012, adaptado).

RISCOS IDENTIFICADOS	P	I	NÍVEL DE RISCO INERENTE (NRI)	EFICÁCIA DO CONTROLE	RISCO DE CONTROLE (RC)	NÍVEL DE RISCO RESIDUAL (NRR)
Risco 1	Alta - 8	M. Alto - 10	RE - 80	Inexistente	1,0	RE - 80
Risco 2	Média - 5	Alto - 8	RM - 40	Mediano	0,6	RM - 24
Risco 3	Baixa - 2	Alto - 5	RM - 10	Fraco	0,8	RB - 8

Documentação da análise

A documentação da etapa de análise de riscos geralmente inclui: (a) abordagem ou o método de análise utilizado, as fontes de informação consultadas e os participantes do processo de análise; (b) as especificações utilizadas para as classificações de probabilidade e impacto dos riscos; (c) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e sua descrição, bem como considerações quanto à análise desses elementos; (d) a descrição

dos controles internos existentes, as considerações quanto à sua eficácia e o risco de controle; e (e) o nível de risco inerente e o residual.

AVALIAÇÃO DE RISCOS

A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e/ou sua magnitude é aceitável ou tolerável ou se algum tratamento é exigido (ABNT, 2009).

Nessa etapa, portanto, se faz uso da compreensão e do nível do risco obtidos na etapa de análise de riscos para tomar decisões acerca dos riscos analisados, em especial: (a) se um determinado risco precisa de tratamento e a prioridade para isso; (b) se uma determinada atividade deve ser realizada ou descontinuada; e (c) se controles internos devem ser implementados ou, se já existirem, se devem ser modificados, mantidos ou eliminados.

Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento associados aos níveis de risco (nível recomendado de atenção, tempo de resposta requerido, quem deve ser comunicado etc.). Segue-se um exemplo simples.

■ **Quadro 8:** Diretrizes para priorização e tratamento de riscos (BRASIL, 2013a, adaptado).

NÍVEL DE RISCO	CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS
RE	Nível de risco **muito além do apetite a risco**. Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo.
RA	Nível de risco **além do apetite a risco**. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
RM	Nível de risco **dentro do apetite a risco**. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
RB	Nível de risco **dentro do apetite a risco**, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

A documentação desta etapa é importante instrumento de accountability e geralmente consiste em uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades.

TRATAMENTO DE RISCOS

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes. Um dos benefícios da gestão de riscos é o rigor que proporciona ao processo de identificação e seleção de alternativas de respostas aos riscos (ABNT, 2009; COSO, 2006).

Opções de tratamento de riscos incluem evitar, reduzir (mitigar), transferir (compartilhar) e aceitar (tolerar) o risco, devendo-se observar que elas não são mutuamente exclusivas.

a) Evitar o risco é a decisão de não iniciar ou de descontinuar a atividade, ou ainda desfazer-se do objeto sujeito ao risco.

b) Reduzir ou mitigar o risco consiste em adotar medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos. Os procedimentos que uma organização estabelece para tratar riscos são denominados de atividades de controle interno.

c) Compartilhar ou transferir o risco é o caso especial de se mitigar a consequência ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco, mediante contratação de seguros ou terceirização de atividades nas quais a organização não tem suficiente domínio.

d) Aceitar ou tolerar o risco é não tomar, deliberadamente, nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização (e.g. quando o risco é considerado baixo), a capacidade para fazer qualquer coisa sobre o risco é limitada ou, ainda, o custo de tomar qualquer medida é desproporcional em relação ao benefício potencial (e.g. gastar mais recursos financeiros para proteger um ativo do que o próprio valor do ativo).

Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação da medida de mitigação do risco e, de outro, os benefícios decorrentes, levando em consideração que novos riscos podem ser introduzidos pelo tratamento e que existem riscos cujo tratamento preventivo não é economicamente justificável, como riscos de grande consequência negativa, porém com probabilidade muito baixa de acontecer (INTOSAI, 2007; ABNT, 2009).

Uma forma especial de se mitigar riscos é a preparação por meio da gestão da continuidade de negócios. Avaliar essa opção de tratamento é especialmente importante quando ocorrem as seguintes condições: a) o objeto da gestão é atividade ou processo crítico da organização, portanto o impacto é muito alto; b) o evento de risco tem baixa probabilidade, o que poderia levar à falsa impressão de que o nível do risco poderia ser tolerado após a implantação de controles preventivos. Porém, nesses casos, convém assumir que o evento de risco irá se concretizar algum dia e, a depender da criticidade do objeto afetado, avalia-se a necessidade de um controle reativo específico: plano de continuidade do negócio. O objetivo desse tipo de preparação é recuperar o funcionamento da atividade ou processo de trabalho afetado, normalmente em outro local, em tempo hábil e com o nível de desempenho adequado aos objetivos da instituição. Os eventos de riscos que são tratados nesses casos são geralmente catastróficos, a exemplo de: incêndios, inundações, terremotos, epidemias etc. Os principais recursos afetados nesses casos são processos, instalações, equipamentos, pessoas e tecnologia, e o foco das ações será recuperá-los ou substituí-los, independentemente do tipo do evento de risco ou da sua fonte.

Ao avaliar os efeitos das diferentes respostas possíveis, a gestão decide a melhor forma de tratar o risco. A resposta ou combinação de respostas selecionada não precisa necessariamente gerar a quantidade mínima de risco residual, mas se gerar um risco residual acima dos limites de exposição estabelecidos, os gestores terão que reconsiderar a opção de resposta ou rever os limites (INTOSAI, 2007).

O processo de tratamento é cíclico e inclui: a) avaliação do tratamento já realizado; b) avaliação se os níveis de risco residual são toleráveis; c) se não forem, definição e implementação de tratamento adicional; e, d) avaliação da eficácia desse tratamento (ABNT, 2009).

A documentação desta etapa integra o registro de riscos da organização e constitui um plano de tratamento de riscos que deve definir a ordem de prioridade para a implementação de cada ação de tratamento, bem como identificar: (a) as razões para a seleção das opções de tratamento, incluindo os benefícios esperados; (b)os responsáveis pela aprovação e pela implementação do plano; (c) as ações propostas, os recursos requeridos, incluindo arranjos de contingência, e o cronograma; (d) as medidas de desempenho e os requisitos para prestação de informações; e (e) as formas de monitoramento da implementação do tratamento e dos riscos (ABNT, 2009).

MONITORAMENTO E ANÁLISE CRÍTICA

O monitoramento e análise crítica é etapa essencial da gestão de riscos e tem por finalidade: (a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que po-

dem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes; (b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos; (c) analisar eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles; e (d) assegurar que os controles sejam eficazes e eficientes no projeto e na operação (ABNT, 2009).

É importante observar a necessidade de segregação de funções também nas atividades de monitoramento. As responsabilidades relativas ao monitoramento e à análise crítica devem estar claramente definidas na política e detalhadas nos planos, manuais ou normativos da gestão de riscos e contemplam atividades como:

a) **monitoramento contínuo** (ou pelo menos, frequente) pelas funções que gerenciam e têm propriedade de riscos e pelas funções que supervisionam riscos, com vistas a medir o desempenho da gestão de riscos, por meio de indicadores chave de risco, análise do ritmo de atividades, operações ou fluxos atuais em comparação com o que seria necessário para o alcance de objetivos ou manutenção das atividades dentro dos critérios de risco estabelecidos;

b) **análise crítica** dos riscos e seus tratamentos realizada pelas funções que gerenciam e têm propriedade de riscos e/ou pelas funções que supervisionam riscos, por meio de autoavaliação de riscos e controles (*Control and Risk Self Assessment* - CRSA); e

c) **auditorias** realizadas pelas funções que fornecem avaliações independentes, seja por meio de auditoria interna ou externa, focando na estrutura e no processo de gestão de riscos, em todos os níveis relevantes das atividades organizacionais, ou seja, procurando testar os aspectos sistêmicos da gestão de riscos em vez de situações específicas.

As atividades de monitoramento e análise crítica devem assegurar que o registro de riscos seja mantido atualizado, bem como que nele sejam documentados os resultados das ações mencionadas acima. ■

CAPÍTULO 4

TÉCNICAS PARA GESTÃO DE RISCOS

CAPÍTULO 4
TÉCNICAS PARA GESTÃO DE RISCOS

A matriz de riscos é conhecida como "matriz de probabilidade/consequência" e constitui apenas uma das possíveis técnicas que podem ser utilizadas para auxiliar a identificação, análise e avaliação de riscos.

A seguir, descrevem-se sumariamente outras técnicas que podem ser utilizadas por gestores e pelo pessoal envolvido na realização dessas atividades. As três primeiras técnicas listadas possuem natureza basilar e podem servir como alternativas para implementar algumas das demais técnicas aqui citadas.

Ressalte-se que é comum a aplicação de mais de uma técnica sobre certo objeto avaliado, haja vista que cada uma delas tem maior ou menor aplicabilidade às etapas de identificação, análise ou avaliação de riscos, conforme aponta a norma NBR ISO/IEC 31010 (ABNT, 2012).

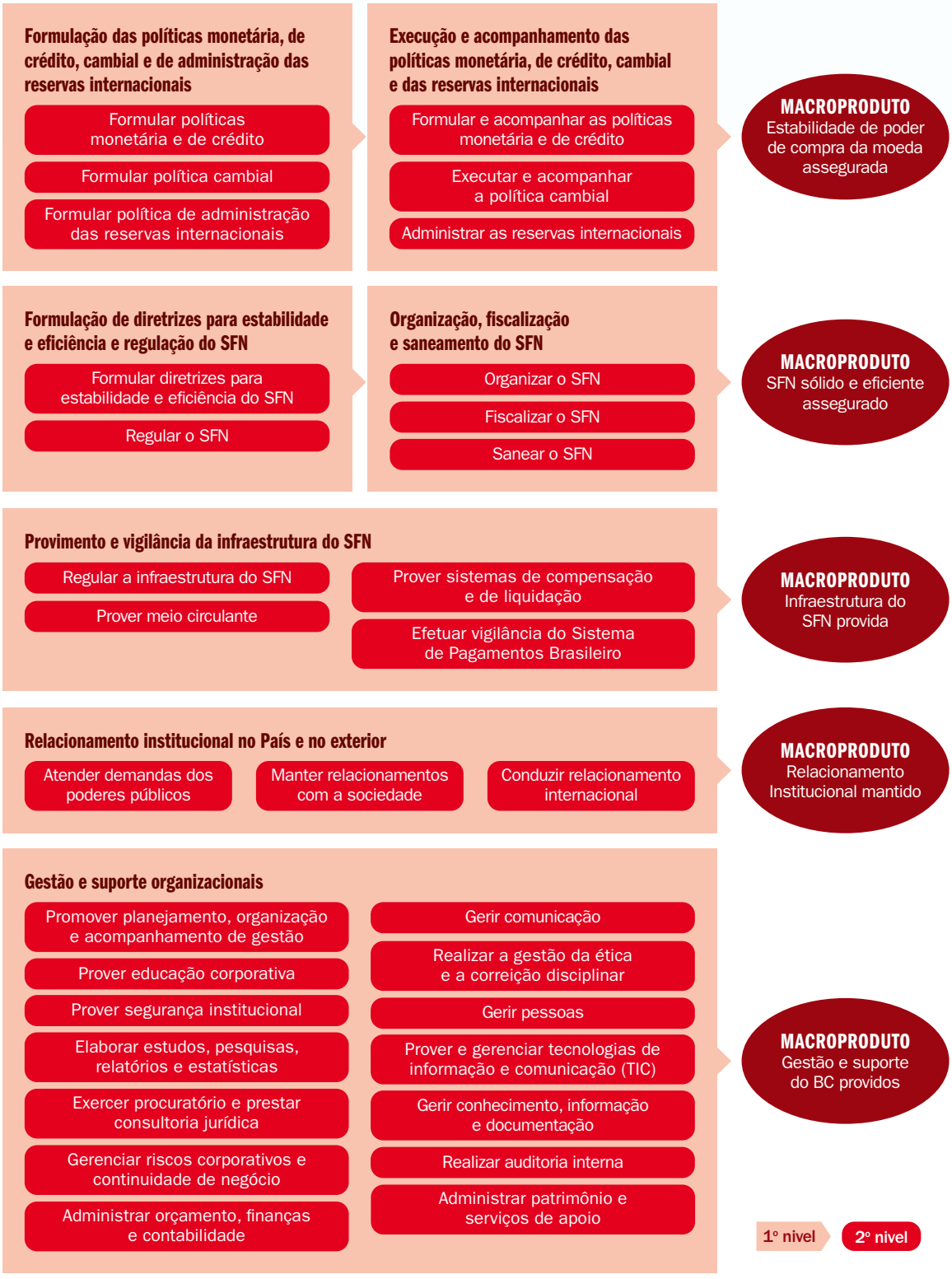
Um possível exemplo do uso conjunto dessas técnicas poderia ser a utilização de *brainstormings* ou entrevistas na fase de identificação de riscos, mais o uso de análise *Bow Tie* ou "E se" estruturado como ferramentas da fase de análise dos riscos e, finalmente, a matriz de probabilidade/consequência, utilizável tanto na fase de análise como na fase de avaliação dos riscos.

PRIORIZAÇÃO DE PROCESSOS

Ainda que a gestão de riscos deva ser parte integrante de todos os processos organizacionais (princípio previsto pela ISO 31000), ela não deve ser aplicada a todos os seus processos com a mesma intensidade, visto que os recursos da organização são limitados. Naturalmente o investimento na gestão de riscos deve ser maior nos processos que mais entregam ou devem entregar valor para as partes interessadas, bem como nas atividades de suporte que podem estar limitando a capacidade de entrega dos processos finalísticos.

Uma ferramenta útil à compreensão de como se organizam os processos de uma organização é a cadeia de valor. Na cadeia de valor, os macroprocessos finalísticos e de suporte, bem como os processos que compõem cada macroprocesso são representados grafica-

mente. Esse tipo de diagrama não indica a estrutura organizacional utilizada para fazer os processos funcionarem. Sua função é facilitar a visualização, de forma sistemática, de como a organização estabeleceu processos e de como eles interagem para criar valor. A título de exemplo, veja-se a cadeia de valor do Banco Central.



■ **Figura 8:** Cadeia de valor do Banco Central do Brasil com macroprocessos de primeiro e segundo níveis

Quando se define o escopo da gestão de riscos em uma organização, é necessário apontar quais processos organizacionais serão submetidos a um arranjo de gestão de riscos mais rigoroso. A priorização de processos organizacionais é importante para orientar a alocação de recursos para a gestão de riscos, bem como quando se planeja uma estratégia gradual de implantação dessa abordagem.

A priorização de processos pode ser mais acurada quando a organização estabeleceu, de forma satisfatória, seus contextos interno e externo. No estabelecimento do contexto externo, importa especialmente descrever as relações da organização com as partes interessadas externas e as percepções destas acerca do valor criado. No estabelecimento do contexto interno, deve-se descrever os objetivos, as estratégias, o escopo e os parâmetros das atividades da organização ou daquelas partes da organização em que o processo de gestão de riscos pode ser aplicado (ABNT, 2009).

Diversos fatores podem ser considerados na priorização de processos representados na cadeia de valor, tais como:

a) relevância estratégica do processo. Inclui definir quais áreas, funções ou atividades são relevantes para a realização dos seus objetivos-chave da organização, às vezes denominados macroprodutos, macro-objetivos ou resultados finalísticos. Para estimar este fator, pode-se valer de entrevistas com pessoas de segmentos representativos das partes interessadas, responsáveis pela governança e administradores da organização, bem como de análises internas para verificar o grau de importância de cada processo para o sucesso da estratégia.

b) materialidade, que indica a representatividade dos recursos financeiros alocados ao processo; e

c) maturidade do processo, que indica a consistência das práticas de gestão de processos empregadas e o atendimento dos produtos e serviços a padrões de entrega estabelecidos. Como fontes de informação para estimar este fator, estão os relatórios de desempenho dos processos; gerentes e servidores responsáveis pelo processo; pesquisas de satisfação com clientes internos e externos do processo; reclamações recebidas pela Ouvidoria; e trabalhos da auditoria interna da organização, da CGU (no âmbito do Poder Executivo) e do TCU.

A análise quantitativa facilita a priorização. Por isso, cada fator deve ser medido por meio de escalas apropriadas, desenvolvidas ou adaptadas segundo as especificidades de cada organização. O quadro sugere escalas para os fatores mencionados acima.

A priorização de processos deve envolver pessoas com visão sistêmica da organização e ser baseada nas melhores informações disponíveis. O ordenamento dos processos deve ser feito com base em um índice numérico, a exemplo deste:

P = RE * Mat/M

Onde: P é a prioridade do processo;
RE é a relevância estratégica do processo;
Mat é a materialidade do processo;
M é a maturidade do processo.

■ **Figura 9:** Exemplo de escalas para medição das variáveis consideradas para a priorização de processos.

FATORES	PONTOS DE ESCALA			
	1	2	3	4
RELEVÂNCIA ESTRATÉGICA DO PROCESSO	O processo tem pouca relevância para a realização dos objetivos-chave da organização (macroprodutos, macro-objetivos ou resultados finalísticos).	O processo tem média relevância para a realização dos objetivos-chave da organização.	O processo tem alta relevância para a realização dos objetivos-chave da organização.	O processo tem relevância muito alta para a realização dos objetivos-chave da organização.
MATERIALIDADE	Menos de 2,0% do orçamento anual.	De 2,0% a 10,0% do orçamento anual.	De 10,0% a 20,0% do orçamento anual.	Mais de 20,0 % do orçamento anual.
MATURIDADE DO PROCESSO	O processo não foi modelado ou sua modelagem não é utilizada para seu gerenciamento. Os resultados acontecem graças a iniciativas individuais. Padrões de entrega de produtos e serviços não existem ou são ignorados. Prática de "apagar incêndios".	O processo foi modelado e sua modelagem é de conhecimento dos servidores que executam o processo. Produtos e serviços costumam atender aos padrões de entrega, mas falhas significativas ainda acontecem.	A gestão do processo é feita com base em modelagem e em indicadores avaliados periodicamente. Métodos e tecnologias de gestão concentrados no nível gerencial. Produtos e serviços atendem aos padrões de entrega na grande maioria das vezes.	A gestão do processo é feita com base em modelagem e com medição de desempenho plenamente incorporada. Métodos e tecnologias de gestão amplamente utilizados pelos servidores da área. Muito raro algum produto ou serviço não atender aos padrões de entrega.

Métodos de priorização de processos podem variar quanto aos fatores de seleção e a forma de cálculo da prioridade de cada processo. Para conhecer outros métodos, pode-se consultar os desenvolvidos pelo Ministério do Planejamento, Desenvolvimento e Gestão (BRASIL, 2017) e pelo Tribunal Regional Eleitoral do Pará (BRASIL, 2018).

BRAINSTORMING

Esta técnica consiste em reunir pessoas conhecedoras de certo ativo ou atividade organizacional e incentivar o fluxo livre de conversação entre elas com o objetivo de identificar possíveis perigos, riscos ou controles associados ao objeto analisado.

A eficácia desta técnica depende muito do papel do facilitador, o qual deve estar apto a oferecer estímulos, provocar a participação das pessoas, incentivar o pensamento criativo, entre outras habilidades.

Esta técnica é particularmente útil para identificar riscos de novas atividades, novas tecnologias ou em situações em que não há dados disponíveis. O produto a ser gerado depende do contexto, podendo ser, por exemplo, uma lista de riscos e de controles.

ENTREVISTAS

Esta técnica baseia-se na formulação prévia de um conjunto de perguntas que servem de guia para o entrevistador e são oportunamente apresentadas às pessoas entrevistadas.

Nas entrevistas estruturadas as perguntas são totalmente pré-definidas, a fim de se garantir que todos os entrevistados abordem as mesmas questões. Entrevistas semi-estruturadas permitem maior liberdade, com exploração de questões que podem surgir ao longo da conversação.

A técnica de entrevistas é apropriada nos casos em que é difícil ou dispendioso reunir as pessoas para análises em grupo ou quando se deseja ouvir as opiniões pessoais, sem interferências ou influências de outros participantes de um grupo.

O produto gerado é a visão dos entrevistados sobre as questões propostas, as quais buscam normalmente identificar eventos de risco, fontes, consequências e controles.

DELPHI

Esta técnica tem por objetivo encontrar consenso entre opiniões de um grupo de especialistas sobre determinado assunto. Na gestão de riscos, é aplicável em qualquer etapa do processo, em especial na identificação, análise e avaliação.

A técnica é aplicada por meio de questionário, geralmente semi-estruturado, que é respondido individual e anonimamente por cada especialista. As respostas são consolidadas e, de forma agregada, levadas ao conhecimento dos especialistas em nova rodada do questionário. Assim, em rodadas sucessivas, permite-se a mudança

de opinião dos respondentes, até que se alcance o consenso.

O produto gerado depende da etapa em que a técnica é aplicada, podendo ser, por exemplo: lista de riscos identificados, níveis de riscos mensurados, opções para tratamento dos riscos acordadas, entre outras possibilidades.

ANÁLISE PRELIMINAR DE PERIGOS (APP)

É um método simples para identificar situações que possam representar perigos para ativos organizacionais ou causar impactos em atividades. É especialmente útil quando há poucas informações disponíveis sobre o ativo, projeto ou atividade objeto da análise.

Na aplicação dessa técnica, as pessoas que detenham informações sobre o objeto da análise são reunidas em grupo. Os participantes consideram as informações existentes, tais como atividades, recursos, ambiente, interfaces entre os diversos elementos e os objetivos a alcançar e produzem, de comum acordo, uma lista de situações perigosas ou de riscos.

O produto gerado é a lista de perigos ou riscos, bem como recomendações quanto à aceitação da situação ou sobre ações de tratamento para implementar ou aprimorar controles e, eventualmente, requisições para avaliações mais detalhadas.

LISTAS DE VERIFICAÇÃO

Trata-se do uso de listas pré-existentes de perigos ou riscos, como instrumento de apoio a outras técnicas de avaliação de riscos. A origem de tais listas normalmente são: experiência, boas práticas, análises tipo APP anteriormente realizadas e registros de incidentes.

O uso desta técnica ocorre da seguinte forma: percorre-se a lista e faz-se um batimento entre o que ela contém – eventos, fontes de risco, controles etc. – e a situação ou objeto que está sendo avaliado. Como resultado, pode-se gerar listas de situações ou riscos inaceitáveis, de controles inadequados ou faltantes, entre outros produtos.

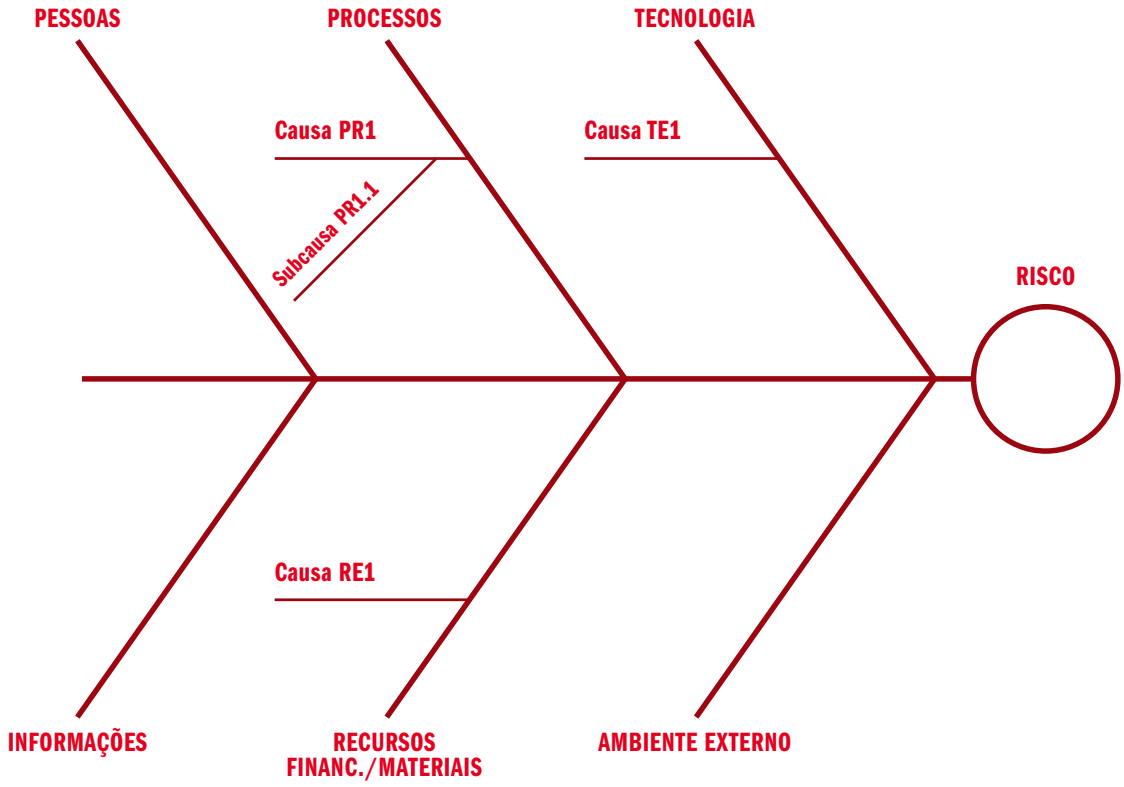
ANÁLISE DE CAUSA RAIZ

Esta análise tenta identificar a raiz ou causas originais ao invés de lidar somente com os sintomas imediatos e óbvios. A avaliação das causas geralmente progride de causas mais evidentes para causas subjacentes, considerando diferentes categorias de fatores, tais como humanos, tecnológicos, materiais, ambientais etc.

A técnica de análise de causa raiz pode ser utilizada desde a etapa de análise dos riscos, na qual contribui para a estimativa da probabilidade, até a etapa de tratamento dos riscos, na qual permite direcionar ações para as causas principais. Ressalte-se que, mais do que buscar

identificar grande quantidade de causas, é mais eficaz identificar e tratar o menor conjunto de causas que mais contribua para a materialização do risco (aplicação da regra 20-80, de Pareto).

As seguintes técnicas, entre outras, podem ser utilizadas para análise de causa raiz: "5 Porquês", árvore de falhas, diagrama de espinha de peixe (Ishikawa), análise de Pareto, etc.



■ **Figura 9:** Exemplo de diagrama de Ishikawa para análise de causa raiz de risco.

TÉCNICA "E SE" ESTRUTURADA (SWIFT)

É o exame sistemático, realizado em equipe, para identificação de riscos de desvios em um processo, sistema ou atividade.

O procedimento é realizado em grupo, pelas pessoas que trabalham rotineiramente com o objeto analisado ou que detenham informações sobre ele. Exige a atuação de um facilitador, que deve provocar a participação das pessoas a

partir de perguntas previamente elaboradas do tipo "e se", "o que aconteceria se", "alguém ou algo pode ...?", "alguém ou algo nunca...?". Essas questões devem estimular a reflexão dos participantes sobre diferentes alternativas e cenários de funcionamento do objeto analisado. Isso também envolve a identificação de controles e de sua eficácia, em diversas situações.

