Plafor

Planejamento e Gestão Orçamentária e Financeira

Introdução à Gestão de Riscos

Robercy Alves da Silva

PlaforEDU
MINISTÉRIO DA EDUCAÇÃO
PÁTRIA AMADA BRASIL GOVERNO FEDERAL

PRESIDÊNCIA DA REPÚBLICA FEDERATIVA DO BRASIL

MINISTÉRIO DA EDUCAÇÃO

SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

Ministério da Educação

Secretaria de Educação Profissional e Tecnológica (SETEC)

Endereço: Esplanada dos Ministérios, Bl. "L" - 4º Andar, Brasília - DF - 70047-900

Telefone: (61) 2022-8618 Site: http://portal.mec.gov.br

Ministro da Educação

Milton Ribeiro

Secretário da Setec

Tomás Dias Sant´Ana

Diretor de Desenvolvimento da Rede Federal de Educação Profissional, Científica e Tecnológica

Kedson Raul de Souza Lima

Coordenação- Geral de Desenvolvimento de Pessoas da Rede Federal de Educação Profissional, Científica e Tecnológica

Silvilene Souza da Silva

Coordenação do GT PlaforEdu

Patrícia Maia

Coordenador do PlaforEdu

Fábio Ribeiro

Equipe Técnica do Curso

Professor-Autor

Robercy Alves da Silva

Coordenação Pedagógica

Marcos Antônio de Oliveira

Administrativo

Allen Gardel Dantas de Luna

Design Instrucional

Fabiane Beletti da Silva

Design Gráfico

Carol Costa

Eduarda Moreira

Diagramação

Eduarda Moreira

Revisão Linguística

Wagner Ramos Campos

Produção Audiovisual

Madeline Jales

Glácio Gley Menezes de Souza

Laurence Campos

Rodolfo da Silva Costa

Produzido pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN).

Sumário

Palavra do Professor

Caro(a) aluno(a), aqui você vai conhecer um pouco mais do universo da gestão de riscos. Seja bem-vindo(a) à disciplina de Introdução à Gestão de Riscos!

Na primeira seção, você fará uma viagem no tempo para conhecer a origem e a história da gestão de riscos. Conhecer as principais motivações que a trouxeram para o meio organizacional, e seus principais conceitos teóricos e normativos.

Na segunda seção, devido a sua importância, você vai conhecer o COSO ERM, um comitê que definiu gerenciamento de riscos corporativos como um processo que deve ser conduzido por todos os agentes da administração.

Na terceira seção, você também conhecerá as principais normas ISO relacionadas com a gestão de risco, e que serão as principais balizas neste mundo da gestão de risco.

Na quarta e última seção, você irá compreender como a gestão de risco pode e deve ser aplicada no setor público.

Assim, esperamos que você aproveite bastante, que consiga compreender a importância da gestão de riscos para o sucesso dos projetos que irá desenvolver no âmbito de sua organização, assim como nos processos e rotinas que desenvolve. Tornando a gestão de risco uma ferramenta obrigatória na sua vida de gestor

Introdução

A incerteza ou o risco é inerente a praticamente todas as atividades humanas. No mundo corporativo onde as empresas e organizações estão constantemente imersas em um cenário de constantes incertezas, sejam elas de fatores econômicos, sociais, legais, tecnológicos e operacionais, a gestão de integridade, riscos e controles internos é de suma importância para a garantia do alcance dos seus objetivos estratégicos.

E deste modo, compete a gestão de riscos a função de assegurar o alcance dos objetivos, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, o cumprimento de prazos, leis e regulamentos etc., implementar estratégias com vistas a evitar o consumo intenso de recursos para solução de problemas inesperados, bem como a melhoria contínua dos processos organizacionais.

No ambiente de trabalho, muitas vezes as organizações se deparam com fatores internos e externos que tornam incerto o êxito do atingimento dos objetivos de um determinado projeto ou de uma atividade que se encontra em desenvolvimento. Independentemente da área, e até mesmo na vida pessoal, os riscos podem afetar o andamento de uma determinada ação, levando-a a uma direção completamente diferente daquela inicialmente planejada.

As responsabilidades do governo em relação ao bem público exigem a adoção de práticas e estratégias eficazes de gestão dos recursos públicos. Neste contexto, a gestão de riscos torna-se uma importante ferramenta para auxiliar na tomada de decisões baseadas em metodologias e normas que geram, dentre outros benefícios, a redução ou a eliminação de retrabalhos e desperdícios.

Motivados pelo que foi descrito, e considerando que a implementação da gestão de riscos no setor público acontece de incipiente, elaboramos esse curso com o objetivo de agregar valor às organizações, por meio da capacitação de gestores, dando a eles ferramentas para materializar o projeto de gestão de riscos em seus próprios órgãos.

Histórico

A gestão de riscos remonta à época em que os primeiros chefes de clãs decidiram fortalecer suas muralhas, realizar alianças com outras tribos ou armazenar provisões para os momentos de incerteza. 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 (HUBBARD, 2009).

Exemplo um pouco mais recente foi a instituição do seguro de incêndio, em meados do século XVII, na Inglaterra (DICKSON, 1960).

O desenvolvimento da teoria da probabilidade, no século XVII, abriu caminho para o uso de métodos quantitativos na gestão de riscos. Entretanto, até meados do século XX, isso estava limitado a setores específicos, como seguros, mercado financeiro e saúde pública (HUBBARD, 2009).

No campo acadêmico, a obra "*Risk, Uncertainty and Profit*", publicada em 1921 por Frank Knight, torna-se referência mundial no campo da gestão de riscos, especialmente por estabelecer conceitos, definir princípios e introduzir alguma sistematização ao tema (FRASER e SIMKINS, 2010).

A gestão de riscos com enfoque corporativo, institucional, constitui área de estudos relativamente nova, iniciando-se somente ao final do século XX. Marco importante foi a publicação do artigo "The Risk

Management Revolution", na revista Fortune, em 1975, o qual sugeria que se estabelecesse a coordenação das várias funções de riscos existentes em uma organização e a aceitação pela alta administração da responsabilidade por instituir políticas e manter supervisão sobre tal função coordenada (FRASER e SIMKINS, 2010).