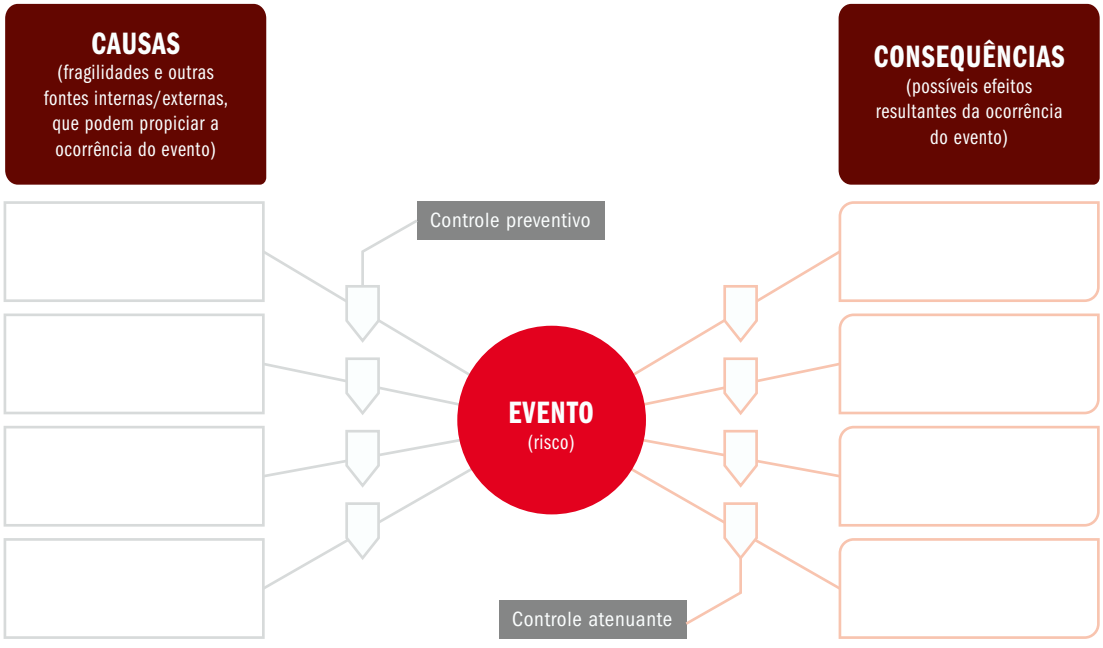
Ações necessárias para o tratamento dos riscos são propostas e, em muitos casos, elabora-se uma classificação qualitativa ou semiquantitativa dos riscos a fim de priorizá-las. Os resultados da aplicação da técnica geralmente são: listas de possíveis eventos, fontes de riscos, consequências e controles, bem como de ações de tratamento priorizadas.

A utilização dessa técnica facilita a criação de um registro de riscos e de plano de tratamento, que podem ser obtidos com pequeno esforço adicional.

ANÁLISE BOW TIE

Técnica que busca analisar e descrever os caminhos de um evento de risco, desde suas causas até as consequências, por meio de uma representação pictográfica semelhante a uma gravata borboleta (*bow tie*). O método tem como foco as barreiras entre as causas e o evento de risco e as barreiras entre o evento de risco e suas consequências.

a)



■ **Figura 10:** Esboço de diagrama "bow tie".

O processo de elaboração do esquema *bow tie* ocorre da seguinte forma:

b) Representa-se o evento de risco como sendo o nó de uma gravata borboleta.

c) As possíveis causas ou fontes do evento de risco são listadas no lado esquerdo do desenho e cada uma delas é conectada por uma linha ao nó da gravata.

d) Barreiras que impedem ou diminuem a possibilidade da causa ou fonte produzir o evento de risco são representadas como barras verticais cruzando essas linhas horizontais do lado esquerdo.

e) De forma análoga, no lado direito do desenho, identificam-se possíveis consequências e cada uma delas é ligada ao nó central por uma linha.

f) Barreiras que impedem ou diminuem o efeito das consequências são representadas como barras verticais cruzando essas linhas horizontais do lado direito. As barreiras do lado esquerdo do esquema representam controles preventivos, no caso de risco negativo ou controles de intensificação ou promoção, no caso de risco positivo/oportunidades. As barreiras do lado direito representam controles reativos visando à atenuação dos efeitos, caso o evento de risco negativo se materialize.

O produto resultante dessa análise é o próprio diagrama esquemático gerado, bem como as informações a ele associadas que foram identificadas: evento de risco, fontes, causas, controles preventivos ou intensificadores e controles reativos de atenuação.

ANÁLISE DE DECISÃO POR MULTICRITÉRIO (MCDA)

Essa técnica tem o objetivo geral de classificar um conjunto de opções por ordem de valor ou prioridade, a partir da percepção de um grupo de pessoas.

O procedimento envolve a identificação do conjunto de opções a serem avaliadas e a definição de fatores ou critérios avaliativos, geralmente estruturados hierarquicamente. Atribuem-se pesos aos fatores avaliativos a partir de notas dos avaliadores, por meio de algum método matemático que agrega todas as percepções. Em seguida, os participantes avaliam cada opção em relação aos fatores, sendo essas percepções novamente agregadas por algum método matemático, de modo a gerar uma nota única para cada opção, considerados os pesos dos fatores.

O produto gerado pela aplicação desta técnica são as opções classificadas na ordem das notas finais atribuídas a cada uma delas. Diferentes métodos podem ser usados para a ponderação dos fatores e para a agregação das notas das opções. O método *Analytic Hierarchy Process* (AHP) é comumente utilizado para esse tipo de análise. O modelo ma-

temático utilizado no AHP envolve cálculos matriciais e a valoração das opções é feita pela comparação par a par entre todas elas, relativamente a cada fator.

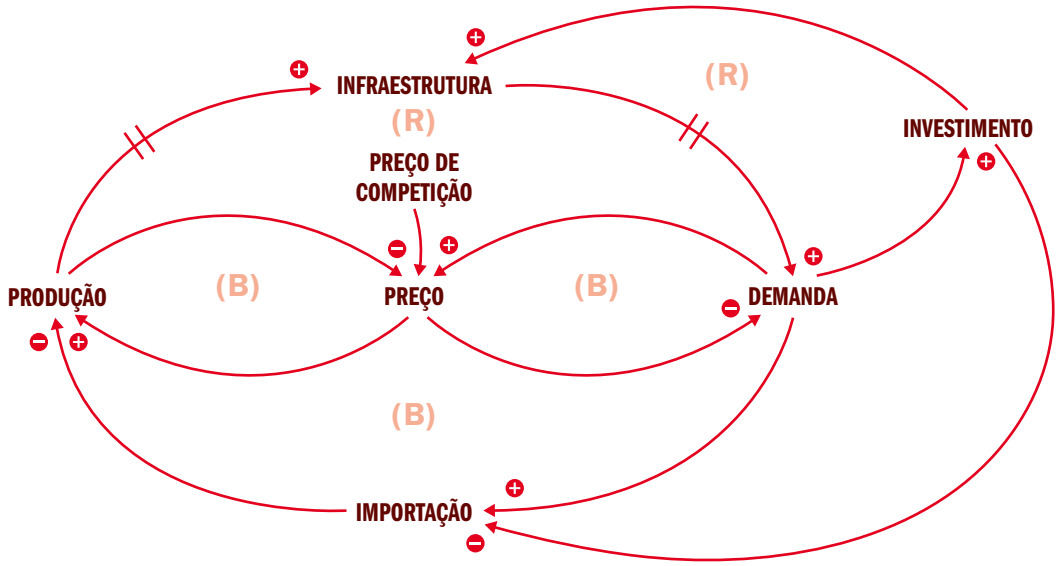
Um ponto forte da técnica Análise de Decisão por Multicritério é que ela abre a possibilidade de tomada de decisão mesmo quando as partes envolvidas possuem objetivos e critérios distintos. Na gestão de riscos, a técnica pode ser útil para classificar riscos ou priorizar ações de tratamento, entre outras aplicações.

PENSAMENTO SISTÊMICO

Pensamento sistêmico diz respeito a um conjunto de conceitos, comportamentos e ferramentas que auxiliam na compreensão de estruturas interdependentes de sistemas complexos. Essa forma de pensamento busca explicitar relações de causalidades entre um conjunto dinâmico de fatores que se interrelacionam.

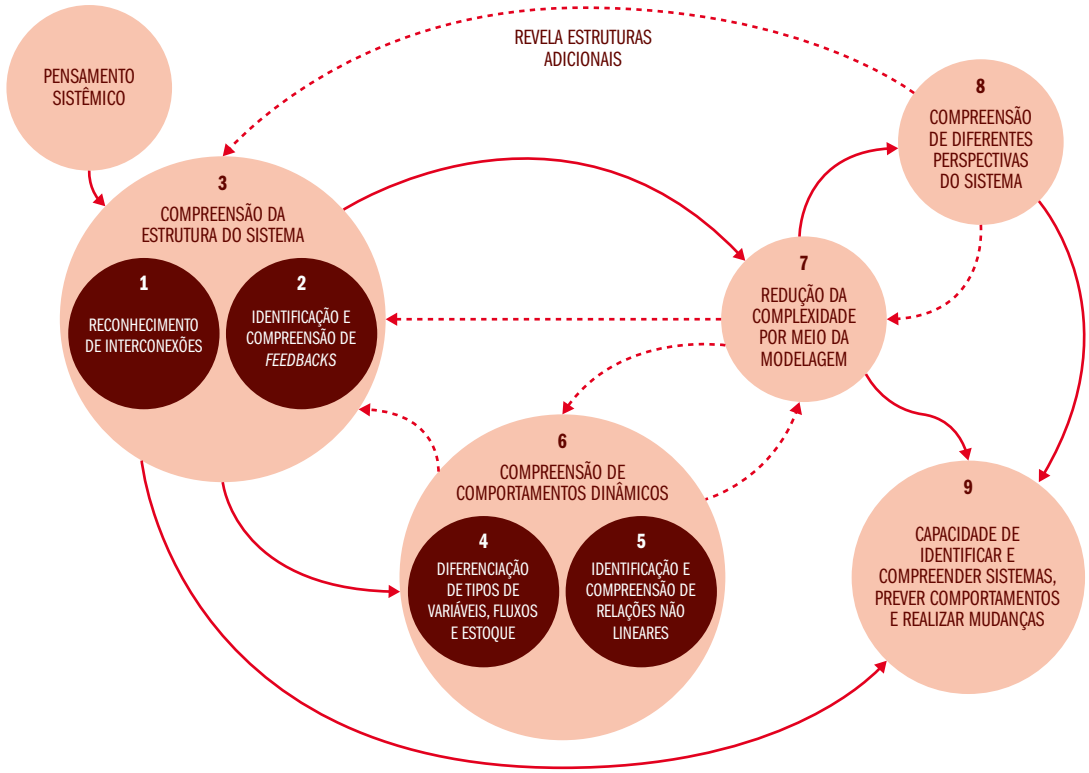
Trata-se de uma disciplina que permite analisar questões de forma holística e integrada, vislumbrar conjuntos dinâmicos de comportamento, identificar e compreender interconexões que conferem ao sistema características únicas, bem como vislumbrar comportamentos prováveis.

Entre as ferramentas utilizadas para apoiar o trabalho estão o diagrama de *loop* de causalidade (CLD), o gráfico de comportamento temporal (BOT), os simuladores de modelo e os simuladores de gestão.



■ **Figura 11:** Exemplo de diagrama de loop de causalidade (CLD).

Em geral, a análise se inicia com a identificação de uma questão/problema central. Em seguida é feita a identificação de fatores e variáveis que afetam essa questão. De forma recursiva, para cada um dos fatores/variáveis identificam-se novas relações de causalidade até que que se fechem os ciclos de balanceamento (B) e reforço (R) que mantém o sistema operando. A análise das interrelações e dos ciclos permite identificar prováveis comportamentos do sistema e contribui para o planejamento de intervenções com maior potencial de adequar o comportamento do sistema aos objetivos desejados. ■



■ **Figura 12:** *Systems Thinking Systemigram* (adaptado de *Research Gate*).

CAPÍTULO 5

LIDERANÇA PARA RISCO

CAPÍTULO 5
LIDERANÇA PARA RISCO

A **governança de riscos** compreende todas as atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. Não é uma atividade autônoma, separada das demais, mas sim parte de todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, atividades operacionais de rotina e processos de gestão em todos os níveis da organização (ABNT, 2009).

Semelhante é a definição de gestão de riscos adotada no modelo COSO II – Gerenciamento de Riscos Corporativos – Estrutura Integrada:

> A gestão de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de 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, 2007).

Desse modo, a governança e a gestão de riscos são partes integrantes e indissociáveis das responsabilidades administrativas, em especial dos gestores, e inclui atividades como (ABNT, 2009; IIA, 2009):

a) estabelecer um ambiente interno apropriado, incluindo a estrutura para gerenciar riscos;

b) estabelecer, articular e comunicar os objetivos, e determinar limites de exposição a riscos aceitáveis;

c) identificar potenciais ameaças e oportunidades ao cumprimento dos objetivos;

d) analisar e avaliar os riscos (i.e., determinar o impacto e a probabilidade e comparar o nível do risco com critérios pré-definidos);

e) selecionar e implantar respostas aos riscos, por meio de controles internos e outras ações de tratamento;

f) comunicar as informações sobre os riscos de forma consistente em todos os níveis;

g) monitorar e coordenar os processos e os resultados da gestão de riscos; e

h) fornecer avaliação (*assurance*) quanto à eficácia com que os riscos são gerenciados.

PRINCÍPIOS, ESTRUTURA E PROCESSO DE GESTÃO DE RISCOS

Os **princípios da gestão** de riscos representam condições que precisam estar incorporadas à estrutura e ao processo para que a gestão de riscos seja eficaz e se torne parte da cultura da organização, traduzindo-se em um conjunto compartilhado de atitudes, valores e comportamentos que caracterizam como a organização aborda o risco.

A **estrutura de gestão de riscos** é a maneira como a entidade se organiza para gerenciar os riscos do seu negócio, representando o conjunto de componentes e arranjos organizacionais para a concepção, a implementação, o monitoramento, a análise crítica e a melhoria contínua da gestão de riscos através de toda a organização. Inclui a política de gestão de riscos, os manuais e guias, os recursos, a definição de objetivos e de papéis e responsabilidades que permitirão incorporar a gestão de riscos em todos os níveis da organização (ABNT, 2009).

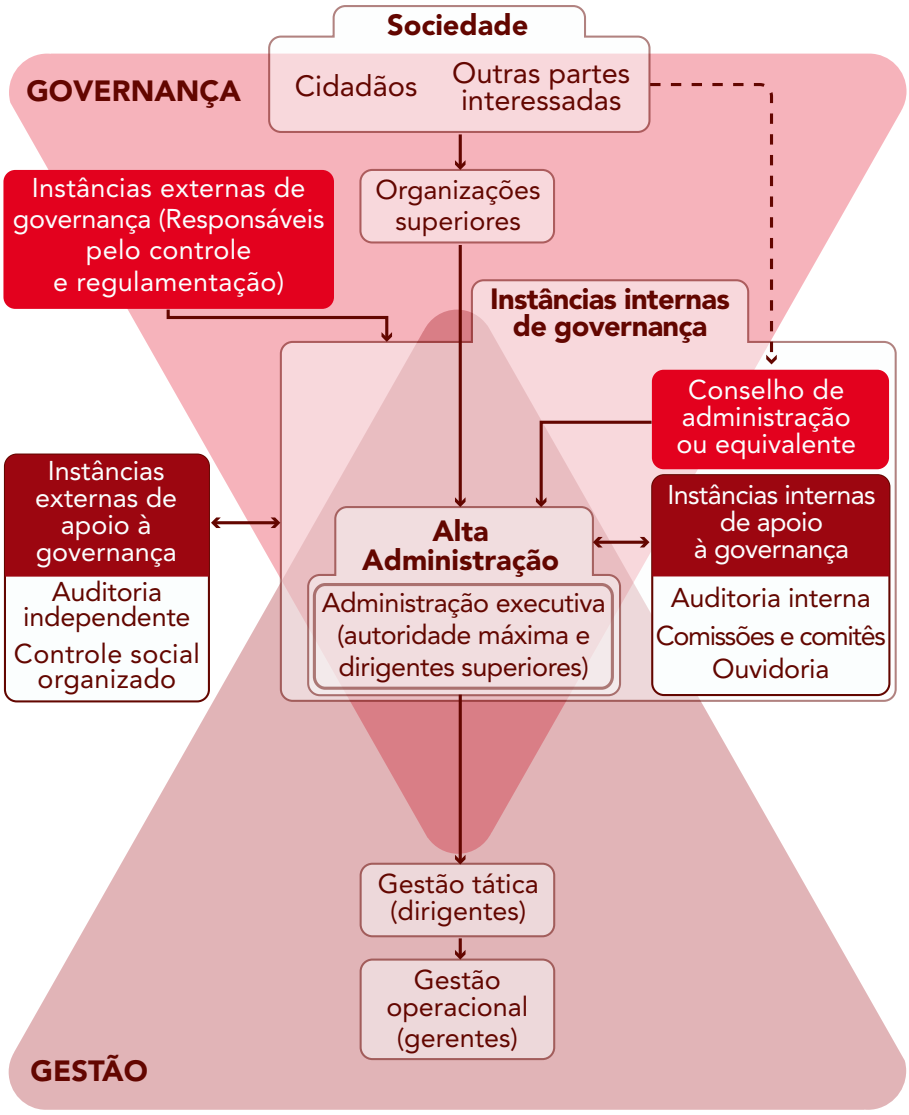
O **processo de gestão de riscos** representa o conjunto de atividades contínuas, realizado pelas pessoas em todos os níveis da entidade, desde a definição das estratégias até o nível das atividades operacionais, concebido para identificar riscos que possam afetar a capacidade da organização em atingir os seus objetivos e para apoiar tomadas de decisões e ações que forem necessárias para mantê-los em níveis compatíveis com os limites de exposição a riscos previamente estabelecidos, de maneira a fornecer segurança razoável do cumprimento dos objetivos.

PAPÉIS E RESPONSABILIDADES

Cada pessoa na organização tem uma parcela de responsabilidade na gestão de riscos (COSO, 2006) e todo o pessoal deve receber uma mensagem clara das instâncias de governança e da alta administração de que as responsabilidades de gestão de riscos devem ser levadas a sério (INTOSAI, 2007). Responsabilidades claras devem ser definidas para que cada grupo de profissionais entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos da organização (IIA, 2013).

A alta administração e as instâncias de governança da instituição têm, coletivamente, a responsabilidade e o dever de prestar contas sobre o estabelecimento dos objetivos da organização, a definição de estratégias para alcançar esses objetivos e o estabelecimento de estruturas e processos de governança

para melhor gerenciar os riscos durante a realização desses objetivos (IIA, 2013). Assim, a instância máxima de governança e a alta administração têm a responsabilidade de assegurar a existência, o monitoramento e a avaliação de um sistema efetivo de gestão de riscos e controle interno, bem como de utilizar as informações resultantes desse sistema para apoiar seus processos decisórios e gerenciar riscos estratégicos (TCU, 2014).



■ **Figura 13:** Sistema de governança de órgãos e entidades da administração pública (TCU, 2014).

Na prática, a instância máxima de governança decide e delega a implantação e operação da gestão de riscos aos executivos da gestão, assumindo um papel de supervisão desses processos. Além disso, usa os serviços de asseguração da auditoria interna para monitorar e avaliar a eficácia dos processos de gestão de riscos e controles por toda a organização.

A supervisão da gestão de riscos pela instância máxima de governança da instituição envolve: (a) saber até que ponto a administração estabeleceu uma gestão de riscos eficaz; (b) estar ciente e de acordo com os limites de exposição a riscos aceitáveis pela organização; (c) revisar o portfólio de riscos assumidos em contraste com os limites de exposição a riscos definidos; e (d) ser notificado em relação aos riscos mais significativos e saber se a administração está respondendo a eles adequadamente (COSO, 2006).

Os gestores são diretamente responsáveis pela concepção, estruturação e implementação da gestão de riscos no âmbito da sua área de atuação. Em qualquer organização, o presidente ou dirigente máximo é o depositário final da responsabilidade pela gestão de riscos, cabendo-lhe assumir a iniciativa. Aos demais gestores cabe apoiar a cultura de gestão de riscos e gerenciar os riscos, dentro de suas esferas de responsabilidade, conforme os limites de exposição a riscos aceitáveis pela organização (COSO, 2006).

Os gestores do nível operacional têm a propriedade dos riscos e a responsabilidade primária pela identificação e pelo gerenciamento dos riscos em suas respectivas áreas, conduzindo procedimentos de riscos e controles diariamente e mantendo controles internos eficazes sobre as operações (COSO, 2006).

O pessoal da linha de frente, que lida diariamente com questões operacionais críticas, está em melhores condições para reconhecer e comunicar riscos, portanto essa responsabilidade é geralmente atribuída a todos os servidores e colaboradores, cujo cumprimento exige canais de comunicação para cima e clara disposição para ouvir da alta administração (INTOSAI, 2007).

Em organizações grandes, dependendo de fatores como ambiente e setores nos quais operam, complexidade das operações, natureza das atividades e grau de regulamentação, pode haver uma função ou unidade organizacional separada para coordenar as atividades de gestão de riscos por toda a organização e fornecer habilidades e conhecimentos especializados. Essa função é mais bem-sucedida quando claramente estabelecida como função de suporte, apoiando e facilitando os gestores a estabelecer, nas áreas sob sua responsabilidade, atividades de gestão de riscos que sejam eficazes e alinhadas às diretrizes institucionais. São responsabilidades dessa unidade ou função, por exemplo:

a) fornecer métodos, técnicas, e ferramentas para unidades de negócios com a finalidade de identificar, avaliar, tratar e monitorar riscos;

b) definir funções e responsabilidades pela gestão de riscos nas unidades de negócio;

c) promover competência em gestão de riscos pela organização;

d) orientar a integração da gestão de riscos com outras atividades de gestão;

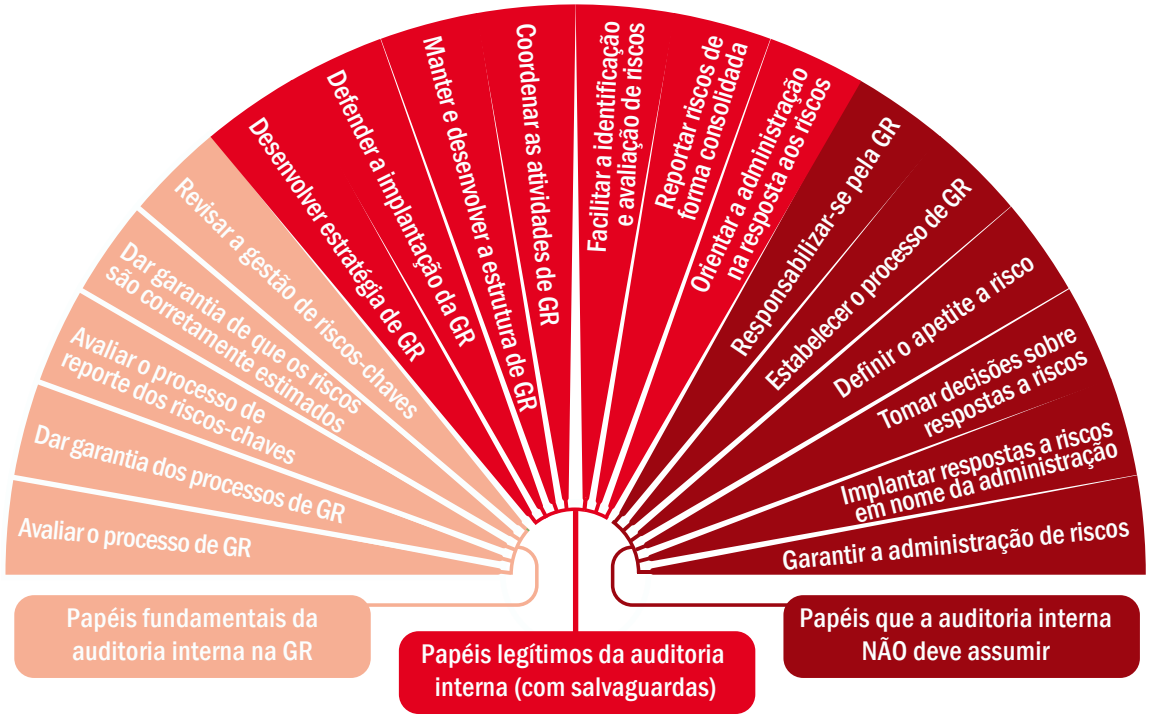
e) estabelecer uma linguagem comum de gestão de riscos, que inclua medidas comuns de probabilidade, impacto e categorias de riscos;

f) comunicar ao presidente e à diretoria executiva o andamento da gestão de riscos (COSO, 2006; IIA, 2009).

Além disso, pode haver uma função ou unidade organizacional de *compliance* que monitore riscos específicos de não conformidade com leis e regulamentos, reportando-se diretamente às instâncias de governança ou à alta administração e aos órgãos reguladores; ou ainda múltiplas funções de *compliance* com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, licitações e contratos, meio-ambiente e controle de qualidade, além de uma função de controladoria que monitore os riscos financeiros e questões de reporte financeiro (IIA, 2013).

Em organizações pequenas, com operações e regulamentação de baixa complexidade, a responsabilidade pela coordenação das atividades de gestão de riscos pode ser atribuída a uma área que cuide do planejamento ou controladoria, ou ainda a uma assessoria do dirigente máximo.

A auditoria interna deve auxiliar a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gestão de riscos, controle e governança (IIA, 2009a). A Figura seguinte indica quais são os papéis fundamentais que auditoria interna deve assumir; os que pode assumir com salvaguardas; e os que não deve assumir, porque comprometeriam a sua independência e a objetividade de seus auditores para fornecer asseguração sobre a eficácia dos processos de gestão de riscos e controle interno da organização.



■ **Figura 14:** O papel da auditoria interna na gestão de riscos (adaptado de IIA, 2009a).

O papel fundamental da auditoria interna na gestão de riscos é fornecer asseguração aos órgãos de governança e à alta administração de que os processos de gestão de riscos operam de maneira eficaz e os maiores riscos do negócio são gerenciados adequadamente em todos os níveis da organização. Para tanto, a auditoria interna deve desenvolver compreensão clara da estratégia da organização e de como ela

é executada, quais os riscos associados e como esses riscos são gerenciados. As atividades indicadas à esquerda da Figura 3 representam esse papel (IIA, 2009).