Somente no ano de 1992 a ideia de gestão de risco corporativo volta a ganhar foco, quando o *Committee of Sponsoring Organizations of the Treadway Commission* – COSO publica o guia *Internal Control - integrated framework* (COSO-IC ou COSO I), com o objetivo de orientar as organizações quanto a princípios e melhores práticas de controle interno, o que inclui práticas de gestão de riscos (COSO, 1992). No mesmo ano, o Comitê Cadbury, do Reino Unido, emite relatório sobre o tema no qual identifica o corpo governante superior da entidade como responsável por definir a política de gestão de riscos, assegurar que a organização entenda todos os riscos aos quais está exposta e supervisionar o processo de gestão de riscos (CADBURY, 1992).

Em 1995, o 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. Normas técnicas assemelhadas logo são publicadas também no Canadá, no Reino Unido e em outros países.

Em 2001, o colapso da empresa Enron revela um esquema gigantesco de manipulação de balanços, ocultação de dívidas, lucros artificialmente inflados e falhas de auditorias. Esse fato influencia a aprovação, em 2002, da chamada Lei Sarbanes-Oxley, que visa assegurar que as empresas que participam do mercado acionário norte-americano possuam estruturas e mecanismos de governança adequados, com vistas a mitigar

riscos, evitar a ocorrência de fraudes e proteger os investidores (USA, 2002).

Em 2004, o COSO publicou o Enterprise Risk Management - integrated framework (COSO-ERM ou COSO II), modelo de referência que estendeu o COSO I, tendo como foco a gestão de riscos corporativos (COSO, 2004). No mesmo ano é firmado o Acordo de Basileia II, aplicável a instituições bancárias em nível mundial, tendo como grande diferencial, em complemento às previsões já existentes no documento firmado em 1988, a inclusão de requisitos específicos relacionados com a gestão de riscos operacionais (BCBS, 2004). Ainda em 2004 é lançada versão atualizada e expandida da norma AS/NZS 4360 (STANDARDS AUSTRALIA, 2004).

Em 2009 é publicada a norma técnica ISO 31.000 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). O modelo preconizado na ISO 31.000 aprimorou os conceitos, as diretrizes e as práticas recomendadas em normas técnicas de aplicação local que a precederam, como a AS/NZS 4360.

Principais Metodologias

Nesta seção encontra-se síntese de alguns dos principais modelos de gestão de riscos:

COSO-IC (COSO I)

Em 1992, o *Committee of Sponsoring Organizations of the Treadway Commission* – COSO publicou o guia *Internal Control - integrated framework* (COSO-IC ou COSO I), com o objetivo de orientar as organizações quanto a princípios e melhores práticas de controle interno,

em especial para assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes.

Nesse modelo, controle interno é definido como um "processo projetado e implementado pelos gestores para mitigar riscos e alcançar objetivos". Por sua vez, risco é definido como "a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos" (COSO, 1992). Ou seja, para o COSO-IC, o controle interno é um processo que tem por objetivo mitigar riscos, com vistas ao alcance dos objetivos.

O modelo do COSO-IC é representado por um cubo no qual as três faces visíveis representam:

i) tipos de objetivos;
ii) níveis da estrutura organizacional e
iii) componentes.

Os tipos de objetivos que o COSO-IC foca são os operacionais do negócio, assegurar relatórios financeiros confiáveis e assegurar conformidade legal/regulatória. A visão relativa à estrutura organizacional busca atingir a organização como um todo, abarcando unidade, departamento, divisão, etc., ou seja, do maior ao menor nível. O modelo concentra-se nos seguintes componentes: ambiente de controle, análise de riscos, atividades de controle, informação e comunicação e monitoração.

Em resumo, as perspectivas mostradas nas três faces do cubo do COSO-IC podem ser entendidas como o conjunto de atividades, recursos e viabilizadores críticos para o processo de controle interno a ser aplicado na instituição em todos os níveis, com vistas a assegurar o alcance de certos tipos de objetivos normalmente existentes nas organizações.

Apesar da avaliação de riscos ser um componente do modelo, todo foco está no processo de controle interno da organização, e não estão contempladas todas as atividades e outros aspectos importantes para a realização de um processo completo de gestão de riscos. Em outras palavras, o COSO-IC, é um modelo de controle interno que utiliza práticas de avaliação de riscos, não tendo sido elaborado com o objetivo de ser um modelo de gestão de riscos em sentido estrito.

O COSO-IC é o framework mais utilizado pelas companhias que possuem ações em bolsa nos Estados Unidos, com vistas ao atendimento da secção 404 da lei norte-americana Sarbanes-Oxley, que trata de assegurar a efetividade dos controles internos sobre relatórios financeiros (USA, 2002). Apesar desse uso especializado, o modelo pode ser aplicado também na avaliação dos controles internos relacionados com as operações, conformidade legal/regulatória e outros objetivos.

Em 2013, uma versão atualizada do COSO-IC foi publicada, na qual destacam-se as seguintes modificações: facilitada a verificação de conformidade com a Lei Sarbanes-Oxley, generalização do objetivo relatórios financeiros para relatórios da gestão em geral e explícita articulação de 17 princípios associados aos componentes do sistema de Controle Interno. A entidade responsável pelo modelo recomenda que as organizações usuárias do COSO-IC passem a utilizar essa nova versão, já que a anterior foi considerada obsoleta a partir de 15 de dezembro 2014.

COSO-ERM (COSO II)

Em 2004, o COSO publicou o Enterprise Risk Management - integrated framework (COSO-ERM ou COSO II), documento que ainda hoje é tido como referência no tema gestão de riscos corporativos.

Esse modelo, como o próprio nome revela, foi projetado com o objetivo de orientar as organizações no estabelecimento de um processo de gestão de riscos corporativos e na aplicação de boas práticas sobre o tema.

Vale lembrar que o COSO-ERM é uma evolução do COSO-IC, ou seja, abrange todo o escopo do modelo anterior e incorpora ferramentas complementares, como se vê na seguinte afirmação: "[o modelo COSO-ERM] não pretende substituir o modelo do controle interno [COSO-IC], mas sim incorporá-lo" (COSO, 2004).

De acordo com o COSO-ERM, a gestão de riscos corporativos é:

> "Processo que permeia toda a organização, colocado em prática pela alta administração da entidade, pelos gestores e demais colaboradores, aplicado no estabelecimento da estratégia e projetado para identificar possíveis eventos que possam afetar a instituição e para gerenciar riscos de modo a mantê-los dentro do seu apetite de risco, com vistas a fornecer segurança razoável quanto ao alcance dos objetivos da entidade "
>
> (COSO, 2004, tradução livre).