A estratégia da organização deve ser um elemento fundamental no desenvolvimento dos planos anuais de auditoria baseados em risco, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e a garantir que os seus recursos são alocados em áreas de maior risco (IIA 2120-3). Além disso, a fim de habilitar a auditoria interna a ajudar a identificar os riscos mais significativos para o alcance dos objetivos da organização, os seus trabalhos devem utilizar uma abordagem de auditoria baseada em risco, permitindo que planos de ação para o tratamento dos riscos identificados sejam efetivamente formulados e monitorados.

Quando uma organização não dispõe de um processo formal de gestão de riscos, a auditoria interna deve levar o fato à atenção das instâncias de governança e à alta administração, recomendando o estabelecimento de tal processo, podendo assumir um envolvimento direto nos primeiros estágios de sua implementação, mediante trabalhos de consultoria. Entretanto, se a auditoria interna ainda não tiver adotado uma abordagem baseada em risco, representada pelas atividades de asseguração descritas à esquerda da Figura 12, é improvável que esteja apta a desempenhar as atividades de consultoria descritas no centro dessa figura (IIA, 2009).

À medida que a maturidade da gestão de riscos da organização evolui e a gestão de riscos torna-se mais inserida nas operações do negócio, o papel da auditoria interna em promover a gestão de riscos vai se reduzindo, voltando a se concentrar em seu papel de asseguração (IIA, 2009).

TRÊS LINHAS DE DEFESA

Mesmo em entidades onde não há uma estrutura ou sistema formal de gestão de riscos, como no caso de organizações pequenas, pode ser possível aumentar a compreensão e a eficácia da abordagem da organização quanto a riscos por meio da delegação e da coordenação das responsabilidades essenciais de gestão de riscos baseando-se na abordagem das Três Linhas de Defesa (IIA, 2013).

A abordagem das Três Linhas de Defesa, embora não seja um modelo de gestão de riscos, é uma forma simples e eficaz para melhorar a comunicação e a conscientização sobre os papéis e as responsabilidades essenciais de gestão de riscos e controles, aplicável a qualquer organização – não importando o seu tamanho ou a sua complexidade – ainda que não exista uma estrutura ou sistema formal de gestão de riscos.

Por essa abordagem, há três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos, como explanado a seguir:

1º) **Funções que gerenciam e têm propriedade de riscos:** a gestão operacional e os procedimentos rotineiros de riscos e controles internos constituem a primeira linha de defesa na gestão de riscos. A gestão operacional serve naturalmente como a primeira linha de defesa porque os controles internos são desenvolvidos como sistemas e processos sob sua orientação e responsabilidade. Nesse nível se identificam, avaliam e mitigam riscos por meio do desenvolvimento e da implementação de políticas e procedimentos internos que possam oferecer garantia razoável de que as atividades estejam de acordo com as metas e objetivos.

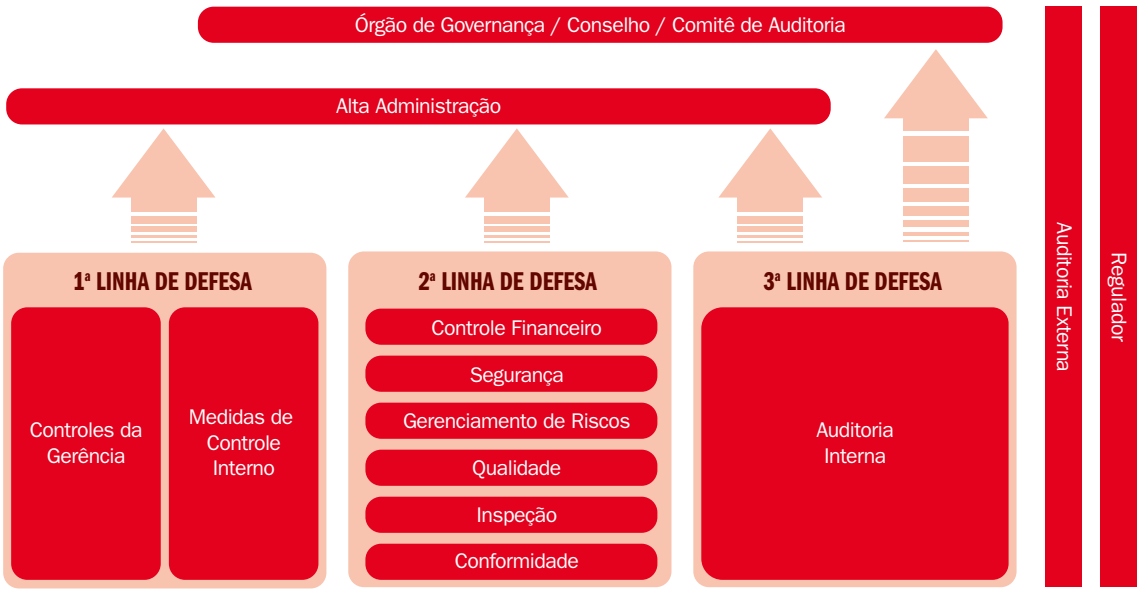
2º) **Funções que supervisionam riscos:** a segunda linha de defesa é constituída por funções – unidades, comitês ou outras estruturas organizacionais – estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão de riscos e controles. As funções específicas variam muito entre organizações e setores, mas são, por natureza, funções de gestão. Seu papel é coordenar as atividades de gestão de riscos, orientar e monitorar a implementação das práticas de gestão de riscos por parte da gestão operacional, apoiar a definição de metas de exposição a risco, monitorar riscos específicos (de *compliance*, por exemplo), bem como ajudar a definir controles e/ou monitorar riscos e controles da primeira linha de defesa.

3º) **Funções que fornecem avaliações independentes:** a auditoria interna constitui a terceira linha de defesa na gestão de riscos ao fornecer avaliações (assegurações) independentes e objetivas sobre os processos de gestão de riscos, controles internos e governança aos órgãos de governança e à alta administração. Tais avaliações devem abranger uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e integridade dos processos de reporte; conformidade com leis e regulamentos) e elementos da estrutura de gestão de riscos e controle interno em todos os níveis da estrutura organizacional da entidade.

Embora a instância máxima de governança e a alta administração não sejam consideradas entre as três linhas de defesa desse modelo, nenhuma consideração sobre gestão de riscos estaria completa sem levar em conta, em primeiro lugar, os papéis essenciais dessas que são as principais partes interessadas e as que estão em melhor posição para instituir e assegurar o bom funcionamento das três linhas de defesa no

processo de gestão de riscos e controles da organização (IIA, 2013). Ressalte-se que, de acordo com as práticas L3.4, C1.1 e C1.2 do "Referencial Básico de Governança" (Brasil, 2014), a alta administração é a responsável maior pela gestão de riscos e a ela cabe: estabelecer, avaliar, direcionar e monitorar o sistema de gestão de riscos e controle interno, bem como assegurar que os gestores implementem práticas de gestão de riscos e controle interno no âmbito da instituição.

Órgãos de controle externo, reguladores, auditores externos e outras instâncias externas de governança estão fora da estrutura da organização, mas podem desempenhar um papel importante em sua estrutura geral de governança e controle, podendo ser considerados linhas adicionais de defesa, que fornecem avaliações tanto às partes interessadas externas da organização, como às instâncias internas de governança e à alta administração da entidade (IIA, 2013). ■



■ **Figura 15:** Modelo de Três Linhas de Defesa (adaptado de IIA, 2013).

CAPÍTULO 6

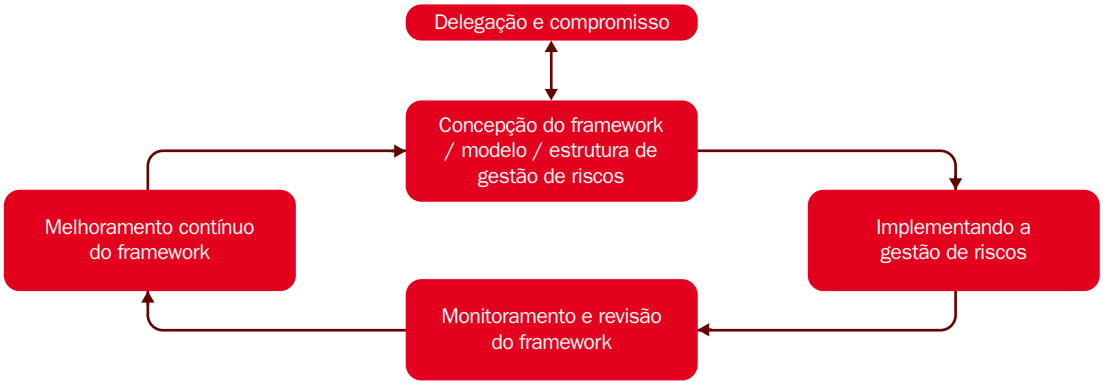
BOAS PRÁTICAS DE GESTÃO DE RISCOS

CAPÍTULO 6
BOAS PRÁTICAS DE GESTÃO DE RISCOS

O **risco** pode ser definido como uma medida de incerteza e compreende os fatores que podem facilitar ou impedir o alcance dos objetivos organizacionais.

De acordo com o *The International Federation Of Accoutants* – IFAC, **a gestão de riscos** pode ser vista como um processo de compreensão dos objetivos organizacionais; identificação dos riscos associados à realização dos objetivos; avaliação dos riscos, incluindo a probabilidade e impacto potencial de riscos específicos; desenvolvimento e implementação de programas/procedimentos para lidar com os riscos identificados; e monitoramento e avaliação de riscos, bem como de programas/procedimentos estabelecidos para lidar com os riscos.

De acordo com a ISO 31000:2009, uma **estratégia de implantação da gestão de riscos** envolve aspectos como: a delegação e o compromisso; a concepção de *framework*; a implementação da gestão de risco; o monitoramento e revisão do *framework*; e a melhoria contínua do *framework*.



■ **Figura 16:** Relacionamento entre os componentes da estrutura para gerenciar riscos, adaptado de ISO 31000:2009

Estabelecer uma **estrutura de gestão de riscos**, bem como monitorá-la e avaliá-la, são boas práticas que contribuem para a eficácia e melhoria do desempenho organizacional.

Para que esse fim seja alcançado, recomenda-se: definir papéis e responsabilidades relacionados à gestão de riscos; definir estratégia e diretrizes para gestão de riscos; definir critérios de classificação de risco e grau de tolerância a risco;definir e implantar política de gestão de riscos; definir e implantar processo de gestão de riscos; identificar, avaliar, analisar, tratar e monitorar riscos críticos; dentificar e implantar controles internos para tratar riscos críticos; definir e implantar plano de continuidade; monitorar e avaliar a estrutura de gestão de riscos; bem como, aprimorar continuamente a estrutura de gestão de riscos.

POR ONDE COMEÇAR?

Muitas organizações que se propõem a **implantar a gestão de risco** questionam-se acerca de **por onde** devem **começar**. Conversando com instituições que já deram o primeiro passo nessa direção, identificamos que, em sua maioria, elas seguiram passos semelhantes:

a) montaram um grupo de trabalho;

b) realizaram estudos preliminares;

c) definiram a estratégia de implantação e a arquitetura de gestão de riscos;

d) definiram a política de gestão de riscos;

e) definiram a responsabilidade das partes interessadas;

f) definiram o processo de gestão de riscos;

g) implementaram a gestão de riscos, por meio da implantação em unidades, processos e projetos piloto e, posteriormente, adaptação e disseminação para outros objetos e contextos;

h) monitoram e revisam.

Embora essa não seja a única forma, e não podemos garantir que seja a melhor, tem sido frequentemente adotada no setor público brasileiro. A seguir apresentaremos algumas práticas encontradas que podem ser facilmente replicadas.

Grupo de trabalho

A primeira prática comumente adotada para implantação da gestão de riscos no âmbito de uma organização consiste na formação de um grupo de trabalho. Idealmente, esse grupo deve ser composto por pessoas que conheçam e/ou tenham interesse em aplicar, os principais modelos, processos, técnicas e ferramentas de gestão de risco; devem possuir habilidades técnicas e gerencias suficientes para serem capazes de definir a

estratégia, propor mudanças em processos e normativos, planejar e coordenar o processo de implantação; devem ainda ter atitudes que contribuam para o resultado como, por exemplo, interesse no tema, automotivação e persistência para continuar mesmo em face a resistências comumente encontradas.

Estudos preliminares

Feito isso, o próximo passo consiste em realizar estudos preliminares que visam aprofundar o conhecimento acerca do tema "gestão de riscos" e, mais importante, acerca do ambiente interno e externo no qual a organização está inserida. Aqui o que se busca é identificar que processo, unidades e projetos são críticos para a organização e se beneficiariam mais da adoção imediata de práticas de gestão de risco. Entre as ferramentas e técnicas que podem apoiar essa atividade estão: revisão de literatura, análise documental, visitas técnicas, entrevistas, análise SWOT, análise de cenários, BIA (*business impact analysis*), análise de custo-benefício e análise de viabilidade.

Estratégia de implantação e definição de arquitetura

Conhecido o ambiente, o próximo passo consiste em definir a estratégia de implantação. A estratégia deve apontar, pelo menos: quais objetivos a organização quer alcançar com a gestão de riscos; quem são os responsáveis pela coordenação da implantação da gestão de riscos; que estruturas (processos, ferramentas, normas e pessoas) são necessários; quais objetos, estruturas, processos e projetos são críticos e se beneficiariam da adoção dessas práticas; e qual a melhor ordem e momento para implantação.

De acordo com o IBGC (2007), para implantar um modelo de Gestão de Riscos Corporativos (GRCorp) e promover uma cultura de gerenciamento de riscos na organização deve-se elaborar uma arquitetura para facilitar e viabilizar o gerenciamento do risco propriamente dito, cuja concepção e implementação trazem inúmeros benefícios para a organização, tais como: (a) aderência dos processos internos ao perfil de riscos estabelecido pelo conselho de administração; (b) clareza quanto às regras de governança para gerir a exposição a risco; (c) endereçamento de lacunas de capacitação de pessoas, processos e sistemas; e (d) implementação de sistemas de controles eficazes.

Ainda conforme o IBGC, a arquitetura para o GRCorp deve girar em torno e se condicionar aos objetivos estratégicos e metas da organização. Para tanto é importante que esses estejam definidos e sejam gerenciados; norteiem as prioridades da organização no que se refere a riscos e controles internos. Não por menos, o IBGC sugere que um conjunto de perguntas, descritas no quadro abaixo, sejam feitas para cada um dos objetivos da organização, de sorte a orientar a definição da arquitetura de GRCorp a ser adotada.

■ **Quadro 10:** Insumos para formulação de arquitetura para o GRCorp, adaptado de IBGC (2007).

DIMENSÕES	QUESTÕES DE REFERÊNCIA
PROCESSOS CRÍTICOS (PARA O GRCORP)	a) Quais são os macroprocessos identificados como relevantes na fase de levantamento dos riscos? b) Quais são os princípios que irão nortear eventual redesenho dos processos? c) Qual é o mecanismo para se descontinuar e/ou criar processos novos a partir da implantação do modelo de GRCorp? d) Quais são as ações críticas para mitigar os riscos relevantes?
GOVERNANÇA DE GERENCIAMENTO DE RISCOS	a) Quais são os fóruns de decisão envolvidos? b) Quais são os papéis e responsabilidades desses fóruns? c) Qual é a composição desses fóruns? d) Quais são as alçadas? e) Quais são as políticas necessárias para tomada de decisão ágil e eficaz?
ORGANIZAÇÃO E PESSOAS	a) Existem as capacitações necessárias? Quais são as lacunas? Como endereçá-las? b) O modelo organizacional facilita a identificação, monitoramento e mitigação dos riscos relevantes? c) Como está sendo tratada a questão da sucessão de postos/pessoas-chave na organização?
SISTEMAS DE CONTROLE	a) Existem controles adequados para mensurar a exposição? b) Os relatórios gerenciais facilitam a identificação, monitoramento e mitigação dos riscos? c) Os sistemas de TI (Tecnologia da Informação) são adequados?
COMUNICAÇÃO	a) Há comunicação adequada com os colaboradores? b) Existe uniformidade conceitual quanto ao modelo de GRCorp? c) O perfil de riscos e seus benefícios estão devidamente comunicados para a organização? d) Há um claro alinhamento entre o perfil de riscos e os valores e cultura corporativa? e) As responsabilidades e direitos decisórios estão devidamente explicitados e comunicados? f) Há comunicação adequada com os *stakeholders* externos?

Política de gestão de riscos

Respondidas aquelas perguntas e tomadas as decisões, passa-se à definição da política de gestão de riscos[4]. De acordo com a ISO 31000:2009, esse documento deve explicitar: (a) os objetivos e o comprometimento da organização em relação à gestão

4 O TCU dispõe de Política de Gestão de Riscos, que consta da Resolução nº 287/2017 e do Anexo II dessa publicação.

de riscos; (b) a justificativa da organização para gerenciar riscos; (c) as ligações entre os objetivos e políticas da organização com a política de gestão de riscos; (d) as responsabilidades para gerenciar riscos; (e) a forma com que são tratados conflitos de interesses; (f) o comprometimento de tornar disponíveis os recursos necessários para auxiliar os responsáveis pelo gerenciamento dos riscos; (g) a forma com que o desempenho da gestão de riscos será medido e reportado; e (h) o comprometimento de analisar criticamente e melhorar periodicamente a política e a estrutura da gestão de riscos em resposta a um evento ou mudança nas circunstâncias.

Delegação e comprometimento

De acordo com a ISO 31000:2009, a introdução da gestão de riscos e a garantia de sua contínua eficácia requerem comprometimento forte e sustentado a ser assumido pela administração da organização, bem como um planejamento rigoroso e estratégico para obter-se esse comprometimento em todos os níveis. Para tanto, convém que a administração: (a) defina e aprove a política de gestão de riscos; (b) assegure que a cultura da organização e a política de gestão de riscos estejam alinhadas; (c) defina indicadores de desempenho para a gestão de riscos que estejam alinhados com os indicadores de desempenho da organização; (d) alinhe os objetivos da gestão de riscos com os objetivos e estratégias da organização; (e) assegure a conformidade legal e regulatória; (f) atribua responsabilidades nos níveis apropriados dentro da organização; (g) assegure que os recursos necessários sejam alocados para a gestão de riscos; (h) comunique os benefícios da gestão de riscos a todas as partes interessadas; e (i) assegure que a estrutura para gerenciar riscos continue a ser apropriada.

Processo de gestão de riscos

Aprovada a política de gestão de riscos e definida a responsabilidade das partes interessadas, o próximo passo consiste na **definição do processo de gestão de riscos**[5]. Neste ponto, é bom atentar para o fato que dentro de uma mesma organização podem existir múltiplos processos de gestão de riscos, cada um deles adequado para um determinado tipo de objetivo e objeto.

Expressões como risco de projeto, risco operacional, risco legal, risco de mercado, risco de crédito, risco de liquidez, risco de contágio, risco de reputação, risco de fraude e corrupção[6] são alguns exemplos de conceitos associados a modelos/processos de gestão de riscos especializados. O quadro adiante apresenta exemplos genéricos de tipos de riscos dentro dos contextos externos e internos de uma organização.

5 Alguns exemplos de iniciativas nacionais afetas à gestão de riscos encontram-se no Anexo III.
6 O TCU dispõe de Referencial de Combate a Fraude e Corrupção, disponível na biblioteca de publicações e no site htt://www.governancapublica.gov.br.

Existe rica e variada literatura versando sobre possíveis formas de se gerenciar riscos. Em comum entre vários modelos, estão aspectos como o estabelecimento de contexto; identificação, análise e avaliação de riscos; tratamento de riscos; comunicação, consulta; e monitoramento de riscos. **O desafio que se impõe nesse momento é o de garantir a integração dos modelos e processos estabelecidos de sorte a conciliar necessidades específicas e gerais, e assegurar a governabilidade, o controle e a gestão integrada dos riscos.**

■ **Quadro 11:** Insumos para formulação de arquitetura para o GRCorp, adaptado de IBGC (2007).

CONTEXTO EXTERNO	CONTEXTO INTERNO
RISCOS ECONÔMICOS	**RISCOS FINANCEIROS**
· Disponibilidade de capital · Emissões de crédito, inadimplência · Concentração · Liquidez · Mercados financeiros · Desemprego · Concorrência · Fusões / aquisições	· Falta de liquidez · Disponibilidade de bens · Acesso ao capital
RISCOS SOCIOAMBIENTAIS	**RISCOS DE PESSOAL**
· Emissões e dejetos · Energia · Desenvolvimento sustentável	· Capacidade dos empregados · Atividade fraudulenta · Saúde e segurança
RISCOS SOCIAIS	**RISCOS OPERACIONAIS**
· Características demográficas · Comportamento do consumidor · Cidadania corporativa · Privacidade · Terrorismo	· Capacidade · Design · Execução · Dependências / fornecedores
RISCOS TECNOLÓGICOS	**RISCOS TECNOLÓGICOS**
· Interrupções · Comércio eletrônico · Dados externos · Tecnologias emergentes	· Integridade de dados · Disponibilidade de dados e sistemas · Seleção de sistemas · Desenvolvimento · Alocação · Manutenção
RISCOS NATURAIS	**RISCOS DE IMAGEM**
· Desastres naturais	· Exposição negativa em meios de comunicação · Perda de confiança de partes interessadas
RISCOS LEGAIS/REGULATÓRIOS	**RISCOS LEGAIS/REGULATÓRIOS**
· Multas, sanções aplicadas por órgãos reguladores	· Suspensão de licenças de funcionamento · Legislação · Política pública · Regulamentos

Implementação da gestão de riscos

Findas as etapas de delegação e concepção, inicia-se a implementação. Na implementação da estrutura de gestão de riscos, conforme a ABNT ISO/IEC 31000, convém que: se defina a estratégia e o momento apropriado para implementação da estrutura; aplique-se a política e o processo de gestão de riscos aos processos organizacionais; atenda-se aos requisitos legais e regulamentares; assegure-se de que a tomada de decisões, incluindo o desenvolvimento e o estabelecimento de objetivos, esteja alinhada com os resultados dos processos de gestão de riscos; mantenham-se sessões de informação e treinamento; e consulte-se e comunique-se com as partes interessadas para assegurar que a estrutura da gestão de riscos continua apropriada.

Monitoramento e revisão

Ressalte-se, por oportuno, que, a fim de assegurar que a gestão de riscos seja eficaz e contribua para o desempenho organizacional, a ABNT ISO/IEC 31000 recomenda que as organizações monitorem e analisem criticamente a estrutura estabelecida. Para tanto, orientam-nas a: medir o desempenho da gestão de riscos utilizando indicadores, os quais devem ser analisados criticamente de forma periódica para garantir sua adequação; medir periodicamente o progresso obtido ou o desvio em relação ao plano de gestão de riscos; analisar criticamente e de forma periódica se a política, o plano e a estrutura da gestão de riscos ainda são apropriados, dado o contexto externo e interno das organizações; reportar sobre os riscos, sobre o progresso do plano de gestão de riscos e como a política de gestão de riscos está sendo seguida, e analisar criticamente a eficácia da estrutura da gestão de riscos. ■

CAPÍTULO 7

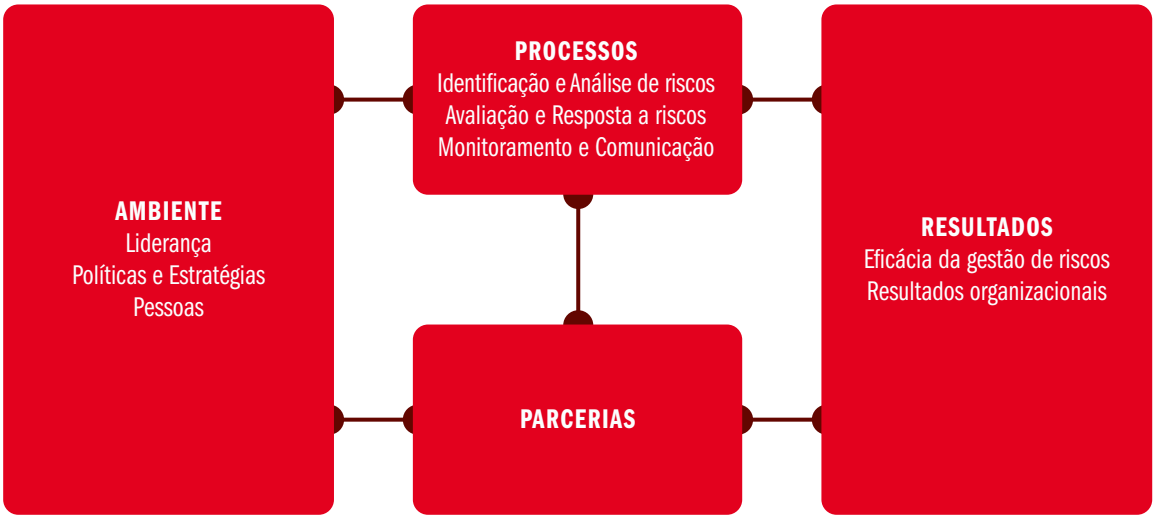
MODELO DE AVALIAÇÃO

CAPÍTULO 7
MODELO DE AVALIAÇÃO

Como forma de contribuir com o monitoramento, a revisão e a melhoria contínua dos modelos de gestão de risco adotados pela administração pública, o TCU desenvolveu um modelo de avaliação da maturidade organizacional em gestão de riscos, publicado pela Portaria-Segecex nº 9, de 18 de maio de 2017.

Tal modelo tem por referência boas práticas preconizadas pelo COSO GRC (COSO, 2004 e 2016), ABNT NBR ISO 31000 Gestão de Riscos – Princípios e Diretrizes (ABNT, 2009) e Orange Book (UK, 2004 e 2009), bem como pela IN-MP/CGU Nº 1/2016.

O modelo é composto de quatro dimensões e sua aplicação apoia-se nos **critérios descritos no Anexo IV** – Critérios para avaliação da maturidade em gestão de riscos, que também indica as fontes dos critérios.



■ **Figura 17:** Modelo de avaliação da maturidade em gestão de riscos proposto pelo TCU (BRASIL, 2013).

O modelo tem como premissas que a maturidade da gestão de riscos de uma organização é determinada pelas capacidades existentes em termos de liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho da organização no cumprimento de sua missão institucional de gerar valor para as partes interessadas com eficiência e eficácia, transparência e *accountability*, e conformidade com leis e regulamentos.

DIMENSÃO - AMBIENTE

A dimensão "Ambiente", tomada do modelo COSO GRC, engloba boas práticas, também presentes no modelo britânico, relacionados com a governança de riscos, a consideração do risco na definição da estratégia e dos objetivos em todos os níveis e aspectos humanos da gestão de riscos. Tais componentes denominam-se, respectivamente, liderança, políticas e estratégias, e pessoas.

Na dimensão "Ambiente" procura-se avaliar as capacidades existentes para que a gestão de riscos tenha as condições necessárias para prosperar na organização.

Liderança

A importância do papel da alta administração na implementação e operação da gestão de riscos é destacado em todos os modelos. O COSO GRC destaca a importância da liderança para a gestão de riscos: para que uma organização possa desfrutar de um gerenciamento de riscos eficaz, a atitude e o interesse da alta administração devem ser claros e definitivos, bem como permear toda a organização. Não é suficiente apenas dizer as palavras corretas; uma atitude de "faça o que digo e não o que faço" somente gerará um ambiente inadequado (COSO, 2016).

Em essência, busca-se avaliar em que medida os responsáveis pela governança e a alta administração exercem as suas responsabilidades de governança de riscos e alinhamento da cultura organizacional. Espera-se que assumam um compromisso forte e sustentado com a gestão de riscos, promovendo-a e dando suporte, e exerçam supervisão para obter comprometimento com o tema em todos os níveis da organização, de modo que se possa ter uma expectativa razoável de que, no cumprimento da sua missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir os seus objetivos de gerar, preservar e entregar valor às partes interessadas, tendo o cidadão e a sociedade como destinatários principais.

Políticas e Estratégias

A gestão de riscos deve fazer parte das considerações sobre estratégias e planos em todos os níveis críticos da entidade, concretizando-se pelo processo de gerenciamento de riscos nas operações, funções e atividades relevantes nas diversas partes da organização.

Nesta seção, busca-se avaliar em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.

Organizações com políticas e estratégias de gestão de riscos adequadas contam com:

(a) um processo e métodos para definir claramente objetivos e tolerâncias a risco ou variações aceitáveis no desempenho para permitir que os seus riscos e resultados possam ser gerenciados, incorporando-se explicitamente indicadores-chave de desempenho e de risco em seus processos de governança e gestão;

(b) competências e capacidade para identificar eventos potenciais que podem impactar a organização, o governo ou a comunidade e fazer uso de medidas práticas e razoáveis para gerenciar esses eventos e asseguração de que a sua administração e o seu corpo executivo:

1. estão adequadamente informados sobre as exposições a risco da organização;

2. estão completa e diretamente envolvidos em estabelecer e rever o processo de gestão de riscos em suas áreas; e

3. alocam recursos adequados e suficientes para a gestão de riscos, levando em conta o perfil de risco, o tamanho, a complexidade, a estrutura e o contexto da organização.

Pessoas

O gerenciamento de riscos é um processo efetuado pelo conselho de administração, pela diretoria executiva e pelos demais empregados, isto é, pelas pessoas, mediante o que fazem e o que dizem. São as pessoas que estabelecem a missão, a estratégia e os objetivos e implementam os mecanismos de gerenciamento de riscos da organização (COSO, 2004).

O gerenciamento de riscos afeta as ações das pessoas, pois devem adotar comportamentos requeridos pelos procedimentos prescritos e, principalmente, passar a pensar e enxergar o negócio com base em riscos. As ações das pessoas, por sua vez, afetam o desempenho da gestão de riscos - positivamente, quando agem de forma alinhada à política de gestão de riscos, e negativamente, quando não agem assim. A gestão de riscos deve proporcionar os mecanismos necessários para ajudar as pessoas a entender o risco no contexto dos objetivos da organização, bem como suas responsabilidades e seus limites de autoridade, criando uma associação clara e estreita entre os deveres das pessoas e como

elas os cumprem no tocante à estratégia e aos objetivos da organização (COSO, 2004).

Assim, são atributos importantes que devem estar presentes na conformação de um ambiente de gestão de riscos apropriado: o grau de conhecimento das pessoas sobre os objetivos da organização, a existência de canais de comunicação para que questões relacionadas a risco sejam levantadas e decididas, a definição clara de responsabilidades e limites de autoridade em relação aos processos de gestão de riscos, a existência de arcabouço conceitual de risco uniformemente conhecido e utilizado na organização, e a oferta de cursos de capacitação sobre o tema..

Nesta seção, busca-se avaliar em que medida as pessoas da organização estão informadas, habilitadas e autorizadas para exercer seus papéis e suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades; e seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.

DIMENSÃO - PROCESSOS

Os processos de gestão de riscos constituem o coração dos modelos de gestão de riscos. Para lidar com os riscos que podem impactar os objetivos de uma organização, processos devem ser estabelecidos para identificar riscos; avaliar a probabilidade de ocorrência e o impacto sobre os resultados pretendidos; escolher o tipo apropriado de resposta para cada risco; desenhar e implementar respostas para os riscos priorizados; comunicar os assuntos relacionados a risco às partes interessadas; e monitorar a integridade da estrutura e do processo de gestão de riscos. Tais processos devem estar incorporados e integrados aos processos de governança e de gestão, finalísticos e de apoio.

Esta dimensão, portanto, aborda os aspectos relacionados ao processo de gestão de riscos, procurando avaliar em que medida a organização estabeleceu um processo formal, com padrões e critérios definidos para a identificação e análise de riscos, avaliação e resposta a riscos, incluindo a seleção e a implementação de respostas aos riscos avaliados, e monitoramento e comunicação relacionada a riscos e controles.

Identificação e análise de riscos

Nesta seção, busca-se avaliar em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente às operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chave da organização), de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos.

Avaliação e resposta a riscos

Nesta seção, busca-se avaliar em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente

para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento.

Monitoramento e comunicação

Nesta seção, busca-se avaliar em que medida as atividades de monitoramento e comunicação relacionada a riscos e controles com partes interessadas, internas e externas, estão estabelecidas e são aplicadas de forma consistente na organização, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes quanto a seu desenho e operação.

DIMENSÃO - PARCERIAS

Parcerias são quaisquer arranjos estabelecidos para possibilitar relacionamento colaborativo entre partes, visando o alcance de objetivos de interesse comum. As parcerias são usualmente estabelecidas para atingir um objetivo estratégico ou a entrega de um produto ou serviço, sendo formalizadas por um determinado período, implicando a negociação e o claro entendimento das funções de cada parte, bem como dos benefícios decorrentes (BRASIL, 2009, p. 21). Envolvem, portanto riscos e benefícios compartilhados.

Esta dimensão trata de aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas, quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas, procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e sobre o seu gerenciamento.

DIMENSÃO - RESULTADOS

Esta dimensão trata de aspectos relacionados aos efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.

A razão de ser da gestão de riscos é apoiar as organizações na consecução dos resultados planejados. Portanto, todos os objetivos relevantes da organização devem fazer parte do escopo da gestão de riscos, que deverá contribuir para que haja efeitos positivos no alcance de todos eles. Os efeitos produzidos pela gestão de riscos em uma organização se dão em duas esferas: uma de efeitos imediatos e outra de efeitos mediatos.

Na esfera dos efeitos imediatos, denominada eficácia da gestão de riscos, estão os efeitos das práticas de gestão de riscos na qualidade do processo decisório, na coordenação entre unidades organizacionais, no gerenciamento de riscos com parceiros, no aperfeiçoamento de planos e políticas organizacionais, na comunicação sobre riscos com partes interessadas e no envolvimento do pessoal com a avaliação e o controle dos riscos. Os efeitos ditos mediatos são aqueles que surgem a partir da presença dos efeitos imediatos. Em outras palavras, por meio de uma gestão de riscos eficaz consegue-se melhorar resultados, por meio da otimização do desempenho da organização na sua capacidade de gerar, preservar e entregar valor.

DETERMINAÇÃO DO NÍVEL DE MATURIDADE

As capacidades existentes na organização em termos de liderança, políticas e estratégias, e preparo das pessoas para gestão de riscos, bem como o emprego dessas capacidades a processos e parcerias e os resultados obtidos com a gestão de riscos na melhoria do desempenho organizacional, podem ser avaliadas separadamente. Pode-se, portanto, falar em maturidade da organização em cada uma das dimensões do modelo, como também em maturidade global em gestão de riscos, ao se considerar todas as dimensões do modelo.

Para isso, é necessário avaliar se os princípios, a estrutura (ou os componentes) e os processos colocados em prática para o gerenciamento de riscos por toda a organização estão presentes e funcionando de forma integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização.

Avaliando os índices de maturidade de cada aspecto

O cálculo dos índices de maturidade para cada aspecto da gestão de riscos é realizado atribuindo-se quatro pontos para a presença integral e consolidada da prática ou característica de gestão enfocada, um, dois ou três, quando a presença é parcial, de acordo com sua intensidade, e zero ponto à ausência total, conforme a escala para avaliação de evidências de auditoria.

No caso de questões que admitem apenas respostas sim/não, atribuiu-se quatro pontos ao 'sim' e zero ponto ao 'não'.

Para as questões que se desdobram em itens, cada item obterá um número decimal como pontuação, resultante da divisão dos valores de pontuação possíveis (de zero a quatro, conforme explicado no parágrafo anterior) pelo número de itens que compõem a questão. Por exemplo, para uma questão com cinco itens, cada item poderá receber de zero a no máximo 0,8 (4/5).

Avaliando os índices de maturidade de cada dimensão

O índice de maturidade de cada dimensão (Ambiente; Processos; Parcerias; e Resultados) é apurado tomando-se o somatório de pontos do conjunto de questões que a compõe e calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível, expressando esse quociente com um número entre 0% e 100%. Se, por exemplo, uma dimensão obtém 40 pontos de 76 possíveis (19 questões x 4 pontos = 76 pontos), então o índice de maturidade dessa dimensão seria de 52,6% (40/76 x 100).

Determinando o nível de maturidade global da gestão de riscos

O índice de maturidade global da gestão de riscos é obtido pela média ponderada dos índices de maturidade das dimensões (IMD) pelos seguintes pesos:

DIMENSÃO	PESO	EXEMPLO		
		IMD	PESO	PONDERADO
Ambiente	40	52,6	0,4	21,0
Processos	30	45,9	0,3	13,8
Parcerias	10	80,1	0,1	8,0
Resultados	20	49,5	0,2	9,9
ÍNDICE DE MATURIDADE GLOBAL				52,7

■ **Figura 18:** Modelo de avaliação da maturidade em gestão de riscos: pesos

Os pesos de cada dimensão foram determinados usando-se a técnica *Analytic Hierarchy Process* - AHP (COYLE, 2004) aplicada às respostas dadas por oito especialistas do TCU a comparações duas-a-duas da importância relativa das quatro dimensões do modelo. A técnica AHP presta-se a facilitar a tomada de decisão por meio da hierarquização de opções com base na opinião de um grupo de pessoas acerca dos atributos de cada opção.

O índice global derivado desse cálculo permite classificar o nível de maturidade de uma organização em uma das cinco faixas.

ÍNDICE DE MATURIDADE APURADO	NÍVEL DE MATURIDADE
De 0% a 20%	Inicial
De 20,1% a 40%	Básico
De 40,1% a 60%	Intermediário
De 60,1% a 80%	Aprimorado
De 80,1% a 100%	Avançado

■ **Figura 19:** Modelo de avaliação da maturidade em gestão de riscos: níveis de maturidade

Note que os **critérios de avaliação de maturidade** selecionados pelo TCU para compor seu modelo de avaliação estão disponíveis no **Anexo IV** deste referencial. Mais informações acerca do **Modelo de avaliação de maturidade em gestão de risco** estão disponíveis na **Portaria-Segecex nº 2**, publicada pelo TCU em 22 de janeiro de 2018, aprovando o Roteiro de Avaliação de Maturidade da Gestão de Riscos, acessível no portal do TCU em www.tcu.gov.br/governanca/ ou em http://portal.tcu.gov.br/controle-externo/normas-e-orientacoes/tecnicas-estudos-e-ferramentas-de-apoio/ ■

REFERÊNCIAS BIBLIOGRÁFICAS

REFERÊNCIAS BIBLIOGRÁFICAS

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

_____. ABNT NBR ISSO/IEC 31010: *Gestão de riscos: Técnicas para o processo de avaliação de riscos*. Rio de Janeiro, 2012.

_____. ABNT ISO GUIA 73: G*estão de Riscos: Vocabulário*, 2009a.

_____. ABNT NBR ISO 26000:2010 – Diretrizes sobre responsabilidade social. Rio de Janeiro, 2010.

AUSTRÁLIA. *AS/NZS* 4360:2004 – *Risk Management*, Australia Standards, 2004. Disponível em: <http://infostore.saiglobal.com/store/details.aspx?ProductID=381579>. Acesso em: maio, 2016.

AVALOS, José Miguel Aguilera. *Auditoria e gestão de riscos*; Instituto Chiavenato (org.) – São Paulo : Saraiva, 2009.

BCBS (Basel Committee on Banking Supervision). *International Convergence of Capital Measurement and Capital Standards*: A Revised Framework. Basel: Bank for International Settlements, 2004. Disponível em: <http://www.bis.org/publ/bcbs128.htm>. Acesso em: maio, 2016.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. *Guia de Orientação para o Gerenciamento de Riscos*. Secretaria de Gestão Pública. Departamento de Inovação e Melhoria da Gestão. Gerência do Programa GESPÚBLICA. Brasília, 2013. Disponível em <http://www.planejamento.gov.br/secretarias/upload/Arquivos/segep/projeto/2013_03_01_Produto_VII_Risco_Oportunidade_PT.pdf>. Acesso em: março 2015.

_____. _____. *Método de Priorização de Processos*. Brasília, 2017. Disponível em <http:// http://www.planejamento.gov.br/assuntos/gestao/controle-interno/metodo-de-priorizacao-de-processos>. Acesso em: fevereiro 2018.

_____. _____ e Controladoria-Geral da União. *Instrução Normativa Conjunta* N° 1, de 10 de

maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, 2016. Disponível em <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=14&data=11/05/2016>. Acesso em: maio 2016.

_____. Tribunal de Contas da União. *Técnica de Auditoria Mapa de Processo*. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2003.

_____. _____. *Manual de auditoria operacional*. Brasília: TCU, 2010. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Análise SWOT e Diagrama de Verificação de Risco aplicados em Auditoria*. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010a. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Técnica de pesquisa para auditorias*. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010b. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Instrução Normativa* 63/2010. Estabelece normas de organização e de apresentação dos relatórios de gestão e das peças complementares que constituirão os processos de contas da administração pública federal, para julgamento do Tribunal de Contas da União, nos termos do Art. 7° da Lei n° 8.443, de 1992. Brasília: TCU, 2010c. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Técnica de Indicadores de Desempenho para Auditorias*. Brasília: TCU, Segecex, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010d. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Padrões de Levantamento. Portaria-Segecex* 15/2011. Brasília: TCU, Segecex, Secretaria Adjunta de Planejamento e Procedimentos (Adplan) e Secretaria Adjunta de Supervisão e Suporte (Adsup), 2011. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Curso Avaliação de Controles Internos*. Conteudistas: Antonio Alves de Carvalho Neto, Bruno Medeiros Papariello. Aula 2. Modelos de referência para controle interno. 2. ed. – Brasília: TCU, Instituto Serzedello Corrêa, 2012.

_____. _____. *Acórdão* n° 2467/2013-TCU-Plenário. Ata 35, Sessão de 11/09/2013. Levantamento de auditoria para elaboração de indicador para medir o grau de maturidade de entidades públicas na gestão de riscos. Brasília, 2013. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Curso Gestão de Riscos – Princípios e Diretrizes*. Antonio Alves de Carvalho Neto. 1. ed. presencial (slides) – Brasília: TCU, Instituto Serzedello Corrêa, 2013a.

_____. _____. *Técnica de grupo focal para auditorias*. Brasília: TCU, Secretaria de Métodos Aplicados e Suporte à Auditoria (Seaud), 2013b. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Resolução*-TCU nº 246, de 30 de novembro de 2011. Altera o Regimento Interno do Tribunal de Contas da União, aprovado pela Resolução TCU nº 155, de 4 de dezembro de 2002. Brasília, 2015. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Normas de Auditoria do Tribunal de Contas da União*. Revisão Junho 2011. Brasília: TCU, 2011. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Regimento Interno do Tribunal de Contas da União*. Brasília: TCU, 2012. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Referencial básico de governança aplicável a órgãos e entidades da administração pública*. Versão 2. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2014. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. Tribunal Regional Eleitoral do Pará. *Plano Anual de Auditoria*. Belém, 2018. Disponível em < http://www.justicaeleitoral.jus.br/arquivos/plano-anual-de-auditoria-paa-2018-tre-pa >. Acesso em: fevereiro 2018.

CADBURY, A. *Report of the Committee on the financial aspects of corporate governance*. Londres: Gee and Company Ltd, 1992. Disponível em: <http://www.ecgi.org/codes/documents/cadbury.pdf>. Acesso em: maio, 2016.

CANADÁ. Secretaria do Conselho do Tesouro do Canadá. *Framework for the management of risk. Ottawa*, 2010a. Disponível em: <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text>. Acesso em: maio de 2012.

_____. Secretaria do Conselho do Tesouro do Canadá. *Guide to integrated risk management*. Ottawa, 2010b. Disponível em: <http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggirtb-eng.asp>. Acesso em: maio de 2012.

COYLE, G. *The Analytic Hierarchy Process*. Pearson Educational: New York, 2004.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. *Controle Interno: Estrutura Integrada: Sumário Executivo e Estrutura*. Tradução: PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2013. Disponível em: <http://www.iiabrasil.org.br/new/2013/downs/coso/COSO_ICIF_2013_Sumario_Executivo.pdf>. Acesso em: março, 2017.

_____. *Gerenciamento de Riscos Corporativos: Estrutura Integrada: Sumário Executivo e Estrutura* (COSO GRC, 2004). Tradução:

PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2007. Disponível em: <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em: março, 2017.

_____. *Enterprise Risk Management: Align Risk with Strategy and Performance*. COSO, 2016. Disponível em: <http:// http://erm.coso.org/Pages/viewexposuredraft.aspx>. Acesso em: março, 2017.

DAHMS, T. *Risk management and corporate governance: are they the same?* 2008. Disponível em: <http://www.plumcon.com.au/PDF/Risk_Gov_1.pdf>. Acesso em: junho de 2013.

DANTAS, José Alves; RODRIGUES, Fernanda Fernandes; MARCELINO, Gileno Fernandes; LUSTOSA, Paulo Roberto Barbosa. *Custo-benefício do controle*: *proposta de um método para avaliação com base no COSO*. Revista de Contabilidade, Gestão e Governança. 2010.

DE CICCO, Francesco (Rev.). Gestão de Riscos: Diretrizes para implementação da ISO 31000:2009 (Série Risk Management). Risk Tecnologia Editora, 2009.

DICKSON, P. G. M. *The Sun Insurance Office*, 1710-1960: *the history of two and a half centuries of British insurance*. Londres, Oxford University Press, Reino Unido, 1960. Disponível em: <http://www.worldcat.org/title/sun-insurance-office-1710-1960-the-history-of-two-and-a-half-centuries-of-british-insurance/oclc/251088>. Acesso em: maio, 2016.

ESTADOS UNIDOS. General Accounting Office (GAO). GAO-01-1008G: *Ferramenta de gestão e avaliação de controle interno*. Washington, D.C., 2001.

_____. House of Representatives of the United States of America in Congress. *Sarbanes-Oxley Act of 2002*. Corporate responsibility. Disponível em: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>. Acesso em: maio, 2016.

FRASER, J.; SIMKINS, B. J. *Enterprise risk management: today's leading research and best practices for tomorrow's executives*. New Jersey (EUA): John Wiley & Sons, Inc., 2010. Disponível em: <http://www.amazon.com/Enterprise-Risk-Management-Practices-Executives/dp/0470499087>. Acesso em: maio, 2016.

HUBBARD, Douglas W. The Failure of Risk Management: *Why It's Broken and How to Fix It*. New Jersey (EUA): John Wiley & Sons, Inc., 2009. Disponível em: <http://www.amazon.com/Failure-Risk-Management-Why-Broken/dp/0470387955>. Acesso em: maio, 2016.

INTERNATIONAL FEDERATION OF ACCOUNTANTS - IFAC. Governance in the public sector: a governing body perspective. *International public sector study nº 13*, 2001. Disponivel em: <http://www.ifac.org/publications-resources/study-13-governance-public-sector>. Acesso em: maio, 2016.

_____. *Comparison of Principles*. Nova Iorque, NY (EUA), 2013. Disponivel em:

<http://www.ifac.org/system/files/publications/files/Comparison-of-Principles.pdf>. Acesso em: maio, 2016.

_____. *From Bolt-on to Built-in - Managing Risk as an Integral Part of Managing an Organization*. Nova Iorque, NY (EUA), 2015. Disponível em: <https://www.ifac.org/publications-resources/bolt-built>. Acesso em: Julho, 2015.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA - IBGC. *Guia de Orientação para Gerenciamento de Riscos Corporativos* (2007). Disponível em: < http://www.ibgc.org.br/userfiles/3.pdf>. Acessado em: outrubro de 2017.

INSTITUTO DOS AUDITORES INTERNOS - IIA. *Normas Internacionais para a Prática Profissional de Auditoria Interna*. Flórida, 2009. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2009.

_____. *Declaração de Posicionamento do IIA: O Papel da Auditoria Interna no Gerenciamento de Riscos*. Flórida, 2009. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2009a.

_____. *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles*. Flórida, 2013. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2013.

INTOSAI (International Organization of Supreme Audit Institutions). *Reporting Standards in Government Auditing* (ISSAI 400). Viena, 2001. Disponível em: <www.issai.org>. Acesso em: junho 2015.

_____. *Performance Audit Methodology* – to ISSAI 3000 (ISSAI 3000/Appendix 1, 2004). Viena: Intosai, 2004. Disponível em: <www.issai.org>. Acesso em: junho 2015.

_____. Subcomitê de Normas de Controle Interno. *Diretrizes para Normas de Controle Interno do Setor Público – Informações Adicionais sobre Gestão de Risco nas Entidades*. INTOSAI GOV 9130. Viena, 2007. Tradução: Antonio Alves de Carvalho Neto. Brasília, 2013.

KNIGHT, K. *Risk Management: an integral component of corporate governance and good management*. ISO Bulletin, p.21-24, Out. 2003.

LONGO, Cláudio Gonçalo. *Manual de Auditoria e Revisão de Demonstrações Financeiras*. São Paulo: Atlas, 2011.

MARTINS, N. C.; SANTOS, L. R.; DIAS FILHO, J. M. *Governança empresarial, riscos e controles internos: a emergência de um novo modelo de controladoria*. Revista Contabilidade & Finanças, São Paulo,n. 34, p. 7-22, jan./abr. 2004.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT - OCDE. *Avaliações da OCDE Sobre Governança Pública: Avaliação da OCDE sobre o Sistema de Integridade da Administração Pública Federal Brasileira - Gerenciando riscos por uma administração pública mais íntegra*. OECD Publishing, 2011. Disponível em: <http://

www.cgu.gov.br/assuntos/articulacao-internacional/convencao-da-ocde/arquivos/avaliacaointegridadebrasileiraocde.pdf/view>. Acesso em: fevereiro de 2016.

REINO UNIDO (UK). National Audit Office. Focus Groups. *How to apply the technique to vfm work*. London: NAO, 1997.

_____. _____. Comptroller and Auditor General. *Supporting innovation: Managing risk in government departments*. Londres, 2000. Disponível em: <http://www.nao.org.uk/wp-content/uploads/2000/08/9900864.pdf>. Acesso em: outubro de 2014.

_____. HM Treasury. *Management of Risk - Principles and Concepts - The Orange Book*. HM Treasury do HM Government, 2004.

_____._____. *Risk management assessment framework: a tool for departaments*. London, 2009. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/ attachment_data/file/191516/Risk_management_assessment_framework.pdf>. Acesso em: maio de 2012.

SERRA, Alberto. *Modelo aberto de gestão para resultados no setor público*. Tradução de Ernesto Montes-Bradely y Estayes. – Secretaria de Estado da Administração e dos Recursos Humanos (SEARH/RN): Natal, 2008.

SINEK, Simon. *Start with Why: How Great Leaders Inspire Everyone to Take Action*. Penguin Group: New York, 2011. ■

ANEXOS

ANEXO I

RELAÇÃO DA GESTÃO DE RISCO COM OUTRAS DISCIPLINAS

Todas as atividades de uma organização envolvem riscos, decorrentes da natureza das atividades, de realidades emergentes, de mudanças nas circunstâncias e nas demandas sociais e da própria dinâmica da administração pública. Riscos também surgem da necessidade de prestar contas e dar mais transparência à gestão, bem como de cumprir variados requisitos legais e regulatórios.

Logo, as organizações públicas precisam gerenciar riscos, identificando-os, analisando-os e, em seguida, avaliando se devem ser modificados por algum tratamento, de modo a criar as condições para o alcance dos seus objetivos e, posteriormente, monitorando os riscos tratados para verificar se as medidas adotadas cumprem sua função.

A gestão de riscos corretamente implementada e aplicada de forma sistemática, estruturada e oportuna gera benefícios que impactam diretamente os cidadãos e outras partes interessadas da organização pública ao viabilizar o adequado suporte às decisões de alocação e uso apropriado dos recursos públicos nos diversos processos de trabalho da administração pública. Dessa forma, a gestão de riscos pode auxiliar nos esforços de otimização do desempenho da administração pública e dos resultados entregues à sociedade.

A gestão de riscos não ocorre de forma isolada. Na verdade, se integra a diversos outros elementos, tais como *accountability*, governança, gestão e controle interno.

Accountability é um conceito que envolve diversas atividades: no setor público diz respeito ao dever que têm as pessoas ou instituições às quais se confia a gestão de recursos públicos de assumir responsabilidades pela realização de objetivos na implementação de políticas e no fornecimento de bens e serviços públicos custeados com esses recursos, bem como de prestar contas - à sociedade e a quem lhes delegou essas responsabilidades - sobre o desempenho, os resultados obtidos e o uso apropriado dos recursos.

É ainda a obrigação de demonstrar que administrou ou controlou os recursos mediante estratégias que permitiriam segurança razoável do alcance dos objetivos, considerando

os riscos envolvidos. O não cumprimento dessas obrigações de *accountability* é cada vez mais percebido pela sociedade como quebra das responsabilidades confiadas.

Para cumprir tais obrigações, a gestão estratégica das organizações públicas (alta administração apoiada pelas estruturas de governança) define o direcionamento estratégico, explicita os objetivos organizacionais e estabelece a liderança para que essas instituições possam cumprir suas missões. A gestão tática e a operacional, por sua vez, implementam a estratégia para realizar os objetivos.

As ações das estruturas de governança e de gestão buscam, de forma integrada, entregar o melhor valor para os cidadãos na forma de políticas, bens e serviços públicos que atendam às suas necessidades e expectativas e apresentem um retorno condizente com os recursos colocados à disposição da organização, oriundos dos tributos arrecadados da sociedade e de outras fontes de recursos que oneram o cidadão de forma direta ou indireta, como o endividamento público.

Para cumprir os objetivos inerentes às obrigações de *accountability*, tanto a tomada de decisão na definição da estratégia (por parte dos órgãos de governança e da alta administração), como a sua implementação (por parte da gestão tática e operacional), enfrentam influências de fatores internos e externos, que tornam incerto se e quando os objetivos serão atingidos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco" (ABNT, 2009).