Importante observação derivada da definição acima é que o processo corporativo de gestão de riscos previsto no COSO-ERM, além de ser aplicável na realização normal das atividades - operacionais, administrativas e de suporte - deveria ser aplicado também nas atividades de planejamento voltadas à definição da estratégia da organização. Isso fica ainda mais evidente quando se observa que a perspectiva do cubo do COSO-ERM relativa aos objetivos inclui um novo

tipo de objetivo a ser assegurado e que não era listado no COSO-IC, qual seja, a categoria dos objetivos estratégicos.

Na perspectiva do cubo do COSO-ERM que trata dos componentes do modelo, observa-se que a atividade "análise de riscos", anteriormente prevista no COSO-IC, foi substituída e complementada pelas seguintes atividades: identificação de eventos, avaliação de riscos e, por fim, resposta a riscos. Essas atividades devem considerar o apetite de risco e os níveis de tolerância a riscos definidos pela organização:

Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite (COSO, 2004).

Característica marcante do COSO-ERM é a previsão, como parte do modelo, de um componente relacionado com a definição de objetivos.

O COSO-ERM introduz conceitos interessantes como apetite a risco e tolerância a riscos. O primeiro refere-se ao montante de risco que a organização se dispõe a aceitar na criação de valor. O segundo trata do nível de variação aceitável no alcance de um certo objetivo.

Em resumo, verifica-se que o modelo COSO-ERM, ao orientar a aplicação de um processo de gestão de riscos corporativos, incorpora e aprimora o modelo COSO-IC pela inclusão de componentes e elementos adicionais que asseguram a realização de todas as atividades necessárias a tal mister.

Vale lembrar ainda a relação existente entre controle interno, gestão de riscos corporativos e a governança corporativa, como bem definido na versão 2013 do COSO *Internal Control —Integrated Framework*.

ISO 31000:2009

A norma técnica ISO 31000:2009 resultou de esforço da *International Organization for Standardization* (ISO) para criar um padrão internacional para a gestão de riscos corporativos, tendo sido publicada no Brasil sob o nome ABNT NBR ISO 31000:2009 Gestão de riscos – Princípios e diretrizes. Essa norma aprimora os conceitos, as diretrizes e as práticas recomendadas em normas técnicas que a precederam, como a AS/NZS 4360 e tem como objetivo oferecer recomendações para o planejamento, implantação e execução de um processo de gestão de riscos abrangendo toda a organização.

O processo de gestão de riscos preconizado na ISO 31000:2009 não difere muito do que já era previsto em normas técnicas regionais que a antecederam e contempla as seguintes fases ou atividades: estabelecimento do contexto, identificação, análise, avaliação e tratamento de riscos, comunicação e consulta, monitoramento e análise crítica. As maiores novidades da norma são a redefinição do conceito de risco e a explicitação de onze princípios para a gestão de riscos, bem como de cinco atributos para aprimorar a gestão de riscos.

Os princípios da gestão de risco eficaz elencados na ISO 31000:2009 são os seguintes:

i) A gestão de riscos cria e protege valor;
ii) A gestão de riscos é parte integrante de todos os processos organizacionais;
iii) A gestão de riscos é parte da tomada de decisões;
iv) A gestão de riscos aborda explicitamente a incerteza;
v) A gestão de riscos é sistemática, estruturada e oportuna;

vi) A gestão de riscos baseia-se nas melhores informações disponíveis;

vii) A gestão de riscos é feita sob medida;

viii) A gestão de riscos considera fatores humanos e culturais; ix) A gestão de riscos é transparente e inclusiva;

ix) A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças; e

x) A gestão de riscos facilita a melhoria contínua da organização (ABNT, 2009).

Também em 2009, a ISO publicou versão atualizada – e compatível com a ISO 31000 – do guia ISO *Guide 73 - Risk Management Vocabulary*, instrumento importante para a sedimentação de uma linguagem comum e padronizada relativa ao tema.

INTOSAI – Guias GOV 9100 e GOV 9130

A Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) publicou, em 2004, o guia GOV 9100 – *Guidelines for Internal Control Standards for the Public Sector*, com o objetivo de prover um modelo de controle interno no setor público e fornecer uma base contra a qual o controle interno pode ser avaliado, aplicável a todos os aspectos relacionados com o funcionamento de uma organização pública.

Em 2007, a INTOSAI publicou o guia complementar GOV 9130 – *Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management,* com recomendações adicionais ao guia GOV9100. O documento preconiza um modelo para a aplicação da gestão de riscos no setor público e provê uma base contra a qual a gestão de riscos pode ser avaliada.

Esses guias foram baseados, respectivamente, no modelo COSO-IC e COSO-ERM anteriormente citados, com algumas modificações, especialmente adaptações de linguagem e de contexto, de forma a adequar o uso ao setor público.

KING III - King Code of Governance Principles

King III é um modelo de governança corporativa originado na África do Sul e que tem boa aceitação internacional, entre outras razões, por sua elaboração ter contado com a consultoria de Sir Adrian Cadbury, responsável pelo conhecido "Cadbury Report" (CADBURY, 1992). Um dos capítulos do documento que formaliza o modelo trata especificamente da "Governança dos riscos".

A África do Sul exige a aplicação do código de práticas King III em todas as empresas que negociam ações na bolsa de valores de Johannesburg. Entretanto, a conformidade é exigida na forma "apply or explain", ou seja, os dirigentes têm a liberdade de aplicar as recomendações de forma diferente da proposta no modelo, ou aplicar práticas alternativas, sempre no melhor interesse da sua organização. Caso isso ocorra, eles precisam explicar, formalmente, as razões que os levaram a agir de forma diversa da recomendada.

Esse modelo prevê a realização obrigatória de ao menos uma avaliação de riscos por ano na organização, devidamente documentada. Outra característica peculiar do modelo é a explícita incorporação de elementos de governança dos riscos de Tecnologia de Informação no sistema de governança de riscos corporativo: “The risk committee should ensure that IT risks are adequately addressed” (IODSA, 2009).

As Três Linhas de Defesa

O guia Declaração de Posicionamento do IIA *(The Institute of Internal Auditors*): As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles, publicado originalmente em 2012, tem por objetivo prover um modelo simples e efetivo para o esclarecimento dos papéis e responsabilidades essenciais no gerenciamento de riscos e controle.

O IIA constata que as organizações contam com diversos atores desempenhando atividades relacionadas à gestão de riscos, como auditores internos, especialistas em gestão de riscos, executivos de compliance, analistas de qualidade, investigadores de fraude e outros profissionais de riscos e controle. Portanto, 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 riscos e controle da organização, de modo a evitar debates desnecessários sobre as competências e áreas de atuação de cada um.