Gerir riscos é responsabilidade afeta aos gestores nos níveis estratégico, tático e operacional da organização e essa atividade relaciona-se fortemente com a ideia de *accountability*, fato observável especialmente na etapa do processo de gestão de riscos que visa estabelecer e manter comunicação e consulta com as partes interessadas nos diversos riscos institucionais.

Governança no setor público, por sua vez, compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (BRASIL, 2014).

O desafio da governança em organizações públicas é determinar quanto risco aceitar na busca do melhor valor para os cidadãos e outras partes interessadas, o que significa prestar o serviço de interesse público da melhor maneira possível, equilibrando riscos e benefícios (INTOSAI, 2007), além da otimização dos recursos utilizados (ISACA, [COBIT 5, Framework, p. 17]). O instrumento da governança para lidar com esse desafio é a gestão de riscos (TCU, 2014).

Segundo a *The International Federation of Accountants* – IFAC (2013), prestigiadas organizações como o *The Chartered Institute*

of Public Finance and Accountancy – CIPFA, o *Office for Public Management Ltd* – OPM, a *Independent Commission for Good Governance in Public Services* – ICGGPS, o Banco Mundial e o *Institute of Internal Auditors* – IIA concordam que a existência de um sistema efetivo de gestão de riscos é componente essencial para a boa governança no setor público.

No setor público, a boa gestão de riscos contribui para: maior eficiência e eficácia operacional; possibilidade maior de alcançar objetivos relativos a serviços e políticas públicas; maior confiança dos cidadãos; melhora das informações para a tomada de decisões e o direcionamento estratégico; melhora na prevenção de perdas e na gestão de incidentes; atendimento a requisitos legais e regulamentares aplicáveis (BRASIL, 2013).

A gestão de riscos é componente essencial da governança institucional, servindo de referência para a definição e a implantação de medidas mitigadoras e/ou controles internos.

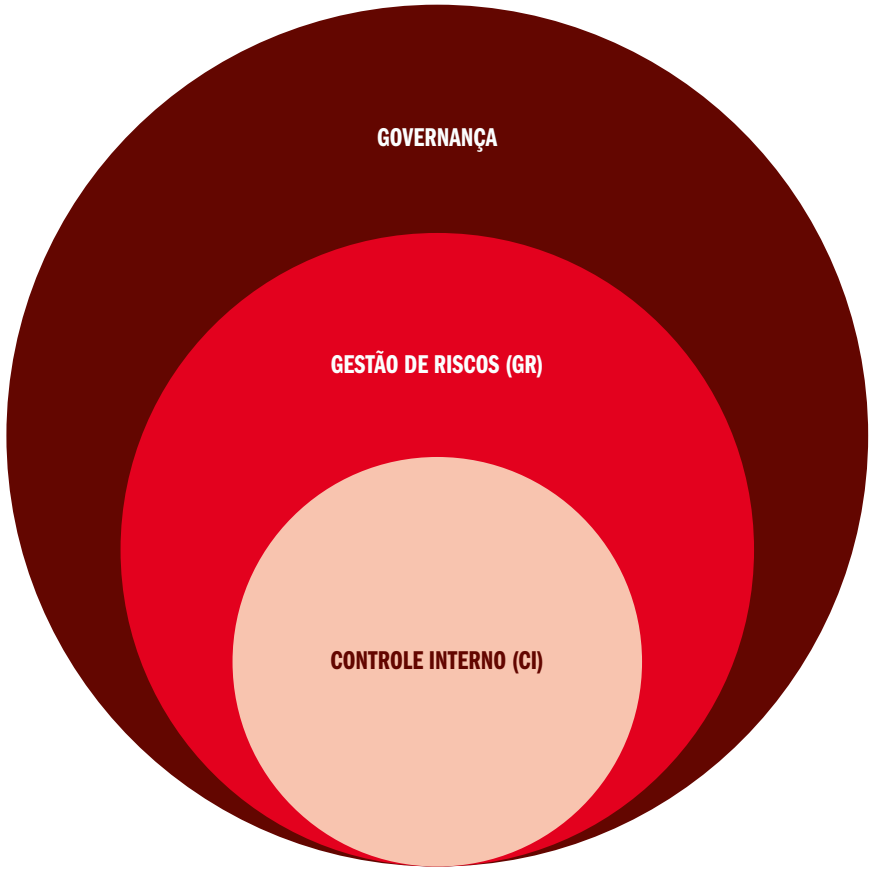
Controles internos ou atividades de controle são ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos (COSO, 2013).

Controle interno refere-se ao processo organizacional estabelecido pela alta administração para assegurar a razoável segurança no alcance de objetivos. Quando tal processo fundamenta-se na aplicação de práticas de gestão de riscos, podemos referir-nos a ele como o processo de gestão de riscos e controle interno ou sistema de gestão de riscos e controles internos, esta última a nomenclatura adotada no "Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública", publicado pelo TCU em 2014. De acordo com esse referencial, é responsabilidade da alta administração das organizações estabelecer, monitorar e avaliar o sistema de gestão de riscos e controles internos (BRASIL, 2014).

É importante não confundir controle interno com a função ou unidade organizacional de auditoria interna. A auditoria interna tem importante papel no processo ou sistema de gestão de riscos e controle interno, como visto em seção anterior, porém não deve ser entendida como sinônimo de "controle interno".

Quanto aos controles internos, ou simplesmente controles, referem-se ao 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 pelo corpo de servidores das organizações, com vistas a enfrentar os riscos. Convém que controles internos sejam implementados somente após adequada identificação, análise e avaliação dos riscos, conforme orientado na seção que descreve o processo de gestão de riscos.

O processo de controle interno é parte integrante da gestão de riscos, que, por sua vez, é parte do processo geral de governança da instituição (COSO, 2013).



■ **Figura 20:** Relação entre Governança, Gestão de Riscos e Controle Interno

ANEXO II

POLÍTICA DE GESTÃO DE RISCOS DO TCU

RESOLUÇÃO - TCU Nº 287
DE 12 DE ABRIL DE 2017

Dispõe sobre a política de gestão de riscos do Tribunal de Contas da União e altera as Resoluções-TCU 266, de 30 de dezembro de 2014, que define a estrutura, as competências e a distribuição das funções de confiança das unidades da Secretaria do Tribunal de Contas da União; a 261, de 11 de junho de 2014, que dispõe sobre a Política de Segurança Institucional (PSI/TCU) e o Sistema de Gestão de Segurança Institucional do Tribunal de Contas da União (SGSIN/TCU); e a 247, de 7 de dezembro de 2011, que dispõe sobre a Política de Governança de Tecnologia da Informação do Tribunal de Contas da União.

O TRIBUNAL DE CONTAS DA UNIÃO, no uso de suas atribuições constitucionais, legais e regulamentares,

considerando que a atuação do Tribunal de Contas da União envolve riscos relacionados a incertezas ou ao não aproveitamento de oportunidades que podem impactar no alcance de resultados e no cumprimento da missão institucional, assim como na imagem e na segurança da instituição e de pessoas;

considerando que a sistematização da gestão de riscos em nível institucional aumenta a capacidade da organização para lidar com incertezas, estimula a transparência organizacional e contribui para o uso eficiente, eficaz e efetivo de recursos, bem como para o fortalecimento da reputação da instituição;

considerando as recomendações atinentes à gestão de riscos na administração pública federal constantes dos acórdãos nº 2.467/2013,

242/2015, 548/2015, 605/2015, 673/2015, 1.220/2015, 1273/2015, 1.294/2015, 2.213/2015 e 2.524/2015, todos do Plenário;

considerando as recomendações das melhores práticas internacionais que tratam da gestão de riscos corporativos, como o COSO/ERM e as normas INTOSAI GOV 9130/2007 e ABNT NBR ISO 31000:2009; e

considerando os estudos e os pareceres constantes do processo nº TC 026.076/2015-2, resolve:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º A política de gestão de riscos do Tribunal de Contas da União observa o disposto nesta Resolução.

§ 1º A política de gestão de riscos integra o Sistema de Gestão de Riscos do Tribunal de Contas da União (SGR/TCU), o qual consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos através de toda a organização e compreende, entre outros: política, estruturas organizacionais, planos, relacionamentos, responsabilidades, atividades, processos e recursos.

§ 2º Integram-se e alinham-se à política de gestão de riscos as normas internas que regulamentam aspectos específicos dessas atividades no âmbito do TCU.

Art. 2º Para os efeitos desta Resolução, entende-se por:

I - risco: possibilidade de que um evento afete o alcance de objetivos;

II - oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos;

III - risco-chave: risco que, em função do impacto potencial ao TCU, deve ser conhecido pela alta administração;

IV - gestão de riscos: atividades coordenadas para dirigir e controlar a organização no que se refere a riscos e a oportunidades;

V - gestor de risco: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco;

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

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

VIII - nível do risco: medida da importância ou significância do risco, considerando a

probabilidade de ocorrência do evento e o seu impacto nos objetivos; e

IX - organização estendida: o próprio TCU e mais as organizações que participam da sua cadeia de valor, dentro e fora do governo, a exemplo do Congresso Nacional, entidades fiscalizadoras superiores, outros órgãos públicos e fornecedores.

CAPÍTULO II
DA GESTÃO DE RISCOS

Art. 3° A gestão de riscos no TCU tem como objetivo auxiliar a tomada de decisão com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais.

Art. 4° Constituem princípios da gestão de riscos no TCU:

I - fomentar a inovação e a ação empreendedora responsáveis;

II - considerar riscos e também oportunidades;

III - aplicar-se a qualquer tipo de atividade ou projeto;

IV - aplicar-se de forma contínua e integrada aos processos de trabalho;

V - basear-se nas melhores informações disponíveis;

VI - ser implantada por meio de ciclos de revisão e melhoria contínua;

VII - considerar a importância dos fatores humanos e culturais; e

VIII - ser dirigida, apoiada e monitorada pela alta administração.

Seção I
Das diretrizes para o processo

Art. 5° O processo de gestão de riscos no TCU contempla o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento de riscos, a comunicação e consulta com partes interessadas, o monitoramento e a melhoria contínua.

§ 1° O estabelecimento do contexto consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos encontra-se inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

§ 2° A identificação do risco compreende o reconhecimento e descrição dos riscos relacionados a um objeto de gestão, envolvendo a identificação de possíveis fontes de riscos, eventos, causas e consequências.

§ 3° A análise do risco refere-se ao desenvolvimento da compreensão sobre o risco e à determinação do nível do risco.

§ 4º A avaliação do risco envolve a comparação do nível do risco com critérios, a fim de determinar se o risco é aceitável.

§ 5º O tratamento do risco compreende o planejamento e a realização de ações para modificar o nível do risco.

§ 6º O monitoramento compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

§ 7º A comunicação e consulta refere-se à identificação das partes interessadas em objetos de gestão de riscos e obtenção, fornecimento ou compartilhamento de informações relativas à gestão de riscos sobre tais objetos, observada a classificação da informação quanto ao sigilo.

§ 8º A melhoria contínua compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento.

Art. 6º O processo de gestão de riscos no TCU deve observar:

I - o ambiente interno, o ambiente externo e a organização estendida;

II - os objetivos estratégicos, táticos e operacionais;

III - a razoabilidade da relação custo-benefício nas ações para tratamento de riscos;

IV - a comunicação tempestiva sobre riscos às partes interessadas; e

V - o acompanhamento dos riscos-chave pela alta administração.

VI - a necessidade de oportunizar a participação dos Ministros Relatores na gestão dos riscos que impactem os processos finalísticos

Parágrafo único. Nas atividades de planejamento, considera-se, sempre que couber, o risco como um dos critérios para seleção e priorização de iniciativas e ações.

Seção II
Das competências e responsabilidades

Art. 7º São instâncias responsáveis pelo Sistema de Gestão de Riscos do Tribunal de Contas da União:

I - o Plenário;

II - o Presidente;

III - a Comissão de Coordenação Geral (CCG);

IV - a Secretaria de Planejamento, Governança e Gestão (Seplan);

V - as unidades-básicas;

VI - o coordenador setorial de gestão de riscos;

VII - os gestores de risco; e

VIII - a Secretaria de Auditoria Interna (Seaud).

§ 1º Propostas de mudanças na política de gestão de riscos devem ser submetidas ao Plenário.

§ 2º Compete ao Presidente definir os limites de exposição a riscos de abrangência institucional.

§ 3º Compete à CCG avaliar propostas de mudança no SGR/TCU, apreciar propostas de limites de exposição a riscos de abrangência institucional, acompanhar a situação dos riscos-chave e determinar eventuais ações corretivas.

§ 4º A Seplan desempenha o papel de unidade central de coordenação e supervisão da gestão de riscos, sendo responsável por avaliar e propor mudanças no SGR/TCU, coordenar a implantação e a operação do SGR/TCU, monitorar riscos-chave e propor limites de exposição a riscos de abrangência institucional e assessorar o Presidente e a CCG em matérias relacionadas à gestão de riscos.

§ 5º Compete ao dirigente de cada unidade básica examinar propostas de alterações no SGR/TCU, monitorar riscos-chave e propor limites de exposição a riscos relacionados à sua área de atuação e designar coordenador setorial de gestão de riscos.

§ 6º Coordenador setorial de gestão de riscos é a pessoa ou unidade responsável por coordenar ações e promover a execução do SGR/TCU no âmbito da unidade básica a que se vincula, prover informações à unidade central, bem como apoiar os dirigentes e os gestores de riscos no desempenho das competências definidas nesta Resolução.

§ 7º Os dirigentes de unidade básica, de coordenação-geral, de unidade e chefes de gabinete são os gestores dos riscos relativos aos objetos de gestão sob sua responsabilidade.

§ 8º Compete ao gestor de risco executar as atividades do processo de gestão de riscos descritas no art. 5º para os objetos de gestão sob sua responsabilidade.

§ 9º Quando houver dúvida sobre a identificação do gestor de determinado risco no âmbito interno das unidades citadas no § 7º, cabe à chefia comum imediata decidir.

§ 10. Na hipótese de dúvida quanto à responsabilidade pela gestão de determinado risco entre unidades representadas na Comissão de Coordenação Geral (CCG), cabe a esse colegiado decidir.

§ 11. Ato do Presidente pode designar outros gestores de riscos.

§ 12. Compete à Seaud avaliar o SGR/TCU, especialmente quanto aos seguintes aspectos: adequação e suficiência dos mecanismos de gestão de riscos estabelecidos, eficácia da gestão de riscos-chave e conformidade das atividades executadas à política de gestão de riscos.

CAPÍTULO III
DAS ALTERAÇÕES EM RESOLUÇÕES

Seção I

Das alterações na Resolução-TCU 284, de 30 de dezembro de 2016.

(NR) (Acórdão nº 891/2017 – TCU – Plenário, de 10/5/2017)

Art. 8º Fica alterado o inciso I do art. 87 da Resolução-TCU 284, de 2016, que passa a vigorar com a seguinte redação:

"Art. 87. Compete à CCG:

I - assessorar o Presidente do TCU na formulação de diretrizes anuais, de políticas de gestão de pessoas, de tecnologia da informação, de riscos e de segurança institucional, assim como em outras matérias que necessitem da cooperação intersetorial das unidades cujos dirigentes compõem a CCG;"

Seção II

Das alterações na Resolução-TCU nº 261, de 11 de junho de 2014

Art. 9º. Fica alterado o § 1º do art. 3º da Resolução-TCU nº 261, de 2014, que passa a vigorar com a seguinte redação:

"Art. 3º (...)

"§ 1º A PSI/TCU é integrada pelas Políticas Corporativas de Segurança da Informação, Segurança Física e Patrimonial, Continuidade de Negócios e Segurança do Trabalho."

Art. 10. Fica excluído o inciso V do art. 7º da Resolução-TCU nº 261, de 2014.

Art. 11. Fica alterado o § 7º do art. 7º da Resolução-TCU nº 261, de 2014, que passa a vigorar com a seguinte redação:

"Art. 7º. (...)

§ 7º A gestão de riscos à segurança institucional tem por objetivo identificar, analisar, avaliar, dar tratamento adequado, comunicar e monitorar os riscos relacionados às dimensões que integram a segurança institucional e observa a política de gestão de riscos do Tribunal;"

Art. 12. Fica alterado o art. 24 da Resolução-TCU nº 261, de 2014, que passa a vigorar com a seguinte redação:

"Art. 24. As diretrizes inerentes às Políticas Corporativas de Continuidade de Negócios e de Segurança do Trabalho deverão ser oportunamente consolidadas na presente Política, com base em estudos e formulações específicos realizados pelas unidades e colegiados da Secretaria do Tribunal competentes, com posterior exame pela CCG."

Seção III

Das alterações na Resolução-TCU nº 247, de 7 de dezembro de 2011

Art. 13. Fica incluído o inciso IX no art. 10 da Resolução-TCU nº 247, de 2011, que passa a vigorar com a seguinte redação:

"Art. 10. (...)

IX - coordenar a formulação de estratégias e diretrizes de gestão de riscos de TI, de forma alinhada à política de gestão de riscos do TCU."

CAPÍTULO IV
DAS DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 14. A política de gestão de riscos do TCU será revista a cada 5 (cinco) anos ou sempre que necessário, no intuito de mantê-la atualizada diante de mudanças no ambiente interno ou externo, a partir de proposta elaborada pela Seplan.

Art. 15. Fica o Presidente do Tribunal autorizado a expedir os atos necessários à regulamentação desta Resolução e dirimir os casos omissos.

Art. 16. Esta Resolução entra em vigor na data de sua publicação.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 12 de abril de 2017.

RAIMUNDO CARREIRO
Presidente

ANEXO III
EXEMPLOS NO SETOR PÚBLICO

No setor público, alguns exemplos de documentos que tratam do tema gestão de riscos e que podem ser encontrados na internet são:

- Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão [7], publicado em janeiro de 2017 pelo Ministério do Planejamento, Desenvolvimento e Gestão – MP.

- Plano de gestão de riscos [8], publicado pelo Tribunal Superior do Trabalho em Junho de 2015, e disponível para consulta em:

- Manual de Gestão de Riscos Corporativos [9], publicado pelo Tribunal de Contas do Estado do Mato Grosso do Sul.

- Resolução nº 4.557, de 23 de fevereiro de 2017, do Bacen [10], que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

- Relatório de gestão de riscos [11], publicado pelo Banco do Brasil.

Esses são apenas alguns exemplos de iniciativas identificadas no setor público brasileiro e que estão sendo apresentados por serem de acesso público e servirem de insumo para aqueles que desejam conhecer como outras organizações estão tratando o tema. **Aqui cabe ressaltar que o TCU não avaliou o mérito e a qualidade dos referidos documentos.**

7 http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc/view
8 https://juslaboris.tst.jus.br/handle/1939/73831
9 http://www.tce.ms.gov.br/portal/download.php?caminho=1&arquivo=MTU2Mi5wZGY=
10 https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50344/Res_4557_v1_O.pdf
11 http://www.bb.com.br/docs/pub/siteEsp/ri/pt/dce/dwn/RelRis.pdf

ANEXO IV

CRITÉRIOS PARA AVALIAÇÃO DA MATURIDADE EM GESTÃO DE RISCOS

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
1. AMBIENTE Nesta dimensão, busca-se avaliar as capacidades existentes na organização em termos de liderança, políticas, estratégias e de preparo das pessoas, incluindo aspectos relacionados com *cultura*, a *governança de riscos* e a *consideração do risco na definição da estratégia* e *dos objetivos* em todos os níveis, para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento da missão institucional na geração de valor para as partes interessadas.	
1.1. Liderança Nesta seção, busca-se avaliar em que medida os responsáveis pela governança e a alta administração exercem suas *responsabilidades de governança de riscos* e *cultura*, assumindo um *compromisso* forte e sustentado e exercendo *supervisão* para obter *comprometimento* com a gestão de riscos em todos os níveis da organização, promovendo-a e dando *suporte*, de modo que possam ter uma expectativa razoável de que no cumprimento da sua missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir os seus objetivos de agregar, preservar e entregar valor às partes interessadas, tendo o cidadão e a sociedade como vetores principais.	
Cultura 1.1.1. A alta administração e os responsáveis pela governança reconhecem importância da cultura, integridade e valores éticos, e da consciência de riscos como aspectos-chave para o reforço da *accountability*:	IN-MP/CGU Nº 1/2016, Art. 8º, I e II; Art. 11, I; Art. 16, I e Art. 21; COSO GRC 2004, 2; COSO GRC *Public Exposure* (PE) 2016, Princípios 3, 4 e 5; ISO 31000:2009, 3, "h" e 4.2; OCDE, 2011.
a) fornecendo normas, orientações e supervisionando a inclusão desses aspectos-chave nos programas de apoio ao desenvolvimento de gestores;	
b) reforçando o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização; e	
c) instituindo políticas, programas e medidas definindo padrões de comportamento desejáveis, tais como códigos de ética e de conduta, canais de comunicação para cima e de denúncia, ouvidoria, e avaliação da aderência à integridade e aos valores éticos.	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
Governança de riscos 1.1.2. Os responsáveis pela governança e a alta administração utilizam instâncias internas (p.ex.: comitês de governança, riscos e controles, auditoria, coordenação de gestão de riscos etc.) e outras medidas para apoiar suas responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização.	IN-MP/CGU Nº 1/2016, Art. 23, II, Art. 17, II, "a" e "d"; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, e 2; ISO 31000:2009, 3, "b", "c", "e" e 4.1.
Supervisão da governança e da alta administração 1.1.3. Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos, inclusive mediante:	IN-MP/CGU Nº 1/2016, Art. 16, parágrafo único; Art. 19, 20 e 23, IX; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, 2 e 5; ISO 31000:2009, 4.2.
a) incorporação explícita e monitoramento regular de indicadores-chave de risco e indicadores-chave de desempenho nos seus processos de governança e gestão;	
b) notificação regular e oportuna sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos;	
c) revisão sistemática da visão de portfólio de riscos em contraste com o apetite a riscos e fornecimento de direção clara para gerenciamento dos riscos;	
d) utilização dos serviços da auditoria interna e de outras instâncias de asseguração para se certificarem de que a administração tem processos eficazes de gerenciamento de riscos e controle; e	
e) definição do nível de maturidade almejado para a gestão de riscos e monitoramento do progresso das ações para atingir ou manter-se no nível definido.	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
1.2. Políticas e estratégias Nesta seção, busca-se avaliar em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.	
Direcionamento estratégico 1.2.1. A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico (objetivos-chave, missão, visão e valores fundamentais da organização), alinhado com as finalidades e as competências legais da entidade, traduzindo uma expressão inicial do risco aceitável (apetite a risco) para a definição da estratégia e a fixação de objetivos estratégicos e de negócios, e para o gerenciamento dos riscos relacionados.	IN-MP/CGU Nº 1/2016, Art. 2º, II; Art. 14, II; Art. 16, II; e Art. 19; COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 1, 3 e 7. ISO 31000:2009, 5.3.3.
1.2.2. A alta administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o *apetite a risco* na forma de uma expressão ampla, porém suficientemente clara, de quanto risco a organização está disposta a enfrentar na implementação da estratégia para cumprir sua missão institucional e agregar valor para as partes interessadas, a fim de orientar a definição de objetivos por toda a organização; a seleção de estratégias para realizá-los; a alocação de recursos entre as unidades e iniciativas estratégicas; e a identificação e o gerenciamento dos riscos, alinhados com o apetite a risco.	IN-MP/CGU Nº 1/2016, Art. 2º, II, e Art. 14, II; Art. 16, II, e V; COSO GRC 2004, 1, 2 e 3; COSO GRC PE 2016, Princípios 1, 7 e 8; ISO 31000:2009, 3, "g" e 5.3.3.
Integração da gestão de riscos ao processo de planejamento 1.2.3. A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização e aos seus desdobramentos de modo que, a partir do direcionamento estratégico e do apetite a risco definidos conforme abordado nas questões 1.2.1 e 1.2.2, são definidos:	IN-MP/CGU Nº 1/2016, Art. 8º, VI; Art. 14, IV; Art. 16, II. COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 9, 10 e 11; INTOSAI GOV 9130/2007, 1.3 e 2.2.
a) os *objetivos estratégicos* de alto nível alinhados e dando suporte à missão, à visão e aos propósitos da organização e selecionadas as estratégias para atingi-los, considerando as várias alternativas de cenários e os riscos associados, de modo a estabelecer uma base consistente para a definição dos objetivos de negócios específicos em todos os níveis da organização; e	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
b) os *objetivos de negócios* específicos associados a todas as atividades, em todos os níveis, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade e as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho), alinhados aos objetivos estratégicos e ao apetite a risco estabelecidos.	IN-MP/CGU Nº 1/2016, Art. 8º, VI; Art. 14, IV; Art. 16, II. COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 9, 10 e 11; INTOSAI GOV 9130/2007, 1.3 e 2.2.
1.2.4. A administração define os objetivos mencionados na alínea "b", acima, e as respectivas medidas de desempenho (metas, indicadores-chave de desempenho, indicadores-chave de risco e variações aceitáveis no desempenho), explicitando-os com clareza suficiente, em termos específicos e mensuráveis, comunicando-os a todas as áreas, funções e atividades relevantes para a realização dos objetivos-chave da organização e aos responsáveis em todos os níveis, a fim de permitir a identificação e avaliação dos riscos que possam ter impacto no desempenho e nos objetivos.	IN-MP/CGU Nº 1/2016, Art. 16, II; COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 10 e 11; COSO 2013, Princípio 6, atributos "a" e "b"; INTOSAI GOV 9130, 2.2.
Política de gestão de riscos 1.2.5. A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, comunicada apropriadamente e disponível para acesso a todos, que aborde os seguintes aspectos:	IN-MP/CGU Nº 1/2016, Art. 17; ISO 31000:2009, 4.3.2.
a) os princípios e objetivos relevantes da gestão de riscos na organização e as ligações entre os objetivos e políticas da organização com a política de gestão de riscos;	IN-MP/CGU Nº 1/2016, Art. 17, I. ISO 31000:2009, 4.3.2.
b) as diretrizes para a integração da gestão de riscos a todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão em todos os níveis da organização e as parcerias com outras organizações;	IN-MP/CGU Nº 1/2016, Art. 17, II, "a"; ISO 31000:2009, 3, "b" e 4.3.4;

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
c) a definição clara de responsabilidades, competências e autoridade para gerenciar riscos no âmbito da organização como um todo e em todas as suas áreas (unidades, departamentos, divisões, processos e atividades), incluindo a responsabilidade pela implementação e manutenção do processo de gestão de riscos e de asseguração da suficiência, eficácia e eficiência de quaisquer controles;	IN-MP/CGU Nº 1/2016, Art. 17, II, "d" e III; ISO 31000:2009, 4.3.3. COSO GRC 2004, 10; COSO GRC PE 2016, Princípio 5;
d) diretrizes sobre como e com qual periodicidade riscos devem ser identificados, avaliados, tratados, monitorados e comunicados, através de um plano de implementação do processo de gestão de riscos, em todos os níveis, funções e processos relevantes da organização;	IN-MP/CGU Nº 1/2016, Art. 17, II, "b" e 18; ISO 31000:2009, 4.3.4 e 4.4.2. COSO GRC 2004, 4 a 9; COSO GRC PE 2016, Princípios 12 a 16 e 21.
e) diretrizes sobre como o desempenho da gestão de riscos, a adequação da estrutura, a aplicação do processo de gestão de riscos e a efetividade da política de gestão de riscos serão medidos e reportados; e	IN-MP/CGU Nº 1/2016, Art. 17, II, "c"; ISO 31000:2009, 4.3.2, 4.3.3 e 4.5; COSO GRC 2004, 8 e 9; COSO GRC PE 2016, Princípios 20 e 21.
f) atribuição clara de competências e responsabilidades pelo monitoramento, análise crítica e melhoria contínua da gestão de riscos, bem como diretrizes sobre a forma e a periodicidade como as alterações devem ser efetivadas.	IN-MP/CGU Nº 1/2016, Art. 17, II, "c" e III; ISO 31000:2009, 4.3.3, 4.5 e 4.6. COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 22 e 23.
Comprometimento da gestão 1.2.6. A alta administração e o corpo executivo da gestão (tática e operacional) estão completa e diretamente envolvidos em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade.	IN-MP/CGU Nº 1/2016, Art. 12 e 16, § único; Art. 17, II, "e" e "f"; Art. 19 e 20; ISO 31000:2009, 4.2 e 4.3.3.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
Alocação de recursos 1.2.7. A administração aloca recursos suficientes e apropriados (pessoas, estruturas, sistemas de TI, programas de treinamento, métodos e ferramentas para gerenciar riscos) para a gestão de riscos, considerando uma relação equilibrada com o tamanho da organização, a relevância das áreas, funções e atividades críticas para a realização dos seus objetivos-chave, bem como com a natureza e o nível dos riscos.	IN-MP/CGU Nº 1/2016, Art. 17, II, "f"; Art. 23, II, III e IX. ISO 31000:2009, 4.3.5. COSO GRC PE 2016, Princípio 2.
1.3. Pessoas Nesta seção, busca-se avaliar em que medida as pessoas na organização estão informadas, habilitadas e autorizadas para exercer seus papéis e suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.	
Reforço da *Accountability* 1.3.1. Todo o pessoal na organização, inclusive prestadores de serviços e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de se levar a sério suas responsabilidades de gerenciamento riscos, bem como é orientado e sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes. Ademais, o pessoal designado para atividades de identificação, avaliação e tratamento de riscos recebe capacitação suficiente para executá-las, inclusive no que diz respeito à identificação de oportunidades e à inovação.	IN-MP/CGU Nº 1/2016, Art. 11, IV e II; e Art. 16, III a VI; INTOSAI GOV 9130/2007, 2.7.3. ISO 31000:2009, 5.2. COSO GRC 2004, 2, 8 e 10; COSO GRC PE 2016, Princípios 3, 5, 20.
Estrutura de gerenciamento de riscos e controles 1.3.2. Os grupos de pessoas que integram as *três linhas de defesa* na estrutura de gerenciamento de riscos e controles por toda a organização têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização, especialmente quanto aos seguintes aspectos:	IN-MP/CGU Nº 1/2016, Art. 2º, III; e 3º e 6º; ISO 31000:2009, 4.3.3. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
a) Na *primeira linha de defesa*, os gestores: I. têm plena consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes; e II. são regularmente capacitados para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema.	IN-MP/CGU Nº 1/2016, Art. 2º, III; e Art. 3º; IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.
b) Na *segunda linha de defesa*, o pessoal que integra funções de coordenação de atividades de gestão de riscos e/ou de gerenciamento de riscos específicos por toda a organização: I. apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade; II. fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos; III. define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização; IV. estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos; V. orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la; VI. comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização.	IN-MP/CGU Nº 1/2016, Art. 2º, III; e Art. 6º; IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
c) Na *terceira linha de defesa*, o pessoal que integra a auditoria interna, especialmente o dirigente dessa função: I. tem conhecimento dos papéis fundamentais que a função de auditoria interna deve assumir em relação ao gerenciamento de riscos, dos que não deve assumir e dos que pode assumir com salvaguardas à independência, previstos na Declaração de Posicionamento do IIA: "*O papel da Auditoria Interna no gerenciamento eficaz de riscos corporativo*", e de fato exerce seus papéis em conformidade com essas orientações; II. tem compreensão clara da estratégia da organização e de como ela é executada, incluindo objetivos, metas, riscos associados e como esses riscos são gerenciados, e alinha as atividades da auditoria interna com as prioridades da organização; III. detém as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.	IN-MP/CGU Nº 1/2016, Art. 2º, III; IIA 2009, O papel da Auditoria Interna no gerenciamento de riscos corporativo; IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B. IIA IPPF Norma 2010, 2100, 2110 e 2210. RES CNJ 171/2013, Art. 10 e 12.
2. PROCESSO Nesta dimensão, examinam-se os processos de gestão de riscos adotados pela gestão, procurando avaliar em que medida a organização dispõe de um modelo de processo formal, com padrões e critérios definidos para a identificação, a análise e a avaliação de riscos; para a seleção e a implementação de respostas aos riscos avaliados; para o monitoramento de riscos e controles; e para a comunicação sobre riscos com partes interessadas, internas e externas.	
2.1. Identificação e análise de riscos Nesta seção, busca-se avaliar em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente às operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chave da organização), de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos.	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
Estabelecimento do contexto 2.1.1. O processo de identificação de riscos é precedido de uma etapa de estabelecimento do contexto envolvendo o entendimento, por parte de todos os participantes do processo, da organização, dos seus objetivos-chave e do ambiente no qual eles são perseguidos, com o fim de obter uma visão abrangente dos fatores internos e externos que podem influenciar a capacidade da organização de atingir seus objetivos, incluindo:	ISO 31000:2009, 5.3. COSO GRC 2004, 4; COSO GRC PE 2016, Princípio 7.
a) a identificação dos objetivos-chave da atividade, do processo ou do projeto objeto da identificação e análise de riscos é realizada considerando o contexto dos objetivos-chave da organização como um todo, de modo a assegurar que os riscos significativos do objeto sejam apropriadamente identificados;	IN-MP/CGU Nº 1/2016, Art. 8º, VI; Art. 16, II; ISO 31000:2009, 5.3.3, "a" e "b"; COSO GRC 2004, 3; COSO GRC PE 2016, Princípio 10.
b) a identificação das partes interessadas (internas e externas), bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, de modo a incluir essas partes interessadas em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta; e	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 5.3.2 e 5.3.3; COSO GRC 2004, 3; COSO GRC PE 2016, 1, item 1.
c) a comunicação e consulta com partes interessadas (internas e externas) para assegurar que as suas visões e percepções, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração no processo de gestão de riscos;	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 5.2. COSO GRC PE 2016, Princípio 20.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
Documentação do estabelecimento do contexto 2.1.2. A documentação da etapa de estabelecimento do contexto inclui pelo menos os seguintes elementos essenciais, para viabilizar um processo de avaliação de riscos consistente:	ISO 31000:2009, 5.3.4, 5.3.5 e 5.7.
a) a descrição concisa dos objetivos-chave e dos fatores críticos para que se tenha êxito (ou fatores críticos para o sucesso) e uma análise dos fatores do ambiente interno e externo (por exemplo, análise SWOT);	
b) a análise de partes interessadas e seus interesses (por exemplo, análise de *stakeholder*, análise RECI, matriz de responsabilidades); e	
c) os critérios com base nos quais os riscos serão analisados, avaliados e priorizados (como serão definidos a probabilidade e o impacto; como será determinado se o nível de risco é tolerável ou aceitável; quais os critérios de priorização para análise, avaliação e tratamento dos riscos identificados).	
Identificação e análise dos riscos 2.1.3. Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos, notadamente quanto aos seguintes aspectos:	
a) são envolvidas pessoas com conhecimento adequado, bem como os gestores executivos das respectivas áreas;	ISO 31000:2009, 5.4.2 e A.3.2.
b) são utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de risco;	ISO 31000:2009, 5.4.2.
c) o processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e outros atos impróprios, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos;	ISO 31000:2009, 5.4.2; COSO 2013, Princípio 8.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
d) o processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto;	IN-MP/CGU Nº 1/2016, Art. 16, III; ISO 31000:2009, 5.4.2.
e) a seleção de iniciativas estratégicas, novos projetos e atividades também têm os riscos identificados e analisados, incorporando-se ao processo de gestão de riscos; e	IN-MP/CGU Nº 1/2016, Art. 14, IV; ISO 31000:2009, 3, "b".
f) os riscos identificados são analisados em termos de probabilidade de ocorrência e de impacto nos objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos.	IN-MP/CGU Nº 1/2016, Art. 16, IV; ISO 31000:2009, 5.4.3.
Documentação da identificação e análise de riscos 2.1.4. No registro de riscos, a documentação da identificação e análise de riscos contém elementos suficientes para apoiar o adequado gerenciamento dos riscos, incluindo pelo menos:	ISO 31000:2009, 5.4.2, 5.4.3 e 5.7.
a) o registro dos riscos identificados e analisados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto;	
b) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise de riscos;	
c) os participantes das atividades de identificação e análise;	
d) a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas;	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
e) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos;	ISO 31000:2009, 5.4.2, 5.4.3 e 5.7.
f) os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco;	
g) a descrição dos controles existentes e as considerações quanto à sua eficácia e confiabilidade; e	
h) o risco residual.	
2.2. Avaliação e Resposta a riscos Nesta seção, busca-se avaliar em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento.	
Critérios para priorização de riscos 2.2.1. Os critérios estabelecidos para priorização de riscos levam em conta, por exemplo, a significância ou os níveis e tipos de risco, os limites de apetite a risco, as tolerâncias a risco ou variações aceitáveis no desempenho, os níveis recomendados de atenção, critérios de comunicação a instâncias competentes, o tempo de resposta requerido, revelando-se adequados para orientar decisões seguras quanto a: a) se um determinado risco precisa de tratamento e a prioridade para isso; b) se uma atividade deve ser realizada, reduzida ou descontinuada; e c) se controles devem ser implementados, modificados ou apenas mantidos.	IN-MP/CGU Nº 1/2016, Art. 16, V; ISO 31000:2009, 5.4.4; COSO GRC 2004, 6; COSO GRC PE 2016, Princípio 14.
Avaliação e seleção das respostas a riscos 2.2.2. A avaliação e a seleção das respostas a serem adotadas para reduzir a exposição aos riscos identificados considera a relação custo-benefício na decisão de implementar atividades de controle ou outras ações e medidas, além de controles internos, para mitigar os riscos.	IN-MP/CGU Nº 1/2016, Art. 14, III; ISO 31000:2009, 5.5.2; COSO GRC PE 2016, Princípio 15.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
2.2.3. Todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento, bem como são formalmente comunicados das ações de tratamento decididas, para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas.	IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, 5.5.2 e A.3.2;
Planos e medidas de contingência 2.2.4. Todas as áreas, funções e atividades relevantes (unidades, departamentos, divisões, processos, projetos) para a realização dos objetivos-chave da organização têm identificados os elementos críticos de sua atuação e têm definidos planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos seus serviços em casos de desastres.	IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.5.3.
Documentação da avaliação e seleção de respostas a riscos 2.2.5. A documentação da avaliação e seleção de respostas aos riscos inclui:	ISO 31000:2009, 5.5.3 e 5.7.
a) o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos da organização, identificando claramente os riscos que requerem tratamento e suas respectivas classificações (de probabilidade, impacto, níveis de risco etc.);	
b) a ordem de prioridade para cada tratamento;	
c) as respostas a riscos selecionadas e as razões para a seleção das opções de tratamento, incluindo a justificativa de custo-benefício;	
d) as ações de tratamento, os recursos requeridos, o cronograma e os benefícios esperados;	
e) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; e	
f) os responsáveis pela aprovação e pela implementação do plano de tratamento de riscos, com autoridade suficiente para gerenciá-lo.	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
2.3. Monitoramento e comunicação Nesta seção, busca-se avaliar em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes no desenho e na operação.	
Informação e comunicação 2.3.1. As atividades de informação e comunicação estão estabelecidas em diretrizes e protocolos efetivamente aplicados durante o processo de gerenciamento de riscos: a) diretrizes e protocolos estão estabelecidos para viabilizar o compartilhamento de informações sobre riscos e a comunicação clara, transparente, tempestiva, relevante e recíproca entre pessoas e grupos de profissionais no âmbito da organização, para que se mantenham informados e habilitados para exercer suas responsabilidades no gerenciamento de riscos; e	IN-MP/CGU Nº 1/2016, Art. 16, VII; ISO 31000:2009, 5.2 e A.3.4; COSO GRC 2004, 8; COSO GRC PE 2016, Princípio 20.
b) há efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos.	ISO 31000:2009, 5.2 e A.3.4.
Sistema de informação 2.3.2. A gestão de riscos é apoiada por um registro de riscos ou sistema de informação que: a) apoia a gestão de riscos da organização e facilita a comunicação entre pessoas e grupos de profissionais com responsabilidades sobre o processo de gestão de riscos, permitindo uma visão integrada das atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, incluindo a sua documentação; e	ISO 31000:2009, 5.7.
b) é mantido atualizado pelas diversas pessoas e funções que têm responsabilidades pela gestão de riscos em todas as áreas da organização, tanto em função das decisões e ações implementadas em todas as etapas do processo de gestão de riscos, quanto pelas atividades de monitoramento e correção de deficiências (tratadas a seguir), pelo menos quanto aos seus resultados e com referências para a documentação original completa.	ISO 31000:2009, 5.7 e 5.6 (final).

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
Monitoramento contínuo e autoavaliações 2.3.3. Em todos os níveis da organização, os gestores que têm propriedade sobre riscos (*primeira linha de defesa*) monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade: a) de modo contínuo, ou pelo menos frequente, por meio de indicadores-chave de risco, indicadores-chave de desempenho e verificações rotineiras, para manter riscos e resultados dentro das tolerâncias a riscos definidas ou variações aceitáveis no desempenho;	
b) por meio de autoavaliações periódicas de riscos e controles (*Control and Risk Self Assessment* – CRSA), que constam de um ciclo de revisão periódica estabelecido; e	IN-MP/CGU Nº 1/2016, Art. 11, V; Art. 16, VIII; ISO 31000:2009, 5.6; COSO 2013, Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.
c) a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança.	
2.3.4. As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha de defesa):	
a) exercem uma supervisão efetiva dos processos de gerenciamento de riscos, inclusive das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa; e	IIA IPPF – Definição da atividade de Auditoria Interna.
b) fornecem orientação e facilitação na condução das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa, mantém sua documentação e comunica os seus resultados às instâncias apropriados da administração e da governança.	
Monitoramento periódico e avaliações independentes 2.3.5. A função de auditoria interna exerce o seu papel de auxiliar a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança:	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
a) estabelece planos anuais ou plurianuais baseados em riscos, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança;	IIA IPPF Norma 2010, 2100 e 2110. RES CNJ 171/2013, Art. 10 e 12.
b) utiliza abordagem baseada em risco ao definir o escopo e planejar a natureza, época e extensão dos procedimentos de auditoria em seus trabalhos, incluindo a identificação e análise dos riscos e o exame de como eles são gerenciados pela gestão da área responsável; e	IIA IPPF Norma 2201 e 2210. RES CNJ 171/2013, Art. 24.
c) fornece asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gestão de riscos e controle operam de maneira eficaz e que os riscos significativos são gerenciados adequadamente em todos os níveis da organização.	IIA 2009, O papel da Auditoria Interna no gerenciamento de riscos corporativo.
2.3.6. Há planos e medidas de contingência definidos para os elementos críticos da atuação da entidade, em todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização e estes são periodicamente testados e revisados.	ISO 31000:2009, 5.6.
Monitoramento de mudanças significativas 2.3.7. Estão estabelecidos e em funcionamento procedimentos e protocolos para monitorar e comunicar mudanças significativas nas condições que possam alterar o nível de exposição a riscos e ter impactos significativos na estratégia e nos objetivos da organização.	COSO 2013, Princípio 9; COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 22.
Correção de deficiências e melhoria contínua 2.3.8. Os resultados das atividades de monitoramento são utilizados para as tomadas de medidas necessárias à correção de deficiências e à melhoria contínua do desempenho da gestão de riscos, incluindo, por exemplo: a) comunicação às instâncias apropriadas da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias; b) elaboração e devido acompanhamento de planos de ação para corrigir as deficiências identificadas e melhorar o desempenho da gestão de riscos.	IN-MP/CGU Nº 1/2016, Art. 8º, XV; ISO 31000:2009, 4.5, 4.6 e A.3.1; COSO 2013, Princípio 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 23.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
3. PARCERIAS Nesta dimensão, examinam-se os aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas (quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas), procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento.	
3.1. Gestão de riscos em parcerias Nesta seção, busca-se avaliar em que medida a organização adota um conjunto de práticas essenciais de gestão de riscos para ter segurança razoável de que os riscos no âmbito das parcerias serão adequadamente gerenciados e os objetivos alcançados.	
Avaliação da capacidade de gestão de riscos das entidades parceiras 3.1.1. O compartilhamento dos riscos é precedido de avaliação fundamentada e documentada da capacidade das potenciais organizações parceiras para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado.	ISO 31000:2009, 4.3.3 e A.3.3;
Definição de responsabilidades, informação e comunicação 3.1.2. São designados responsáveis com autoridade e recursos para tomar e implementar decisões relacionadas ao gerenciamento dos principais riscos relacionados a cada objetivo, meta ou resultado esperado das políticas de gestão compartilhadas por meio de parcerias, e são definidas em quais condições e para quem cada responsável deve fornecer informações.	IN-MP/CGU Nº 1/2016, Art. 20 e 16, VII; ISO 31000:2009, 4.3.3 e A.3.2.
Processo de gestão de riscos em parcerias 3.1.3. O processo de gestão de riscos é aplicado para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado pretendido das políticas de gestão compartilhadas.	ISO 31000:2009, 4.4.2;
3.1.4. Pessoas de todas as áreas, funções ou setores das organizações parceiras com envolvimento na parceria e outras partes interessadas no seu objeto participam do processo de identificação e avaliação dos riscos relacionados a cada objetivo, meta ou resultado esperado das parcerias.	ISO 31000:2009, 5.4.2 e A.3.2.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
3.1.5. Um registro de riscos único é elaborado na identificação e avaliação dos riscos e é atualizado conjuntamente pelas organizações parceiras em função das atividades de tratamento e monitoramento de riscos.	ISO 31000:2009, 5.7 e 5.6 (final).
3.1.6. Há informação regular e confiável para permitir que cada organização parceira monitore os riscos e o desempenho em relação a cada objetivo, meta ou resultado esperado.	IN-MP/CGU Nº 1/2016, Art. 16, VII;ISO 31000:2009, 5.2 e A.3.4; COSO GRC PE 2016, Princípio 20.
3.2. Planos e medidas de contingência Nesta seção, busca-se avaliar em que medida a organização estabelece, em conjunto com as entidades parceiras, planos e medidas de contingência para garantir a recuperação e a continuidade da prestação de serviços em caso incidentes.	
Planos e medidas de contingência 3.2.1. As organizações parceiras definem planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços em casos de desastres ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar. 3.2.2. Os planos e medidas de contingência são periodicamente testados e revisados.	IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.6.
4. RESULTADOS Nesta dimensão, examinam-se os efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.	
4.1. Melhoria dos processos de governança Nesta seção, busca-se avaliar em que medida a organização integra a gestão de riscos em seus processos de governança e gestão e isso tem sido eficaz para a sua melhoria.	

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
Integração da gestão de riscos aos processos organizacionais 4.1.1. Os responsáveis pela governança e a alta administração sabem até que ponto a administração estabeleceu uma gestão de riscos eficaz, integrada e coordenada por todas as áreas, funções e atividades relevantes e críticas para a realização dos objetivos-chave da organização, tendo consciência do nível de maturidade atual e do progresso das ações em curso para atingir ao nível almejado.	IN-MP/CGU Nº 1/2016, Art. 8º, II; Arts. 19, 20, 21, parágrafo único, 22 e 23; ISO 31000:2009, 4.3.4 e A.3.5; COSO GRC 2004, 10. COSO GRC PE 2016, Princípio 1.
4.1.2. Os objetivos-chave, que traduzem o conjunto de valores a serem gerados, preservados e/ou entregues à sociedade estão identificados e refletidos na cadeia de valor, na missão e visão e da organização e nos seus valores fundamentais, formando a base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios.	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 3 "a" e 5.3.1; COSO GRC 2004/2016, Premissa.
4.1.3. Os objetivos estratégicos e de negócios estão estabelecidos, alinhados com o direcionamento estratégico (item anterior), juntamente com as medidas de desempenho (metas, indicadores-chave de desempenho, indicadores-chave de risco e variações aceitáveis no desempenho), permitindo medir o progresso e monitorar o desempenho de todas as áreas, funções e atividades relevantes da organização para a realização dos seus objetivos-chave.	IN-MP/CGU Nº 1/2016, Art. 16, II; ISO 31000:2009, 4.2, itens 3 e 4; COSO GRC 2004, 3. COSO GRC PE 2016, Dimensão 2.
4.1.4. Estão identificados, avaliados e sob tratamento e monitoramento os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chave da organização, com o desempenho sendo comunicado aos níveis apropriados da administração e da governança.	IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, A.2 e A.3.2. COSO GRC 2004, 4; COSO GRC PE 2016, Princípios 12 a 16.

DIMENSÕES DO MODELO DE AVALIAÇÃO E PRÁTICAS RELACIONADAS	FONTES DOS CRITÉRIOS
4.2. Resultados-chave da gestão de riscos Nesta seção, busca-se avaliar em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.	
Entendimento dos objetivos, riscos, papéis e responsabilidades 4.2.1. Os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos.	ISO 31000:2009, A.2.
Garantia proporcionada pela gestão de riscos 4.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, que:	COSO GRC 2004, 1, Anexo 1.1.
a) entendem até que ponto os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chave da organização;	COSO GRC 2004, 1, Anexo 1.1.
b) entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados;	
c) a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável;	
d) as leis e os regulamentos aplicáveis estão sendo cumpridos.	
Eficácia da gestão de riscos 4.2.3. Os riscos da organização estão dentro dos seus critérios de risco, vale dizer, dentro do apetite a risco definido e das variações aceitáveis no desempenho ou tolerâncias a risco estabelecidas, conforme a documentação resultante da aplicação do processo de gestão de risco, atualizada pelas atividades de monitoramento.	ISO 31000:2009, A.2.

ANEXO V

ACÓRDÃO 2.467/2013 – TCU – Plenário

FICHA-SÍNTESE DO ACÓRDÃO
2.467/2013 – TCU – PLENÁRIO
RELATORA: MINISTRA ANA ARRAES
TC 011.745/2012-6

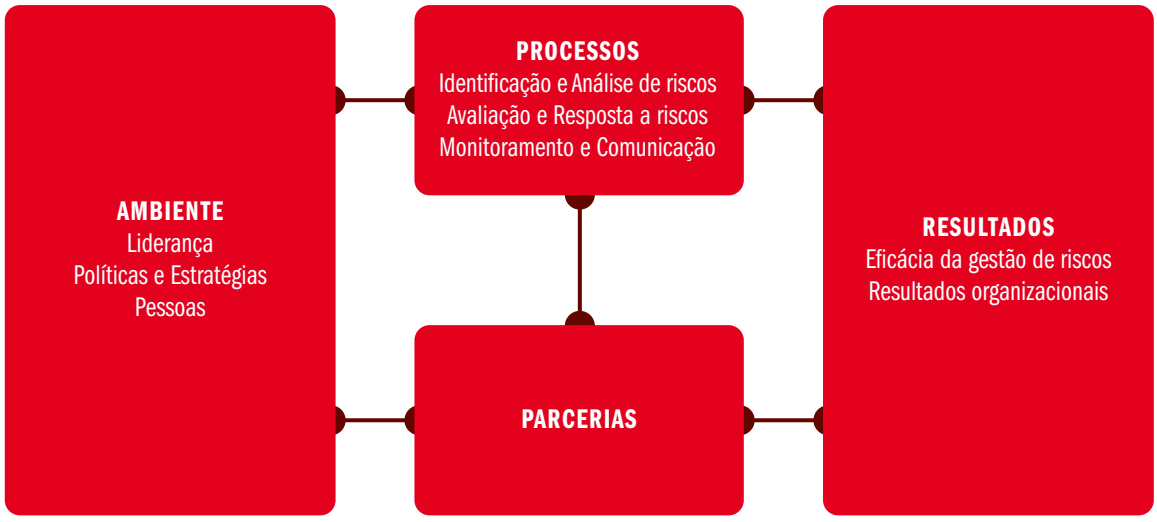
Organizações públicas, privadas e do terceiro setor estão expostas a uma ampla gama de riscos que podem afetar suas operações e o alcance de seus objetivos. Para aumentar a chance de alcançar os resultados pretendidos, as organizações devem gerenciar de forma sistemática seus riscos, o que requer contar com um processo de identificação, avaliação e implementação de respostas a riscos. A gestão de riscos também exige que os riscos e o sistema de gestão de riscos sejam monitorados.

A gestão de riscos é um elemento essencial para a boa governança corporativa justamente porque contribui para reduzir as incertezas que cercam o alcance de resultados. Conhecer o grau de maturidade da gestão de riscos de organizações públicas é importante para que o TCU possa fazer recomendações de caráter estruturante para a melhoria da governança e assim contribuir para a efetividade das políticas e dos serviços públicos.

Levantamento conduzido pelo TCU entre novembro de 2012 e fevereiro de 2013 com 65 entidades da administração pública federal indireta brasileira teve por objetivo avaliar a maturidade da gestão de riscos dessas organizações. O levantamento buscou também identificar os aspectos da gestão de riscos que necessitam ser aperfeiçoados pelas organizações e captar informações relevantes para o planejamento de futuras ações de controle do TCU.

Com base em modelos de referência, em especial COSO ERM e ISO 31000, o TCU elaborou indicador de maturidade[12] em gestão de riscos composto por itens agrupados em quatro dimensões fundamentais de análise: 1) ambiente de gestão de riscos; 2) processos de gestão de riscos; 3) gestão de riscos em parcerias; e 4) resultados obtidos com a gestão de riscos. Cada dimensão do modelo foi detalhada em subdimensões, conforme indicado na figura abaixo.

12 Nesse levantamento foi utilizada uma versão ANTERIOR do modelo de avaliação descrito no capítulo 7 deste referencial.



■ **Figura 21:** Modelo de maturidade utilizado no levantamento conduzido pelo TCU em 2012/2013

Os itens selecionados para compor o indicador de maturidade, organizados em um questionário com 56 perguntas fechadas e oito abertas, representam aspectos relevantes de uma gestão de riscos madura.