No modelo das Três linhas de Defesa proposto pelo IAA, o controle da gerência é a primeira linha de defesa no gerenciamento de riscos. As diversas funções de controle de riscos e supervisão de conformidade (área de risco, comitê de risco etc.) estabelecidas pela gerência são a segunda linha de defesa, enquanto a avaliação independente, feita pela auditoria interna, é a terceira linha de defesa (IIA, 2012).

Para o IIA, as três linhas devem existir de alguma forma, separadas e claramente identificadas, em todas as organizações, não importando o tamanho ou a complexidade do negócio, pois isso assegura a efetividade do gerenciamento de riscos.

O modelo ressalta que o alto nível de independência da auditoria interna não está disponível nas outras linhas de defesa, nem mesmo na segunda. Para manter essa independência, não é aconselhável que se atribua à auditoria interna responsabilidades de gestão, como por exemplo, coordenar ou gerenciar o processo de gestão de riscos da organização.

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

O Livro Laranja

O guia *The Orange Book Management of Risk - Principles and Concepts* foi publicado em 2004 pelo HM Treasury, órgão governamental responsável pelo tesouro ou finanças do Reino Unido. Trata-se de versão aprimorada de guia semelhante publicado em 2001, que teve grande aceitação nos órgãos públicos britânicos, os quais iniciavam, à época, a implantação de seus processos de gestão de riscos.

Esse guia provê um modelo de gestão de riscos que pode auxiliar no desenvolvimento de uma política institucional sobre o tema, além de ser aplicável em diversos níveis, desde a organização como um todo, até projetos ou operações.

Entre os aspectos realçados nessa versão do *Orange Book* está a necessidade de comunicação, revisão e melhoria contínua do processo implantado. Também se enfatiza a necessidade de considerar os relacionamentos de interdependência que a organização mantém com

outras instituições ou, nos termos definidos pelo guia, a organização estendida (UK, 2004).

O modelo define que a aceitação de riscos deve considerar critérios definidos pelos administradores, os quais podem ser (UK, 2004):

1. apetite de risco corporativo - montante de risco considerado aceitável, definido pela alta administração e que, na verdade, pode constituir-se de mais de uma declaração, pois constata-se que pode ser definido por categorias;
2. apetite de risco delegado - semelhante ao anterior, mas definido no âmbito das unidades e divisões organizacionais, de acordo com alçadas pré-definidas; e
3. apetite de risco de projeto - semelhante ao primeiro, mas definido para um projeto específico.

Essa estrutura de apetites em cascata permitiria ao gestor aceitar, em certos casos, até mesmo altos riscos, como deixa explícito o exemplo citado no guia de um projeto considerado especulativo, com altos riscos, mas também com possibilidade de altos retornos.

Política de Gestão de Riscos do Governo da Austrália

O governo da Austrália instituiu recentemente um guia geral para a gestão de riscos, denominado *Australian Government Department Commonwealth Risk Management Policy*. Essa política faz parte dos esforços para aprimorar os níveis de accountability dos órgãos e entidades governamentais por meio do foco em seus objetivos, riscos e controles internos (AUSTRALIA, 2014).

O objetivo da política é incorporar a gestão de riscos na cultura das instituições governamentais, de modo que o entendimento compartilhado sobre riscos leve a tomadas de decisão bem-informadas.

Observe-se que essa política não é de aplicação obrigatória, mas existe recomendação para que cada organização governamental revise e alinhe sua estrutura de gestão de riscos com o modelo nela descrito.

O documento, que é baseado na norma técnica ISO 31000/2009, descreve os seguintes nove elementos-chave:

1. instituir uma política de gestão de riscos;
2. estabelecer um framework para a gestão de riscos;
3. definir as responsabilidades pela gestão de riscos;
4. incorporar a gestão de riscos sistemática nos processos de negócio;
5. desenvolver uma cultura de riscos;
6. comunicar e consultar sobre risco;
7. compreender e gerir o risco partilhado;
8. manter a capacidade de gestão de riscos; e
9. rever e melhorar continuamente a gestão de riscos.

Ferma - Padrão de Gestão de Riscos

O Risk Management Standard é um guia publicado pela *Federation of European Risk Management Associations* (Ferma) e resulta do esforço conjunto de diversas entidades europeias que atuam na promoção do uso da gestão de riscos pelas organizações em geral, inclusive do setor público (FERMA, 2003).

As boas práticas de gestão de riscos contidas no guia da Ferma são bastante similares àquelas prescritas por outros modelos, como os seguintes princípios e orientações, por exemplo:

1. a gestão de riscos aumenta as probabilidades de sucesso no alcance dos objetivos;
2. a gestão de riscos deve ser integrada à cultura da organização, com uma política efetiva direcionada pela alta administração;

3. a organização deve estabelecer critérios contra os quais os riscos são comparados;
4. riscos devem ter proprietários;
5. separação clara de responsabilidades entre gestores, funções de apoio à governança e gestão dos riscos e auditoria interna.

ISACA/Cobit 5

O COBIT é um padrão, modelo ou framework para a governança e gestão de Tecnologia da Informação (TI), desenvolvido pela ISACA[1], publicado inicialmente em 1996. A edição atual, o Cobit 5, disponibilizada em 2012, propõe-se a servir como um modelo completo para a governança e a gestão corporativas de TI, em conformidade com as melhores práticas internacionais, com vistas a apoiar a alta direção e demais gestores na definição e no alcance de objetivos de negócio relacionados com TI.

O modelo Cobit 5 identifica 32 processos de trabalho de gestão de TI e 5 processos afetos à governança de TI em sentido estrito. Um dos processos de governança descrito é o "EDM03 – Garantir a otimização do risco", cujos responsáveis primários ou accountables identificados em tabelas RACI são as instâncias internas de governança e a alta direção. Esse processo contempla as atividades de avaliar, direcionar e monitorar a gestão de riscos de TI.

Entre os insumos que se recomenda produzir nesse processo citam-se: guias de apetite a risco, níveis de tolerância a risco, políticas de gestão de risco, processo aprovado para gestão de riscos e ajustes corretivos da gestão de riscos. Adicionalmente, é identificado o processo "APO12 – Gerenciar riscos", tendo como principais responsáveis os dirigentes e gestores da organização, no qual são tratadas as atividades de identificar, analisar, articular e responder aos riscos, bem como manter

portfólio de riscos e portfólio de ações de mitigação correspondentes (ISACA, 2012).