O questionário construído foi enviado ao dirigente máximo das organizações por meio de correio eletrônico. Os pesquisados foram selecionados por critérios de relevância e materialidade, sendo 26 autarquias, duas fundações, dezessete sociedades de economia mista e vinte empresas públicas.

A análise das respostas permitiu estimar o nível de presença, em cada entidade, de práticas de gestão de riscos. A agregação dessas respostas, por sua vez, expressa por meio de percentagens, possibilitou estimar o nível de maturidade, total e em cada dimensão, da organização conforme critérios a seguir.

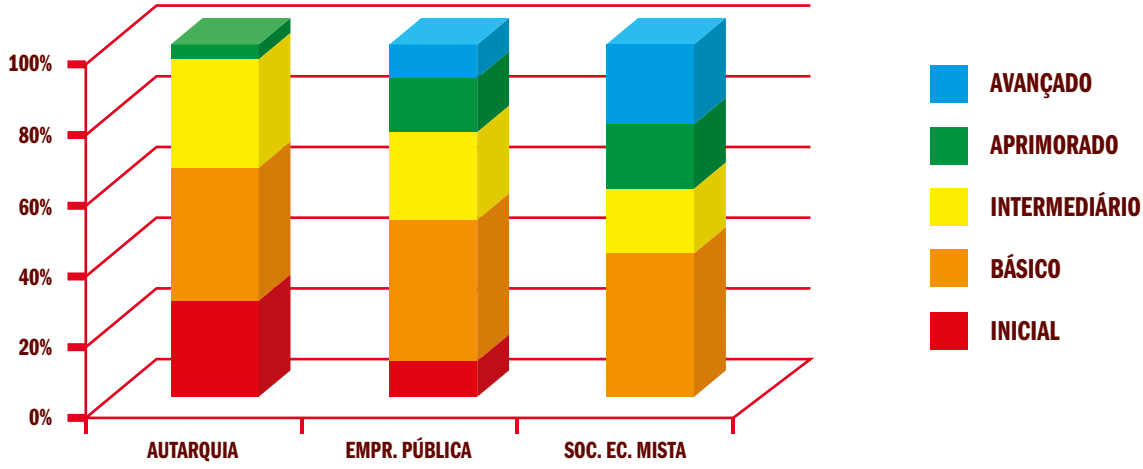
■ **Figura 12:** Maturidade da gestão de riscos

ÍNDICE DE MATURIDADE	NÍVEL DE MATURIDADE	DESCRIÇÃO
0% a 20%	Inicial	Baixo nível de formalização; documentação sobre gestão de riscos não disponível; ausência de comunicação sobre riscos.
20,1% a 40%	Básico	Gestão de riscos tratada informalmente; ainda não há treinamento e comunicação sobre riscos.
40,1% a 60%	Intermediário	Há princípios e padrões documentados, e treinamento básico sobre gestão de riscos
60,1% a 80%	Aprimorado	Gestão de riscos obedece aos princípios estabelecidos; é supervisionada e regularmente aprimorada
80,1% a 100%	Avançado	Gestão de riscos otimizada; princípios e processos de gestão de riscos estão integrados aos processos de gestão da organização.

As descrições de cada nível de maturidade têm caráter indicativo e podem não corresponder exatamente à situação de algumas organizações participantes do levantamento.

No trabalho julgado pelo Acórdão 2467/2013–TCU–Plenário, voltado a avaliar a maturidade da gestão de riscos, especificamente da administração pública indireta, evidenciou-se que dois terços das organizações participantes da pesquisa estão nos níveis básico e intermediário e que apenas 9% da amostra atingiu o estágio avançado. Verificou-se que, se o conjunto de entidades respondentes fosse visto como sendo uma única organização, atribuindo-se peso idêntico para cada uma delas, seu nível de maturidade seria considerado intermediário (índice de 43%). Tais dados indicam haver bastante espaço para que a gestão de riscos possa ser estruturada e fortalecida nas referidas organizações, com potenciais ganhos para a sociedade em termos de maior garantia de que os resultados da ação pública sejam, de fato, alcançados.

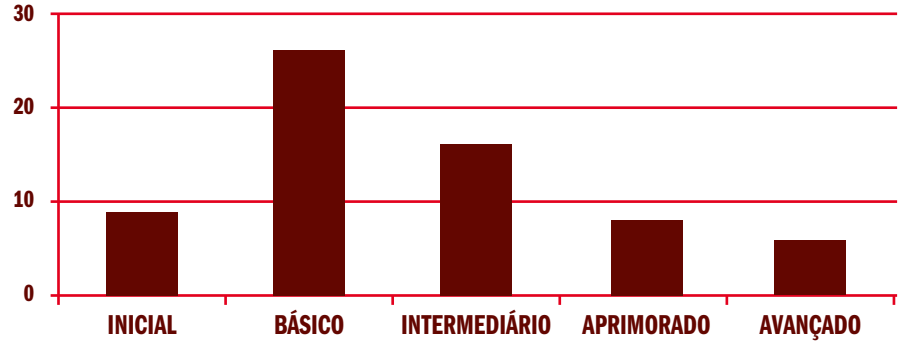
■ **Gráfico 1:** Percentual de entidades em cada nível de maturidade de gestão de riscos segundo sua vinculação ministerial.



Fonte: Acórdão 2467/2013 – TCU – Plenário

Observando-se a amostra de entidades agrupadas segundo sua natureza, demonstrada no gráfico acima, pode-se notar que as sociedades de economia mista têm a gestão de riscos mais desenvolvida que as empresas públicas, as quais, por sua vez, estão à frente das autarquias. O resultado é consistente com o fato de que a gestão de riscos tem origem no ambiente corporativo e é mais necessária em ambientes onde há maior incerteza quanto ao alcance de resultados, bem como com a suposição de que as sociedades de economia mista e as empresas públicas atuam em ambiente mais semelhante ao corporativo do que as autarquias.

■ **Gráfico 2:** Número de entidades segundo o nível de maturidade em gestão de riscos.



Fonte: Acórdão 2467/2013 – TCU – Plenário

Os dados mostram que há muitas oportunidades de melhoria nas práticas de gestão de riscos, ainda que as metas quanto ao nível de maturidade a se alcançar possam variar, conforme a necessidade de cada organização.

Diante desse cenário e, face às incertezas do ambiente econômico, político e social que o Brasil ora enfrenta, torna-se premente uma mudança de postura por parte da Administração Pública com relação a riscos. Em especial, faz-se necessária a disseminação e a prática de métodos e técnicas de gestão de riscos nas organizações públicas (Acórdão 2.467/2013-TCU-Plenário), o que requer, entre outras ações:

a. promover ações para conscientização da vinculação entre a gestão de riscos e o alcance dos objetivos da organização, incluindo o uso dessa atividade nos processos de trabalho que apresentem riscos maiores, como as contratações públicas;

b. instituir política corporativa de gestão de riscos e comunicá-la a todos na organização;

c. estruturar ou aprimorar as etapas de identificação, avaliação, tratamento, monitoramento e comunicação de riscos;

d. instituir a delegação clara e formal da responsabilidade pelo gerenciamento de riscos aos gestores;

e. instituir a capacitação regular de gestores para lidar com riscos;

f. manter os servidores informados dos objetivos e prioridades da organização e de suas unidades, assim como os riscos enfrentados podem afetar o alcance dos objetivos estabelecidos;

g. orientar e estimular os servidores a encaminhar assuntos relacionados a risco às instâncias decisórias adequadas, incluindo as de governança da organização;

h. estruturar e operacionalizar ou aperfeiçoar a gestão de riscos em parcerias.

Aqui cabe destacar que, dentre as deliberações do TCU, estão as determinações direcionadas à Secretaria de Métodos Aplicados e Suporte à Auditoria (Seaud) para que divulgue os resultados do levantamento de forma consolidada, observando-se a confidencialidade das respostas fornecidas; divulgue às entidades participantes as respectivas avaliações individualizadas; e acompanhe as ações do Ministério do Planejamento, Orçamento e Gestão voltadas à disseminação de metodologia de gestão de riscos.

Como resultado deste trabalho, espera-se que as entidades pesquisadas usem os resultados da avaliação para impulsio-

nar seus processos de fortalecimento da gestão de riscos. Entre os benefícios que as organizações poderão obter, destacam-se: maior possibilidade de alcançar seus objetivos; melhoria da eficiência e eficácia operacional; melhoria da governança; maior confiança das partes interessadas na organização; melhoria na prevenção de perdas e gestão de incidentes; melhores informações para a tomada de decisão e o planejamento; e atendimento a requisitos legais e regulamentares aplicáveis.

ANEXO VI

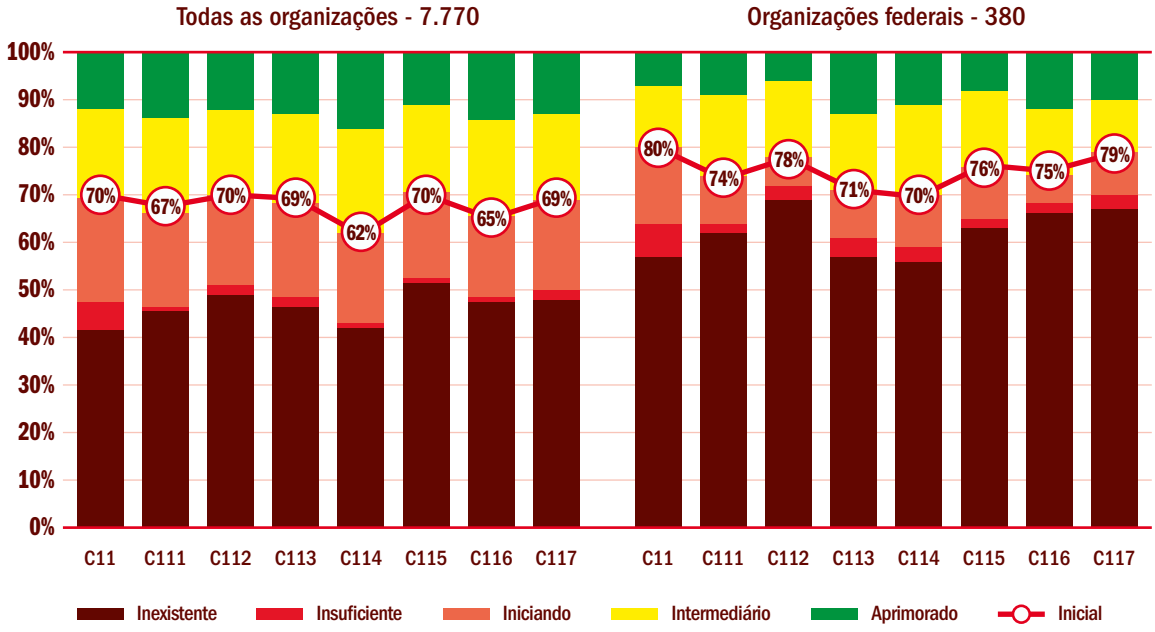
ACÓRDÃO 1.273/2015 – TCU – Plenário

FICHA-SÍNTESE DO ACÓRDÃO
1.273/2015 – TCU – PLENÁRIO
RELATOR: MINISTRO AUGUSTO NARDES
TC Nº 020.830/2014-9

"Organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tornam incertos se e quando atingirão seus objetivos. O efeito que esta incerteza tem sobre os objetivos da organização é chamado de risco" (ABNT NBR ISO 31000:2009).

A gestão de riscos refere-se ao processo de aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, avaliação, tratamento, monitoramento e análise crítica dos riscos (ABNT NBR ISO 31000:2009). Além da identificação e decisão quanto ao tratamento dos riscos, a gestão de riscos envolve também a contínua avaliação da eficácia dos controles internos implantados na organização para mitigar os riscos relevantes.

A autoavaliação em gestão de riscos é parte resultante do Levantamento de Governança Pública, realizado pelo TCU em 2014 (www.tcu.gov.br/perfilgov). Nesse levantamento, 7.770 organizações públicas em todo o país responderam a um questionário sobre boas práticas que podem ser adotadas para desenvolver a governança na organização. Entre as assertivas, havia diversas proposições relacionadas à gestão de riscos. O resultado do levantamento, no que tange à adoção de práticas de gestão de riscos e controles internos está representado na figura abaixo:



C111 - Diretrizes para gestão de riscos e estabelecimento de controles internos estão definidas, e incluem a definição da tolerância ao risco, de papéis e responsabilidades, de critérios de classificação de riscos.

C112 - O processo de gestão de riscos está implantado e contempla os seguintes componentes: ambiente de controle; fixação de objetivos; avaliação de riscos; atividades de controle; informação e comunicação; atividades de monitoramento.

C113 - Riscos críticos da organização estão identificados.

C114 - Controles internos para reduzir os riscos críticos identificados estão implantados.

C115 - Plano de continuidade, relacionado aos elementos críticos de sua área de atuação, está implantado.

C116 - A responsabilidade por coordenar a estrutura de gestão de riscos da organização está atribuida.

C117 - As instâncias internas de governança utilizam as informações resultantes do processo de gestão de riscos para apoiar seus processos decisórios.

■ **Figura 22:** Resultado do levantamento nacional de governança, no que tange à gestão de riscos (2014).

Segundo as respostas declaradas pelas organizações participantes acerca da gestão de riscos e o método de análise utilizado no trabalho, pode-se afirmar que

1. 70% de todas as organizações estariam no estágio de capacidade inicial em "Estabelecer estrutura de gestão de riscos" (C11). No contexto da Administração Pública Federal (APF), 80% das organizações estariam no estágio inicial (C11). Esses resultados sugerem ineficácia da gestão de riscos nessas organizações;

2. 49% de todas as organizações e 69% das organizações federais declararam que o processo de gestão de

riscos não está implantado (estágio de capacidade inexistente, item C112). Esse quadro é considerado crítico para a administração pública, pois interfere diretamente na capacidade de as organizações gerarem valor e cumprirem seus objetivos;

3. 47% de todas as organizações e 57% das organizações federais não identificam riscos críticos (estágio de capacidade inexistente, item C113) e, portanto, não têm como estabelecer controles internos para mitigá-los. Isso mantém a organização exposta a esses riscos, fazendo com que eventos negativos que venham a se concretizar tragam impactos significativos aos objetivos organizacionais, e eventos positivos não sejam aproveitados.

Dentre todas as práticas sugeridas no questionário de governança pública, a prática de gestão de riscos foi a que apresentou menor aderência por parte dos respondentes, com a maioria das organizações classificadas no estágio inicial, e em torno de apenas 10% no estágio de capacidade aprimorada. Os dados obtidos demonstraram a necessidade de aprimoramento da estrutura de gestão de riscos em grande parte da administração pública, de maneira a reduzir o impacto negativo dos riscos sobre as metas organizacionais. É importante observar que o comprometimento da alta administração dessas organizações é essencial para a mudança desse cenário.

Acerca desse tema, assim deliberou o TCU: (a) recomendar à Casa Civil da Presidência da República, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que elaborem modelo de governança para aprimorar a atuação das organizações públicas, que contemple medidas para a solução das fragilidades detectadas no presente levantamento afetas a estratégia, gerenciamento de risco, atuação das unidades de auditoria interna, aprovação formal de planos pelo dirigente máximo, direcionamento estratégico e supervisão de resultados; (b) encaminhar cópia do acórdão que vier a ser proferido nestes autos, acompanhado do relatório e voto que o fundamentam à(o)(s): Tribunal de Contas da União, Câmara dos Deputados e Senado Federal, para que avaliem as orientações contidas no acórdão que vier a ser proferido e adotem as medidas necessárias ao aperfeiçoamento da governança no seu âmbito.

Em resposta à essa deliberação o Ministério do Planejamento, em conjunto com a CGU publicou a Instrução Normativa Conjunta MP/CGU nº 01/2016.

ANEXO VII

ACÓRDÃO 2.127/2017– TCU – Plenário

FICHA-SÍNTESE DO ACÓRDÃO
2.127/2017– TCU – PLENÁRIO
RELATOR: MINISTRO-SUBSTITUTO
MARCOS BEMQUERER
TC Nº 018.218/2017-2

Relatório de Políticas e Programas de Governo (RePP) foi desenvolvido em cumprimento ao disposto no art. 123 da Lei de Diretrizes Orçamentárias (LDO) 2018, que confere ao Tribunal de Contas da União (TCU) a responsabilidade por enviar à Comissão Mista de Planos, Orçamentos Públicos e Fiscalização (CMO) do Congresso Nacional um quadro-resumo relativo à qualidade da implementação e ao alcance de metas e objetivos dos programas e ações governamentais objeto de auditorias operacionais realizadas, para subsidiar a discussão do Projeto de Lei Orçamentária Anual.

No sentido de alcançar seu propósito, o RePP 2017 busca: a) analisar os problemas estruturantes nos pilares da atuação estatal que impactam de forma sistêmica os resultados das políticas, programas e ações governamentais, com base em acórdãos do TCU e em estudos voltados a analisar a estrutura de governança e gestão pública; b) consolidar informações de um conjunto de fiscalizações realizadas pelo TCU a partir de 2014 em políticas, programas e ações governamentais, relacionados a áreas consideradas prioritárias e identificar isoladamente e de forma agregada, os principais problemas que afetam o alcance de resultados desses programas e ações; c) destacar aspectos do contexto nacional relevantes para efetividade da discussão orçamentária, por meio da evolução do tamanho do estado brasileiro, da percepção da sociedade sobre o retorno advindo dos programas e ações governamentais e, finalmente, da evolução de indicador voltado a demonstrar se, comparativa e historicamente, o país tem avançado na direção almejada a um custo adequado para o cidadão e para as empresas.

Desse modo, o relatório traz uma análise ampla e consolidada dos problemas que devem ser enfrentados e superados pelo Estado brasileiro no sentido de garantir efetividade na atuação governamental e transformação da realidade atual.

O Relatório de Políticas e Programas de Governo (RePP) apresenta como achado fundamental que a existência de déficits institucionais de governança e de gestão da administração pública federal produzem ineficiências generalizadas no gasto público federal. As ineficiências apontadas no relatório implicam consideráveis desperdícios e desvios sistêmicos na aplicação dos recursos públicos federais. Com base na análise dos achados consolidados, conclui-se que os referidos déficits institucionais, se não corrigidos, são capazes de perenizar a baixa eficácia dos bens e serviços públicos ofertados pelo Estado, que têm sido percebidos pela sociedade, em regra, como inadequados e de pouca qualidade.

No tocante aos problemas estruturantes na Administração Pública Federal, verificou-se a existência de falhas na estratégia do Estado, como ausência de plano de longo prazo, fragilidades do PPA, ausência generalizada de planos estratégicos institucionais e falta de uniformidade e padronização dos planos nacionais setoriais, que dificultam o desenvolvimento sustentável de políticas e programas públicos e prejudicam a efetividade das ações governamentais.

Além disso, o relatório afirma que a baixa capacidade do Estado em planejar e coordenar as diversas políticas públicas tem levado a aumento do risco de desperdício de recursos, do comprometimento de resultados e da baixa qualidade dos serviços à população. Ademais, existem impropriedades na Governança Orçamentária do país que comprometem a alocação efetiva e eficiente do gasto público.

Outra questão importante apontada foi a **ineficiência dos mecanismos de monitoramento e avaliação governamental e gestão de riscos**, que, respectivamente, dificultam o acompanhamento e aferição de resultados e impedem o alcance dos objetivos almejados.

No intuito de mitigar tais falhas e aprimorar a capacidade de entrega governamental, na proposta de encaminhamento apontam-se oportunidades de aprimoramento em atividades-chave do Estado, notadamente, no arcabouço de planejamento e orçamento e na capacidade de articulação, monitoramento e avaliação da coerência do conjunto de programas e ações governamentais. Aprimoramento esse que será monitorado pelo TCU em ações de controle futuras.

À luz desses e outros achados, o TCU assim deliberou:

Nos termos do art. 123 da Lei de Diretrizes Orçamentárias (LDO) 2018, encaminhar à Comissão Mista do Congresso Nacional, a

que se refere o § 1º do art. 166 da Constituição Federal, quadro-resumo relativo à qualidade da implementação e ao alcance de metas e objetivos dos programas e ações governamentais objetos de auditorias operacionais realizadas para subsidiar a discussão do Projeto de Lei Orçamentária Anual;

Fixar prazo de 60 (sessenta) dias para que a Casa Civil da Presidência da República, o Ministério do Planejamento, Desenvolvimento e Gestão e o Ministério da Fazenda, com o apoio dos demais ministérios, se manifestem acerca das ações já empreendidas para melhorias no arcabouço de planejamento e orçamento e na capacidade de articulação, monitoramento e avaliação da coerência do conjunto de programas e ações governamentais, de forma a sanar as ocorrências apontadas no presente relatório;

Recomendar à Casa Civil da Presidência da República, com fundamento no princípio da eficiência (art. 37 da Constituição Federal) e no art. 3º da Medida Provisória 782/2017, que lhe atribuiu competências relacionadas ao exercício da coordenação e integração, avaliação e monitoramento das ações do Governo, que, em articulação com o Ministério do Planejamento, Desenvolvimento e Gestão e com o Ministério da Fazenda, com apoio dos demais ministérios pertinentes, desenvolva, no prazo de 90 (noventa) dias, plano de ação para sanar falhas e inconsistências identificadas neste relatório, em harmonia com as medidas já empreendidas, a serem informadas conforme o subitem 9.2 deste acórdão e que contemplem os aspectos apontados a seguir, de modo a aprimorar a eficiência e a efetividade de ações, políticas públicas, planos e programas de governo:

(...)

9.3.4. **regulamentação de diretrizes para fortalecimento, avaliação e aprimoramento contínuo da governança das organizações públicas que contemple:** a) institucionalização de processos contínuos de planejamento e gestão estratégica que consignem e revisem sistematicamente objetivos, metas, indicadores e linhas de ação de médio e longo prazo, em coerência com os planos governamentais mais abrangentes, de natureza setorial, regional ou geral; **b) aprimoramento de atividades-chave de governança, como gestão de riscos e processos de monitoramento e avaliação; c) avaliação periódica do nível de maturidade das organizações responsáveis por políticas, programas ou ações de governo; e d) utilização das informações advindas de avaliações na elaboração do projeto de lei orçamentária anual, para minimizar o risco de malversação dos recursos públicos e de não alcance dos resultados esperados;**

9.3.5. **edição de referencial orientativo ou proposta normativa no sentido de que a instituição de políticas públicas para atuação governamental se fundamente em: a) análises de viabilidade, custo-oportunidade e sustentabilidade;** b) avaliação da coerência, das inter-relações e das interdependências entre a nova política proposta e as existentes; c) coerência com os demais instrumentos de planejamento governamental existentes; d) preenchimento de requisitos mínimos, como definição de responsáveis, prazos de vigência, fontes de financiamento, metas e instrumentos de acompanhamento, fiscalização e aferição de resultados;

(...)

9.3.7. **atualização da normatização do Sistema de Controle Interno do Poder Executivo Federal**, de forma a aproximá-lo, no que couber, das normas e padrões internacionais afetos ao tema;

(...)

9.6. encaminhar cópia desta deliberação ao Presidente do Congresso Nacional, à Comissão Mista de Planos, Orçamentos Públicos e Fiscalização do Senado Federal e da Câmara dos Deputados, à Casa Civil da Presidência da República, à Secretaria de Governo da Presidência da República, ao Ministério do Planejamento, Desenvolvimento e Gestão, ao Ministério da Transparência e Controladoria-Geral da União e ao Ministério da Fazenda.

(grifo nosso)

ANEXO VIII

INSTRUÇÃO NORMATIVA CONJUNTA MP/CGU Nº 01/2016

INSTRUÇÃO NORMATIVA CONJUNTA MP/CGU Nº 01 de 2016

Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

O MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO e a CONTROLADORIA-GERAL DA UNIÃO, no uso das atribuições que lhes conferem respectivamente, o inciso X do art. 1º do Anexo I do Decreto no 8.578, de 26 de novembro de 2015, e o § 2º do art. 1º do Anexo I do Decreto no 8.109, de 17 de setembro de 2013, resolvem:

Art. 1º Os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Seção I
Dos Conceitos

Art. 2º Para fins desta Instrução Normativa, considera-se:

I – *accountability*: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

II – apetite a risco: nível de risco que uma organização está disposta a aceitar;

III – auditoria interna: atividade independente e objetiva de avaliação e de consultoria,

desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança. As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos). Compete às auditorias internas oferecer avaliações e assessoramento às organizações públicas, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes e eficazes mitiguem os principais riscos de que os órgãos e entidades não alcancem seus objetivos;

IV – componentes dos controles internos da gestão: são o ambiente de controle interno da entidade, a avaliação de risco, as atividades de controles internos, a informação e comunicação e o monitoramento;

V – 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 pelo 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:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;

b) cumprimento das obrigações de *accountability*;

c) cumprimento das leis e regulamentos aplicáveis; e

d) 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;

VI – fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

VII – gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;

VIII – governança: combinação de processos e estruturas implantadas pela alta administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos;

IX – governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

X – incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros;

XI – mensuração de risco: significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência;

XII – Política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;

XIII – risco: 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;

XIV – 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;

XV – risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco; e

XVI – Sistema de Controle Interno do Poder Executivo federal: compreende as atividades de avaliação do cumprimento das metas previstas no plano plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização, e tendo como órgão central a Controladoria Geral da União. Não se confunde com os controles internos da gestão, de responsabilidade de cada órgão e entidade do Poder Executivo federal.

CAPÍTULO II
DOS CONTROLES INTERNOS DA GESTÃO

Art. 3º Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público. Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos. Esses controles são operados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder

Executivo federal. A definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos das organizações públicas. Assim, tendo em vista os objetivos estabelecidos pelos órgãos e entidades da administração pública, e os riscos decorrentes de eventos internos ou externos que possam obstaculizar o alcance desses objetivos, devem ser posicionados os controles internos mais adequados para mitigar a probabilidade de ocorrência dos riscos, ou o seu impacto sobre os objetivos organizacionais.

§ 1º Os controles internos da gestão, independentemente do porte da organização, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações realizadas.

§ 2º Os controles internos da gestão baseiam-se no gerenciamento de riscos e integram o processo de gestão.

§ 3º Os componentes dos controles internos da gestão e do gerenciamento de riscos aplicam-se a todos os níveis, unidades e dependências do órgão ou da entidade pública.

§ 4º Os dirigentes máximos dos órgãos e entidades devem assegurar que procedimentos efetivos de implementação de controles internos da gestão façam parte de suas práticas de gerenciamento de riscos.

§ 5º Controles internos da gestão adequados devem considerar todos os componentes definidos na Seção III e devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, complexidade, estrutura e missão do órgão ou da entidade pública.

Art. 4º Os controles internos da gestão devem integrar as atividades, planos, ações, políticas, sistemas, recursos e esforços de todos que trabalhem na organização, sendo projetados para fornecer segurança razoável de que a organização atingirá seus objetivos e missão.

Art. 5º Os controles internos da gestão não devem ser implementados de forma circunstancial, mas como uma série de ações que permeiam as atividades da organização. Essas ações se dão em todas as operações da organização de modo contínuo, inerentes à maneira pela qual o gestor administra a organização.

Art. 6º Além dos controles internos da gestão, os órgãos e entidades do Poder Executivo federal podem estabelecer instâncias de segunda linha (ou camada) de defesa, para supervisão e monitoramento desses controles internos. Assim, comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance, por exemplo, podem se constituir em instâncias de supervisão de controles internos.

Art. 7º Os controles internos da gestão tratados neste capítulo não devem ser confundidos com as atividades do Sistema de Controle Interno relacionadas no artigo 74 da Constituição federal de 1988, nem com

as atribuições da auditoria interna, cuja finalidade específica é a medição e avaliação da eficácia e eficiência dos controles internos da gestão da organização.

Seção I
Dos Princípios

Art. 8º Os controles internos da gestão do órgão ou entidade devem ser desenhados e implementados em consonância com os seguintes princípios:

I – aderência à integridade e a valores éticos;

II – competência da alta administração em exercer a supervisão do desenvolvimento e do desempenho dos controles internos da gestão;

III – coerência e harmonização da estrutura de competências e reponsabilidades dos diversos níveis de gestão do órgão ou entidade;

IV – compromisso da alta administração em atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos da organização;

V – clara definição dos responsáveis pelos diversos controles internos da gestão no âmbito da organização;

VI – clara definição de objetivos que possibilitem o eficaz gerenciamento de riscos;

VII – mapeamento das vulnerabilidades que impactam os objetivos, de forma que sejam adequadamente identificados os riscos a serem geridos;

VIII – identificação e avaliação das mudanças internas e externas ao órgão ou entidade que possam afetar significativamente os controles internos da gestão;

IX – desenvolvimento e implementação de atividades de controle que contribuam para a obtenção de níveis aceitáveis de riscos;

X – adequado suporte de tecnologia da informação para apoiar a implementação dos controles internos da gestão;

XI – definição de políticas e normas que suportem as atividades de controles internos da gestão;

XII – utilização de informações relevantes e de qualidade para apoiar o funcionamento dos controles internos da gestão;

XIII – disseminação de informações necessárias ao fortalecimento da cultura e da valorização dos controles internos da gestão;

XIV– realização de avaliações periódicas para verificar a eficácia do funcionamento dos controles internos da gestão; e

XV – comunicação do resultado da avaliação dos controles internos da gestão aos responsáveis pela adoção de ações corretivas, incluindo a alta administração.

Seção II
Dos Objetivos dos Controles Internos da Gestão

Art. 9º Os controles internos da gestão devem ser estruturados para oferecer segurança razoável de que os objetivos da organização serão alcançados. A existência de objetivos claros é pré-requisito para a eficácia do funcionamento dos controles internos da gestão.

Art. 10. Os objetivos dos controles internos da gestão são:

I – dar suporte à missão, à continuidade e à sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos do órgão ou entidade;

II – proporcionar a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica das operações;

III – assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisões, ao cumprimento de obrigações de transparência e à prestação de contas;

IV – assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria organização; e

V – salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

§ 1º Ética se refere aos princípios morais, sendo pré-requisito e suporte para a confiança pública.

§ 2º As operações de um órgão ou entidade serão econômicas quando a aquisição dos insumos necessários se der na quantidade e qualidade adequadas, forem entregues no lugar certo e no momento preciso, ao custo mais baixo.

§ 3º As operações de um órgão ou entidade serão eficientes quando consumirem o mínimo de recursos para alcançar uma dada quantidade e qualidade de resultados, ou alcançarem o máximo de resultado com uma dada qualidade e quantidade de recursos empregados.

§ 4º As operações de um órgão ou entidade serão eficazes quando cumprirem objetivos imediatos, traduzidos em metas de produção ou de atendimento, de acordo com o estabelecido no planejamento das ações.

§ 5º As operações de um órgão ou entidade serão efetivas quando alcançarem os resultados pretendidos a médio e longo prazo, produzindo impacto positivo e resultando no cumprimento dos objetivos das organizações.

Seção III
Da Estrutura dos Controles Internos da Gestão

Art. 11. Na implementação dos controles internos da gestão, a alta administração, bem como os servidores da organização, deverá

observar os componentes da estrutura de controles internos, a seguir descritos:

I - ambiente de controle: é a base de todos os controles internos da gestão, sendo formado pelo conjunto de regras e estrutura que determinam a qualidade dos controles internos da gestão. O ambiente de controle deve influenciar a forma pela qual se estabelecem as estratégias e os objetivos e na maneira como os procedimentos de controle interno são estruturados. Alguns dos elementos do ambiente de controle são:

a) integridade pessoal e profissional e valores éticos assumidos pela direção e pelo quadro de servidores, incluindo inequívoca atitude de apoio à manutenção de adequados controles internos da gestão, durante todo o tempo e por toda a organização;

b) comprometimento para reunir, desenvolver e manter colaboradores competentes;

c) filosofia da direção e estilo gerencial, com clara assunção da responsabilidade de supervisionar os controles internos da gestão;

d) estrutura organizacional na qual estejam claramente atribuídas responsabilidades e delegação de autoridade, para que sejam alcançados os objetivos da organização ou das políticas públicas; e

e) políticas e práticas de recursos humanos, especialmente a avaliação do desempenho e prestação de contas dos colaboradores pelas suas responsabilidades pelos controles internos da gestão da organização ou política pública;

II – avaliação de risco: é o processo permanente de identificação e análise dos riscos relevantes que impactam o alcance dos objetivos da organização e determina a resposta apropriada ao risco. Envolve identificação, avaliação e resposta aos riscos, devendo ser um processo permanente;

III – atividades de controles internos: são atividades materiais e formais, como políticas, procedimentos, técnicas e ferramentas, implementadas pela gestão para diminuir os riscos e assegurar o alcance de objetivos organizacionais e de políticas públicas. Essas atividades podem ser preventivas (reduzem a ocorrência de eventos de risco) ou detectivas (possibilitam a identificação da ocorrência dos eventos de risco), implementadas de forma manual ou automatizada. As atividades de controles internos devem ser apropriadas, funcionar consistentemente de acordo com um plano de longo prazo, ter custo adequado, ser abrangentes, razoáveis e diretamente relacionadas aos objetivos de controle. São exemplos de atividades de controles internos:

a) procedimentos de autorização e aprovação;

b) segregação de funções (autorização, execução, registro, controle);

c) controles de acesso a recursos e registros;

d) verificações;

e) conciliações;

f) avaliação de desempenho operacional;

g) avaliação das operações, dos processos e das atividades; e

h) supervisão;

IV - informação e comunicação: as informações produzidas pelo órgão ou entidade devem ser apropriadas, tempestivas, atuais, precisas e acessíveis, devendo ser identificadas, armazenadas e comunicadas de forma que, em determinado prazo, permitam que os funcionários e servidores cumpram suas responsabilidades, inclusive a de execução dos procedimentos de controle interno. A comunicação eficaz deve fluir para baixo, para cima e através da organização, por todos seus componentes e pela estrutura inteira. Todos os servidores/funcionários devem receber mensagem clara da alta administração sobre as responsabilidades de cada agente no que concerne aos controles internos da gestão. A organização deve comunicar as informações necessárias ao alcance dos seus objetivos para todas as partes interessadas, independentemente no nível hierárquico em que se encontram;

V – monitoramento: é obtido por meio de revisões específicas ou monitoramento contínuo, independente ou não, realizados sobre todos os demais componentes de controles internos, com o fim de aferir sua eficácia, eficiência, efetividade, economicidade, excelência ou execução na implementação dos seus componentes e corrigir tempestivamente as deficiências dos controles internos:

a) monitoramento contínuo: é realizado nas operações normais e de natureza contínua da organização. Inclui a administração e as atividades de supervisão e outras ações que os servidores executam ao cumprir suas responsabilidades. Abrange cada um dos componentes da estrutura do controle interno, fortalecendo os controles internos da gestão contra ações irregulares, antiéticas, antieconômicas, ineficientes e ineficazes. Pode ser realizado pela própria Administração por intermédio de instâncias de conformidade, como comitês específicos, que atuam como segunda linha (ou camada) de defesa da organização; e

b) avaliações específicas: são realizadas com base em métodos e procedimentos predefinidos, cuja abran-

gência e frequência dependerão da avaliação de risco e da eficácia dos procedimentos de monitoramento contínuo. Abrangem, também, a avaliação realizada pelas unidades de auditoria interna dos órgãos e entidades e pelos órgãos do Sistema de Controle Interno (SCI) do Poder Executivo federal para aferição da eficácia dos controles internos da gestão quanto ao alcance dos resultados desejados.

Parágrafo único. Os componentes de controles internos da gestão definem o enfoque recomendável para a estrutura de controles internos nos órgãos e entidades do setor público e fornecem bases para sua avaliação. Esses componentes se aplicam a todos os aspectos operacionais de cada organização.

Seção IV
Das Responsabilidades

Art. 12. A responsabilidade por estabelecer, manter, monitorar e aperfeiçoar os controles internos da gestão é da alta administração da organização, sem prejuízo das responsabilidades dos gestores dos processos organizacionais e de programas de governos nos seus respectivos âmbitos de atuação.

Parágrafo único. Cabe aos demais funcionários e servidores a responsabilidade pela operacionalização dos controles internos da gestão e pela identificação e comunicação de deficiências às instâncias superiores.

CAPÍTULO III
DA GESTÃO DE RISCOS

Art. 13. Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas nesta Instrução Normativa.

Seção I
Dos Princípios da Gestão de Riscos

Art. 14. A gestão de riscos do órgão ou entidade observará os seguintes princípios:

I – gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;

II – estabelecimento de níveis de exposição a riscos adequados;

III – estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;

IV – utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico; e

V – utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

Seção II
Dos Objetivos da Gestão de Riscos

Art. 15. São objetivos da gestão de riscos:

I – assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;

II – aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis; e

III – agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

Seção III
Da Estrutura do Modelo de Gestão de Riscos

Art. 16. Na implementação e atualização do modelo de gestão de riscos, a alta administração, bem como seus servidores ou funcionários, deverá observar os seguintes componentes da estrutura de gestão de riscos:

I – ambiente interno: inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional e políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos;

II– fixação de objetivos: todos os níveis da organização (departamentos, divisões, processos e atividades) devem ter objetivos fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução;

III – identificação de eventos: devem ser identificados e relacionados os riscos inerentes à própria atividade da organização, em seus diversos níveis;

IV – avaliação de riscos: os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas. Os riscos devem ser avaliados quando à sua condição de inerentes e residuais;

V – resposta a riscos: o órgão/entidade deve identificar qual estratégia seguir (evitar, transferir, aceitar ou tratar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco;

VI – atividades de controles internos: são as políticas e os procedimentos estabelecidos e executados para mitigar os riscos que a organização tenha optado por tratar. Também denominadas de procedimentos de controle, devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão preventivos e detectivos, bem como a preparação prévia de planos de contingência e resposta à materialização dos riscos;

VII – informação e comunicação: informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos; e

VIII – monitoramento: tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.

Parágrafo Único. Os gestores são os responsáveis pela avaliação dos riscos no âmbito das unidades, processos e atividades que lhes são afetos. A alta administração deve avaliar os riscos no âmbito da organização, desenvolvendo uma visão de riscos de forma consolidada.

Seção IV
Da Política de Gestão de Riscos

Art. 17. A política de gestão de riscos, a ser instituída pelos órgãos e entidades do Poder Executivo federal em até doze meses a contar da publicação desta Instrução Normativa, deve especificar ao menos:

I – princípios e objetivos organizacionais;

II – diretrizes sobre:

a) como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização;

b) como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos;

c) como será medido o desempenho da gestão de riscos;

d) como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos;

e) a utilização de metodologia e ferramentas para o apoio à gestão de riscos; e

f) o desenvolvimento contínuo dos agentes públicos em gestão de riscos; e

III – competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade.

Art. 18. Os órgãos e entidades, ao efetuarem o mapeamento e avaliação dos riscos, deverão considerar, entre outras possíveis, as seguintes tipologias de riscos:

a) riscos operacionais: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

b) riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;

c) riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade; e

d) riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Seção V
Das Responsabilidades

Art. 19. O dirigente máximo da organização é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão.

Art. 20. Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado.

§ 1º O agente responsável pelo gerenciamento de determinado risco deve ser o gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

§ 2º São responsabilidades do gestor de risco:

I – assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da organização;

II – monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas

resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e

III – garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização.

CAPÍTULO IV
DA GOVERNANÇA

Seção I
Dos Princípios

Art. 21. São princípios da boa governança, devendo ser seguidos pelos órgãos e entidades do Poder Executivo federal:

I – liderança: deve ser desenvolvida em todos os níveis da administração. As competências e responsabilidades devem estar identificadas para todos os que gerem recursos públicos, de forma a se obter resultados adequados;

II – integridade: tem como base a honestidade e objetividade, elevando os padrões de decência e probidade na gestão dos recursos públicos e das atividades da organização, com reflexo tanto nos processos de tomada de decisão, quanto na qualidade de seus relatórios financeiros e de desempenho;

III – responsabilidade: diz respeito ao zelo que se espera dos agentes de governança na definição de estratégias e na execução de ações para a aplicação de recursos públicos, com vistas ao melhor atendimento dos interesses da sociedade;

IV – compromisso: dever de todo o agente público de se vincular, assumir, agir ou decidir pautado em valores éticos que norteiam a relação com os envolvidos na prestação de serviços à sociedade, prática indispensável à implementação da governança;

V – transparência: caracterizada pela possibilidade de acesso a todas as informações relativas à organização pública, sendo um dos requisitos de controle do Estado pela sociedade civil. As informações devem ser completas, precisas e claras para a adequada tomada de decisão das partes interessas na gestão das atividades; e

VI – *Accountability*: obrigação dos agentes ou organizações que gerenciam recursos públicos de assumir responsabilidades por suas decisões e pela prestação de contas de sua atuação de forma voluntária, assumindo integralmente a consequência de seus atos e omissões.

§ 1º Para uma efetiva governança, os princípios devem ser aplicados de forma integrada, como um processo, e não apenas individualmente, sendo compreendidos por todos na organização.

§ 2º Os agentes da governança institucional de órgãos e entidades, por subsunção a tais princípios, devem contribuir para aumentar a confiança na forma como são geridos os recursos colocados à sua disposição, reduzindo a incerteza dos membros da sociedade sobre a forma como são geridos os recursos e as organizações públicas.

CAPÍTULO V
DO COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES

Art. 22. Riscos e controles internos devem ser geridos de forma integrada, objetivando o estabelecimento de um ambiente de controle e gestão de riscos que respeite os valores, interesses e expectativas da organização e dos agentes que a compõem e, também, o de todas as partes interessadas, tendo o cidadão e a sociedade como principais vetores.

Art. 23. Os órgãos e entidades do Poder Executivo federal deverão instituir, pelos seus dirigentes máximos, Comitê de Governança, Riscos e Controles.

§ 1º No âmbito de cada órgão ou entidade, o Comitê deverá ser composto pelo dirigente máximo e pelos dirigentes das unidades a ele diretamente subordinadas e será apoiado pelo respectivo Assessor Especial de Controle Interno.

§ 2º São competências do Comitê de Governança, Riscos e Controles:

I – promover práticas e princípios de conduta e padrões de comportamentos;

II – institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;

III – promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;

IV – garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;

V – promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;

VI – promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;

VII – aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;

VIII – supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;

IX – liderar e supervisionar a institucionalização da gestão de riscos e dos controles inter-

nos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade;

X – estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada ao nível de unidade, política pública, ou atividade;

XI – aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;

XII – emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos; e

XIII – monitorar as recomendações e orientações deliberadas pelo Comitê.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 24. A Controladoria-Geral da União, no cumprimento de suas atribuições institucionais, poderá:

I – avaliar a política de gestão de riscos dos órgãos e entidades do Poder Executivo federal;

II – avaliar se os procedimentos de gestão de riscos estão de acordo com a política de gestão de riscos; e

III – avaliar a eficácia dos controles internos da gestão implementados pelos órgãos e entidades para mitigar os riscos, bem como outras respostas aos riscos avaliados.

Art. 25. Esta Instrução Normativa Conjunta entra em vigor na data de sua publicação.

VALDIR MOYSÉS SIMÃO
Ministro do Planejamento, Orçamento e Gestão

LUIZ AUGUSTO FRAGA NAVARRO DE BRITTO FILHO
Ministro Chefe da Controladoria-Geral da União

ANEXO IX

Glossário

***Accountability* pública** – obrigação que têm as pessoas, físicas ou jurídicas, públicas ou privadas, às quais se tenha confiado recursos públicos, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a sociedade e a quem lhes delegou essas responsabilidades sobre o cumprimento de objetivos e metas e o desempenho alcançado na gestão dos recursos públicos. É, ainda, obrigação imposta a uma pessoa ou entidade auditada de demonstrar que administrou ou controlou os recursos que lhe foram confiados em conformidade com os termos segundo os quais eles lhe foram entregues (TCU, 2011). Ver também Responsabilização.

Aceitar risco – ver Resposta a risco.

Alta administração – gestores que integram o nível executivo mais elevado da organização com poderes para estabelecer as políticas, os objetivos e conduzir a implementação da estratégia para realizar os objetivos da organização.

Análise de riscos – processo de compreender a natureza e determinar o nível (magnitude, severidade) de um risco ou combinação de riscos, mediante a combinação das consequências e de suas probabilidades (ABNT, 2009).

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).

Arranjos de contingência – acordos que estabelecem como as partes devem proceder caso um ou mais riscos se concretizem.

Atividade – termo genérico utilizado para expressar operações, ações ou transações que uma organização, pessoa ou entidade realiza com vistas ao alcance de objetivos determinados, refletindo os fluxos de trabalho cotidianos que formam os processos de trabalho (TCU, 2012).

Atividades de controle – ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração

para mitigar os riscos à realização dos objetivos (COSO, 2013).

Avaliação de riscos – processo de comparar os resultados da análise de riscos com os critérios de risco da organização, para determinar se um risco e/ou sua magnitude é aceitável ou tolerável (ABNT, 2009).

Consequência – resultado de um evento que afeta positiva ou negativamente os objetivos da organização.

Controles internos – ver Atividades de controle.

Critérios de auditoria – referências usadas para mensurar ou avaliar o objeto de auditoria (ISSAI 100; ISA/NBCTA Estrutura Conceitual para trabalhos de asseguração). O referencial que indica o estado requerido ou desejado ou a expectativa em relação ao objeto de auditoria. Reflete como deveria ser a gestão, provendo o contexto para compreensão dos achados de auditoria e para a avaliação das evidências de auditoria (BRASIL, 2011).

Estrutura de gestão de riscos – conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização (ABNT, 2009).

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).

Evitar risco – ver Resposta a risco.

Fonte de risco – elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco (ABNT, 2009).

Gerenciamento de riscos - aplicação de uma arquitetura (princípios, estrutura e processo) para identificar riscos, analisar e avaliar se devem ser modificados por algum tratamento a fim de atender critérios de risco. Ao longo desse processo, comunica-se e consulta-se as partes interessadas, monitora-se e analisa-se criticamente os riscos e os controles que os modificam, a fim de assegurar que nenhum tratamento de risco adicional é requerido (ABNT, 2009).

Gerenciamento de riscos corporativos – processo efetuado pelo conselho de administração, gestores e outras pessoas, aplicado na definição da estratégia e através de toda a entidade, estruturado para identificar potenciais eventos que possam afetar a entidade e gerenciá-los para mantê-los dentro de seu ape-

tite a risco, de modo a fornecer uma garantia razoável quanto à realização dos objetivos da entidade (COSO GRC, 2004; INTOSAI, 2007).

Gestão – estruturas responsáveis pelo planejamento, execução, controle, ação, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a consecução de seus objetivos, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas (TCU, 2014).

Gestão de riscos – atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco (ABNT, 2009).

Gestor – pessoa que ocupa função de gestão em qualquer nível hierárquico da organização.

Governança – conjunto de políticas e processos que moldam a maneira como uma organização é dirigida, administrada, controlada e presta contas do cumprimento das suas obrigações de *accountability*. No setor público, a governança compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (BRASIL, 2014).

Identificação de riscos – processo de busca, reconhecimento e descrição de riscos; envolve a identificação das fontes de risco, os eventos, suas causas e suas consequências potenciais (ABNT, 2009), pode envolver análise de dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas.

Indicadores-chave 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-chave da organização, com o objetivo de comparar esta medida com metas preestabelecidas (TCU, 2010d, adaptado).

Indicadores-chave 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-chave da organização (TCU, 2010d, adaptado).

Macroprocessos – processos mais abrangentes da organização. Representam conjuntos de atividades agregadas, em nível de abstração amplo, que formam a cadeia de valor de uma organização, explicitando como ela opera para cumprir sua missão e atender as necessidades de suas partes interessadas (BRASIL, 2011). Ver também Processo.

Mapa de processo - representação gráfica da sequência de atividades que compõem um processo, fornecendo uma visão dos fluxos operacionais do trabalho, incluindo, a depender do nível de análise que se deseja

realizar, a evidenciação dos agentes envolvidos, os prazos, o fluxo de documentos, o processo decisório (BRASIL, 2003).

Matriz de avaliação de riscos – papel de trabalho que estrutura e sistematiza a identificação de riscos, a análise de riscos e a avaliação de riscos, incluindo a avaliação de controles internos e outras respostas a riscos, podendo incluir as decisões sobre o tratamento de riscos.

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

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

Mitigar risco – ver Resposta a risco.

Monitoramento – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças em relação ao 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).

Objetivos-chave – os macro-objetivos, macroprodutos ou resultados finalísticos que geram, preservam e entregam valor público em benefício do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos (SERRA, 2008).

Obrigações de *accountability* – ver *Accountability* pública.

Órgão de governança – conselho de administração, diretoria colegiada ou órgãos com responsabilidade de supervisão geral da direção estratégica de entidades e das responsabilidades relacionadas às obrigações de *accountability*.

Parceria - arranjo estabelecido a fim de possibilitar um relacionamento colaborativo entre as partes (denominadas parceiras) visando o alcance de objetivos específicos previamente acordados entre eles.

Parte interessada (*stakeholder*) – pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade da organização (ABNT, 2009).

Plano de gestão de riscos – esquema dentro da estrutura de gestão de riscos que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos, incluindo, tipicamente, procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades (ABNT, 2009).

Um manual ou complemento à política de gestão de riscos que pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização (ABNT, 2009, adaptado).

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).

Processo – conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos/serviços (saídas) com valor agregado. Processos são geralmente planejados e realizados de maneira contínua para agregar valor na geração de produtos e serviços. Processos podem ser agrupados em macroprocessos e subdivididos em subprocessos (BRASIL, 2011).

Processo de avaliação de riscos – processo global representado pelo conjunto de métodos e técnicas que possibilitam a identificação de riscos, a análise de riscos e a avaliação de riscos que possam impactar os objetivos de organizações, programas, projetos e atividades. Envolve a identificação das fontes de risco, dos eventos e de sua probabilidade de ocorrência, de suas causas e suas consequências potenciais, das áreas de impacto, das circunstâncias envolvidas, inclusive aquelas relativas a cenários alternativos (ABNT, 2009, adaptado).

Processo de gestão de riscos – aplicação sistemática de políticas, procedimentos e práticas de gestão em atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica de riscos (ABNT, 2009). Sinônimo de gerenciamento de riscos.

Processos de governança – os processos que integram os mecanismos de liderança, estratégia e controle e que permitem aos responsáveis pela governança a avaliar, direcionar e monitorar a atuação da gestão (BRASIL, 2014).

Responsabilização (*accountability*) – responsabilidade de uma organização ou indivíduo sobre suas decisões e atividades e prestação de contas a seus órgãos de governança, autoridades legais e, de modo mais amplo, às demais partes interessadas no que se refere a essas decisões e atividades (ABNT, 2010). Ver também *Accountability* pública.

Responsáveis pela governança – pessoas ou organizações com responsabilidade de supervisão geral da direção estratégica da entidade e das obrigações de *accountability* da organização (ISSAI 1003).

Respostas a risco – opções 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 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); possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades (BRASIL, 2010c); efeito da incerteza nos objetivos (ABNT, 2009).

Risco de controle – possibilidade de que os controles adotados pela administração não sejam eficazes para tratar o risco a que se propõe.

Risco de oportunidade – risco associado a aproveitar oportunidades que podem gerar benefícios à organização.

Risco estratégico – risco de longo prazo ou risco de oportunidade relacionado aos objetivos estratégicos e às estratégias adotadas para alcançá-los.

Risco inerente – o risco intrínseco à natureza do negócio, do processo ou da atividade, independentemente dos controles adotados.

Risco operacional – risco de perdas resultantes direta ou indiretamente de falha ou inadequação de processos internos, pessoas e sistemas ou de eventos externos.

Risco residual – o risco retido de forma consciente ou não pela administração, que remanesce mesmo após o tratamento de riscos.

Risco significativo – aquele com grande probabilidade de ocorrer e, se ocorrer, ter um impacto relevante nos objetivos (LONGO, 2011).

Riscos-chave – riscos estratégicos e riscos operacionais relevantes para o negócio, relacionados aos objetivos-chave da organização.

Transferir risco – Ver Repostas a riscos.

Tratamento de riscos – processo de implementar respostas a risco selecionadas. Ver Repostas a riscos.

Valor público – produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização pública que representem respostas efetivas e úteis às necessidades ou demandas de interesse público e modifiquem certos aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos (SERRA, 2008).

Responsabilidade pelo Conteúdo

- Coordenação-Geral de Controle Externo de Resultado de Políticas e Programas Públicos (Coger)
- Secretaria de Métodos e Suporte ao Controle Externo (Semec)
- Secretaria de Planejamento, Governança e Gestão (Seplan)

Responsabilidade Editorial

- Secretaria-Geral da Presidência (Segepres)
- Secretaria de Comunicação (Secom)
- Núcleo de Criação e Editoração (NCE)

Projeto Gráfico, Diagramação e Capa

- Núcleo de Criação e Editoração (NCE)

Fotos

- Istock

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Métodos e Suporte ao Controle Externo (Semec)
SAFS Qd 4 Lote 1 - Anexo III - sala 419
CEP: 70.042-900 - Brasília – DF
Tel: (61) 3316-7902
semec@tcu.gov.br

Impresso pela Sesap/Segedam

Missão

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

Visão

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.

Objetivo estratégico relacionado

Induzir o aperfeiçoamento da gestão de riscos e controles internos da Administração Pública.