Além de descrever os processos EDM03 e APO12 no guia "Cobit 5 Enabling Processes", a ISACA publicou também o guia "Cobit 5 for Risk", o qual descreve com maior profundidade práticas e métodos para auxiliar no processo de gestão de riscos de TI como um todo e especialmente nas atividades relacionadas com a análise, avaliação e resposta a riscos. Esse guia também destaca a importância de uma perspectiva denominada função de riscos, que envolve a instituição de uma política e uma estrutura organizacional responsável por implantar e fomentar o processo de gestão de riscos de TI.

O guia "Cobit 5 for Risk" sugere a classificação dos riscos em categorias como: entrega de valor ou estratégicos, programas/projetos e operacionais. A metodologia para análise, identificação e tratamento dos riscos parte do levantamento de cenários de risco, que devem ser catalogados num Risk Register ou universo de riscos, juntamente com os demais artefatos gerados. Os cenários são submetidos a análise, na qual se consideram os chamados fatores de riscos (ambiente externo e forças e fraquezas do ambiente interno). Na etapa de análise ponderam-se a probabilidade e as consequências, sendo que, para estas são sugeridos alguns tipos de impactos a considerar, como: não alcance de objetivos estratégicos, financeiros, legais/regulatórios, imagem/reputação e operacionais/produtividade. O guia destaca a importância de existirem critérios definidos pela alta direção (apetite de risco e tolerância a riscos) para subsidiar a decisão quanto à adoção de ações de mitigação.

Na análise de um cenário de risco, o guia "Cobit 5 for Risk" concentra a atenção em elementos denominados habilitadores pelo modelo Cobit5. Habilitadores podem ser entendidos como controles existentes, faltantes ou deficientes e que constituem vulnerabilidades. Também devem ser

considerados os habilitadores ao se avaliar e selecionar ações de mitigação. Os habilitadores considerados no Cobit5 são:

i) Princípios, políticas e modelos;
ii) Processos de trabalho;
iii) Estruturas organizacionais;
iv) Cultura corporativa, ética e comportamento;
v) Informação;
vi) Serviços, infraestrutura e aplicações; e
vii) Pessoas, habilidades e competências.

Embora voltados para a gestão de riscos de TI, subtema especializado da governança, os guias da ISACA demonstram que as atividades de gestão de riscos recomendadas são praticamente as mesmas sugeridas nos demais modelos analisados. Também é reforçada a necessidade de existirem critérios orientadores da gestão de riscos e monitoração da alta direção sobre os resultados alcançados, preferencialmente no escopo de um processo de gestão institucional.

Acordos de Basileia I e II e III

A denominação dos acordos de Basileia deriva da cidade suíça de mesmo nome, a qual sedia o Comitê de Supervisão Bancária de Basileia (BCBS). Essa organização é formada pelas autoridades monetárias de quase 30 países relevantes no cenário econômico mundial, inclusive o Brasil. Os acordos de Basileia constituem uma série de recomendações para assegurar a regulação e a supervisão e buscar maior estabilidade e menor risco nas atividades bancárias. O Comitê não possui autoridade transnacional para fazer valer suas recomendações, portanto os países membros e outros países interessados as

implementam por meio de leis e regulamentações nacionais específicas, o que explica a relativa lentidão para sua completa adoção.

O Acordo de Basileia I, de 1988, era primariamente focado em estabelecer limites à atuação dos bancos com base no chamado risco de crédito, o qual decorre da possibilidade da insolvência de clientes. Com base no risco de crédito total do conjunto de ativos, uma reserva de capital e também um limite de alavancagem são calculados para o banco, limitando assim suas operações e o risco que ele representa para o sistema financeiro (BCBS, 1998).

No Acordo de Basileia II, de 2004, passa-se a considerar no cálculo da reserva de capital não apenas os riscos de crédito, mas também os riscos de mercado e os riscos operacionais. Além disso, o novo acordo aumenta a capacidade de supervisão por parte das autoridades centrais reguladoras e exige maior transparência nos relatórios e publicações destinados ao mercado e ao público em geral (BCBS, 2004).

Os acordos de Basileia têm por alvo o setor bancário, porém certos princípios, regras, mecanismos de controle e metodologias neles definidos podem oferecer insumos para a implantação de um processo de gestão de riscos em organizações que atuam em outras áreas de atividade, inclusive no setor público.

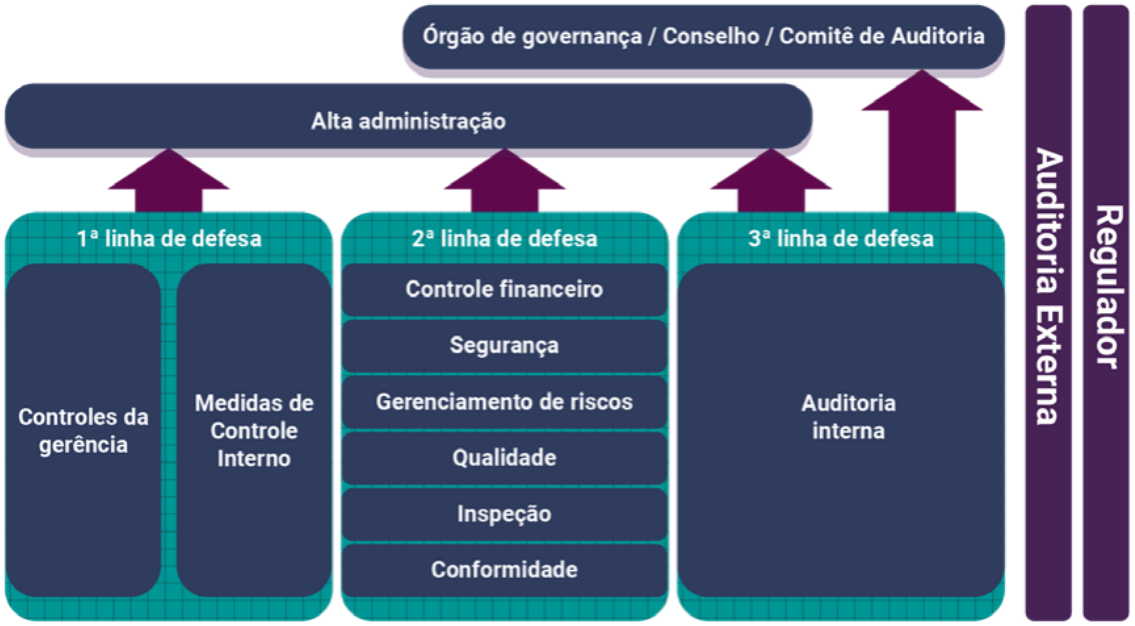
ID	*CARACTERÍSTICAS*	COSO Internal Control - versão 2013	COSO ERM - 2004 + Guias complemen	AS/NZS 4360:2004 + Management Guidelines	ISO 31000:2009 + ISO Guide 73:2009	United Kingdom HM Treasury Orange Book	Australian Government Department Commonwealth	Ferma A Risk Management Standard	IFAC Managing Risk as an Integral Part	KING III Code for Governance Principles	INTOSAI GOV 9130 Guidelines for Internal
	1.1 Considera oportunidades além de riscos	Não.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
2	Necessidade de instituir Política de Gestão de riscos	Não.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
3	Necessidade de serem definidos "critérios" de riscos	Parcialmente.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
4	Declara que o processo de gestão de riscos é customizável	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
5	Encoraja buscar a melhoria contínua da gestão de riscos	Parcialmente.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
6	Prega a necessidade de embutir a gestão de riscos na rotina dos processos de trabalho e na cultura	Não	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
7	Associação de riscos com objetivos	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
	7.1 Aplicável na seleção da estratégia	Não.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Não deixa explícito.	Sim.
8	Recomenda criar e manter um portfólio/registro corporativo de riscos	Não.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Parcialmente.	Sim.	Sim.
9	Alerta sobre necessidade de considerar o custo de tratamento de riscos	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.
10	Orienta para a necessidade de documentar as atividades de gestão de riscos	Parcialmente.	Sim.	Sim.	Sim.	Sim.	Sim.	Parcialmente.	Parcialmente.	Sim.	Sim.
11	Declara que os riscos devem ter "proprietários"	Parcialmente.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Parcialmente.	Parcialmente.
12	Implementar a gestão de riscos não é garantia de total sucesso	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Sim.	Não deixa explícito.	Sim.

As três linhas de defesa

Esse modelo ficou conhecido e foi amplamente difundido a partir da Declaração de Posicionamento do *The Institute of Internal Auditors* (IIA): o modelo de Três Linhas de Defesa no gerenciamento eficaz de riscos e controles é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais. O modelo apresenta um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, e é aplicável a qualquer organização – não importando seu tamanho ou complexidade.

No modelo de Três Linhas de Defesa, o controle da gerência é a primeira linha de defesa no gerenciamento de riscos, as diversas funções

de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa, e a avaliação independente é a terceira. Cada uma dessas três "linhas" desempenha um papel distinto dentro da estrutura mais ampla de governança da organização. A imagem abaixo apresenta a esquematização deste modelo:



Agora detalharemos alguns pontos importantes sobre esse modelo:

• **1ª Linha de Defesa:** Gestão Operacional Como primeira linha de defesa, os gerentes operacionais gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles. Sendo assim, a gerência operacional é responsável por manter controles internos eficazes e por conduzir procedimentos de riscos e controle diariamente. Faz parte de suas atribuições identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos para garantir que as atividades estejam de acordo com as metas e objetivos. Por meio de uma estrutura de

responsabilidades em cascata, os gerentes do nível médio desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução, por parte de seus funcionários, desses procedimentos.

• **2ª Linha de Defesa:** Funções de gerenciamento de riscos e conformidade, As funções específicas variam entre organizações e indústrias, mas, quando se trata das funções típicas, temos três importantes características (ou atividades):

a) função (e/ou comitê) de gerenciamento de riscos: facilita e monitora a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional. Além disso, auxilia os proprietários dos riscos (ou seja, a alta administração da organização) a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização;

b) função de conformidade: monitora diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis. Nesse quesito, a função reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade;

c) função de controladoria: monitora os riscos financeiros e questões de reporte financeiro.

• **3ª Linha de Defesa:** Auditoria Interna Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização. É importante destacar que esse alto nível de independência

não está disponível na segunda linha de defesa. A auditoria interna promove avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle. Embora os órgãos de governança e a alta administração não sejam considerados dentre as três "linhas" desse modelo, nenhuma discussão sobre sistemas de gerenciamento de riscos estaria completa sem considerar, em primeiro lugar, os papéis essenciais dos órgãos de governança e da alta administração. Os órgãos de governança e a alta administração são as principais partes interessadas atendidas pelas "linhas" e são as partes em melhor posição para ajudar a garantir que o modelo de Três Linhas de Defesa seja aplicado aos processos de gerenciamento de riscos e controle da organização

Normas e regulamentações

No âmbito da Administração Pública Federal, existe um conjunto de normas e regulamentações relacionadas à temática de gestão de integridade, riscos e controles, dentre elas destacamos as mais relevantes:

- Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016, dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. • Portaria nº 150, de 4 de maio de 2016, institui o Programa de Integridade e o Comitê de Gestão Estratégica do Ministério do Planejamento, Desenvolvimento e Gestão e Portaria nº 425, de 30 de dezembro de 2016, que altera a Portaria MP nº 150, de 4 de maio de 2016, que instituiu o programa de Integridade e o Comitê de Gestão Estratégica do Ministério do Planejamento, Desenvolvimento e Gestão. • Política de Gestão de Integridade, Riscos

e Controles Internos da Gestão, Portaria nº 426, de 30 de dezembro de 2016, dispõe sobre a instituição da Política de Gestão de Integridade, Riscos e Controles da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

- Resolução CEG/MF nº 05/2014, que institui o Comitê de Gestão Integrada de Riscos Corporativos no âmbito do Programa de Modernização Integrada do Ministério da Fazenda (PMIMF). • Portaria MPS nº 534/2014, que estabelece princípios e diretrizes para a gestão de riscos no âmbito do Ministério da Previdência Social e de suas entidades vinculadas, dá outras providências.
- Portaria MPS nº 08/2015, que aprova o Manual de Gerenciamento de Riscos, no âmbito do Ministério da Previdência Social e de suas entidades vinculadas. Embora reconheçamos que a lista acima não é exaustiva, os normativos mencionados possibilitam às organizações uma excelente fonte de consulta para a implementação da gestão de riscos.

O COSO ERM

De acordo com o COSO ERM, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização. Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e é classificada em quatro categorias: • 1 - Estratégicos – metas gerais, alinhadas com sua missão. • 2 - Operações – utilização eficaz e eficiente dos recursos. • 3 - Comunicação – confiabilidade de relatórios. • 4 - Conformidade – cumprimento de leis e regulamentos aplicáveis.

O COSO ERM definiu oito componentes em sua estrutura, quais sejam:

- Ambiente de controle;
- Fixação de objetivos;
- Identificação de eventos;
- Avaliação de riscos;
- Resposta ao risco;
- Atividades de controle;
- Informações e comunicações;
- Monitoramento.

A figura abaixo representa o Cubo COSO ERM, indicando a relação entre a dimensão dos objetivos da instituição, a dimensão dos níveis da organização e os oito componentes dessa estrutura, vejamos:

Ambiente e controle

Este componente está relacionado ao núcleo de qualquer Organização, o pessoal (Recursos Humanos) – atributos individuais, principalmente integridade, valores éticos e competência, e o ambiente no qual operam. Ele provê uma atmosfera na qual as pessoas conduzem suas atividades e cumprem suas responsabilidades de controle, servindo de base para os demais componentes, retrata a "consciência e a cultura de controle" e é afetado fortemente pelo histórico e pela cultura da organização. Segundo o Instituto de Auditores Internos (IIA), o Ambiente de Controle representa: Atitudes e ações do Conselho e da Administração em relação à importância dos controles dentro da organização, definindo o tom da organização.

O Ambiente de Controle está intrinsecamente relacionado aos controles não operacionais, que estão fortemente relacionados com os valores das pessoas da organização e são igualmente importantes para gerar um ambiente de controle saudável. Entretanto, não são detectados pelas abordagens e ferramentas tradicionais de auditoria, requerendo técnicas não tão comumente utilizadas, para que se obtenham evidências suficientes sobre a existência deste componente, tais como a observação do ambiente. O ambiente de controle deve demonstrar o grau e comprometimento em todos os níveis da administração, com a qualidade do controle interno em seu conjunto. É o principal componente. Os fatores relacionados ao ambiente de controle incluem, dentre outros:

- integridade e valores éticos;
- competência das pessoas da entidade;
- estilo operacional da organização;
- aspectos relacionados com a gestão;
- forma de atribuição da autoridade e responsabilidade.

Fixação de objetivos

Definidos pela alta administração, os objetivos devem ser divulgados a todos os componentes da organização, antes da identificação dos eventos que possam influenciar na consecução dos objetivos. Eles devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

Identificação de eventos

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

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

Após a identificação de eventos, separando-se as oportunidades dos riscos, vamos atuar sobre esses últimos, por meio da avaliação de riscos, quando determinaremos a forma de tratamento para cada risco identificado, e qual o tipo de resposta a ser dada a esse risco.

Avaliação de riscos

A organização deve estar consciente dos riscos relevantes que envolvem o negócio, bem como deve gerenciar esses riscos de forma que os objetivos estratégicos não venham a ser prejudicados. Assim, é pré-requisito o estabelecimento, por parte da organização, de objetivos

estratégicos alinhados a sua Missão e Visão, para que ela opere de forma conjunta e organizada. A gestão de riscos (identificação e avaliação de riscos e definição de respostas, dentre elas, controles) interage com o Planejamento Estratégico, à medida que a organização, ao identificar e tratar os riscos e implementar controles internos focados nesses riscos, estará aumentando a probabilidade de alcance dos objetivos definidos. Ou seja, a gestão de riscos é considerada uma boa prática de governança da organização, ao incluir aspectos relacionados à accountability (prestação de contas, no sentido de que a gestão está alinhada às diretrizes estratégicas), à transparência (que é um pré-requisito para uma adequada prestação de contas), dentre outros.

Resposta ao risco

Para cada risco identificado, será prevista uma resposta que poderá ser: evitar, aceitar, compartilhar ou reduzir. Vejamos, de acordo com o COSO, o que sugere cada uma dessas respostas:

• evitar: sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável;

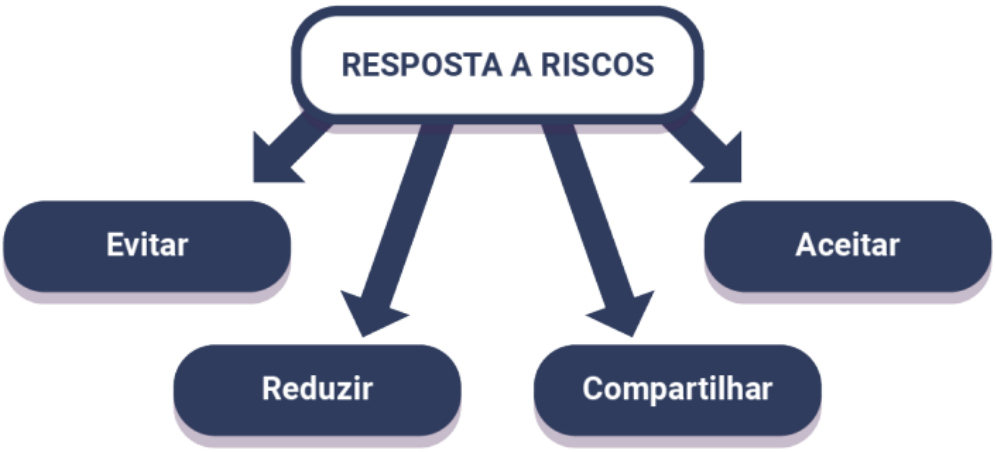
• reduzir: diminui o risco residual a um nível compatível com as tolerâncias desejadas ao risco;

• compartilhar: uma ação é tomada para transferir ou compartilhar riscos em toda a entidade ou com partes externas;

• aceitar: indica que o risco inerente já esteja dentro das tolerâncias ao risco.

É importante observarmos que aceitar o risco é uma forma de responder ao risco. Ou seja, se você "não fizer nada" em relação ao risco, você ainda estará respondendo a ele, desde que essa inércia seja consciente. Isso pode vir a ocorrer, por exemplo, quando o custo de implementação de uma medida qualquer para responder a determinado

risco fique muito alto, maior até do que os benefícios que a resposta traria para a organização. A imagem abaixo demonstra as quatro possibilidades de resposta aos riscos:



Em relação a riscos, é importante apresentar dois conceitos:

- Risco inerente: é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos.
- Risco residual: é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes.

Atividades de controle

As Atividades de Controle geralmente estão expressas em políticas e procedimentos de controle, que devem ser estabelecidos e aplicados para auxiliar e assegurar que ações identificadas pela administração, como necessárias para tratar os riscos relacionados ao cumprimento dos objetivos da organização, sejam realizadas de forma eficaz. As atividades de controle estão comumente voltadas para três categorias de riscos: de

processo ou operacionais; de registros; e de conformidade. Assim, as atividades de controle contribuem para assegurar que:

- os objetivos sejam alcançados;
- as diretrizes administrativas sejam cumpridas;
- as ações necessárias para gerenciar os riscos com vistas à consecução dos objetivos da entidade estejam sendo implementadas. As Atividades de Controle, se estabelecidas de forma tempestiva e adequada, podem vir a prevenir ou administrar os riscos inerentes ou em potencial da entidade. São exemplos de tipologias de atividades de controle:

- atribuição de autoridade e limites de alçada;
- revisão segregada;
- autorizações e aprovações;
- controles físicos;
- segregação de funções;
- verificações; • conciliações;
- indicadores de desempenho;
- revisão de desempenho operacional;
- programas de contingência e planos de continuidade dos negócios.

Monitoramento

Compreende o acompanhamento da qualidade do controle interno, visando a assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos. Pressupõe uma atividade desenvolvida ao longo do tempo. O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno pode "reagir" de forma dinâmica, ajustando-se conforme as condições o determinem. O monitoramento pode ser realizado por meio de:

• atividades contínuas; e

• avaliações independentes (por exemplo, auditorias internas e externas).

As atividades contínuas são incorporadas às demais atividades normais da organização, e as avaliações independentes garantem a eficácia do gerenciamento dos riscos ao longo do tempo. Modernamente também são utilizadas as autoavaliações, processo que pode ter um grande auxílio dos auditores, pois esses podem partir dessa autoavaliação para realizarem suas avaliações independentes, no sentido de confirmarem o que foi autoavaliado. O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a frequência das avaliações independentes dependerão basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento. Diferentemente das atividades de controle, que são concebidas para dar cumprimento aos processos e às políticas da organização e visam a tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de melhorias.

A ISO 31000

A ISO 31000 é a Norma Internacional da Gestão de Risco, que trata de estabelecer as diretrizes para condução desse processo em uma organização empresarial. Em seu texto, busca definir as boas práticas que regem o setor e norteiam o modo ideal de realizar o gerenciamento de ameaças.

Cada empresa precisará lidar com uma série de riscos moldados de acordo com as particularidades do segmento de mercado no qual atuam. Ao mesmo tempo, precisam prestar contas sobre as práticas adotadas, gerando valor e respeito para a governança corporativa da organização.

Apesar desse nível de autonomia que é garantido para cada companhia na hora de fazer o seu gerenciamento de riscos, o mercado exige um nível de padronização para assegurar a credibilidade das ações e dos resultados obtidos.

Daí a necessidade de conhecer a ISO 3001, a Norma Internacional da Gestão de Risco, que define os princípios do PGR e fornece um escopo básico para sua implementação em diferentes momentos da evolução de uma organização.

Conheça a fundo a ISO 31000, entenda como ela indica que se realize o gerenciamento de riscos, e confira os benefícios que podem ser adquiridos com sua utilização.

Ela faz a recomendação que o processo de gestão de riscos seja conduzido de maneira integrada à gestão empresarial, sendo considerado inclusive em momentos de tomada de decisão, como por exemplo na formação de parcerias e da cadeia de suprimentos.

Os riscos são abordados na norma ISO 31000 como efeitos da incerteza sobre objetivos, portanto, trazem uma definição ampla das diretivas recomendadas. Isso permite que cada empresa adapte o texto da ISO 31000, traduzido pela ABNT, para a sua realidade.

O gerenciamento de riscos é de extrema importância para proteger a operação de uma empresa, ao mesmo tempo que lhe agrega valor e a transforma em uma alternativa de investimento valiosa para o mercado.

Com esse objetivo em foco, a ISO 31000 se direciona a fatores organizacionais para que uma empresa possa otimizar o planejamento interno e a tomada de decisões para alcançar suas metas.

A abordagem sobre gestão de riscos da ISO 31000 pode ser amplamente personalizada para se adequar a cada organização, no entanto, não pode se distanciar dos princípios básicos definidos para a norma, que são os seguintes:

- Integração: a gestão de riscos deve considerar todas as atividades e relações de uma empresa;
- Estrutura e abrangência: informações levantadas pela gestão de riscos recebem um tratamento abrangente e estruturado a fim de gerar resultados consistentes;
- Personalização: a gestão de riscos deve ser personalizada para estar de acordo com as particularidades e objetivos da empresa;
- Inclusão: assim como na boa governança corporativa, deve-se promover a equidade, conscientização e inclusão de todos os interessados sobre as práticas da gestão de riscos;
- Dinamismo: o processo adotado para gestão de riscos deve ser dinâmico e flexível, ou seja, precisa estar pronto para se adequar à mudanças da legislação ou do mercado para se manter eficiente;
- Fornecimento da melhor informação: a melhor qualidade de informação possível deve ser garantida a todo momento durante o processo;
- Melhoria contínua: seguindo a recomendação sobre dinamismo, o princípio da melhoria determina que o processo de gestão de riscos deve sempre ser revisado e otimizado para conseguir os melhores resultados possíveis.

Como podemos observar, os princípios da norma ISO 31000 definem um padrão a ser mantido para obtenção de resultados satisfatórios, ao mesmo tempo que permitem à organização elaborar o processo de acordo com as suas necessidades únicas.

Os processos recorrentes permeiam as etapas do gerenciamento de riscos com base na ISO 31000, que se dá no seguinte formato:

1. Escopo, contexto e critérios

Avaliando o contexto interno e externo, é desenhado um escopo da gestão de riscos para a empresa, elencando seus critérios, objetivos e ambientação completa. É uma etapa inicial de grande importância, em

que a comunicação constante e a análise crítica dos dados apontados devem ser priorizadas.

2. Identificação de riscos

Para dar sequência ao processo de gestão de riscos, deve-se questionar tudo que possa servir para identificar o risco, incluindo o que pode acontecer, quando, onde, como e por quê.

3. Análise de riscos

Na etapa de análise, é onde deve ser criada a matriz de gestão de riscos, determinando as consequências dos riscos, probabilidade de acontecerem e o nível de impacto sofrido pela organização em cada evento.

4. Avaliação de riscos

Considerando a projeção da análise de riscos e os critérios determinados para o seu gerenciamento por parte da empresa, se estabelecem as prioridades e os riscos que demandam uma tratativa imediata.

5. Tratamento de riscos

Por fim, temos a etapa de tratamento efetivo dos riscos, em que a gestão de riscos baseada na ISO 31000 irá identificar as alternativas, analisar sua viabilidade e eficiência, preparar um plano de contingência ou mitigação de riscos e avaliar a existência de ameaças residuais.

A Norma Internacional da Gestão de Riscos ISO 31000 pode ser aplicada em diversos momentos de uma organização, elevando o nível de governança corporativa e obviamente combatendo os riscos operacionais.

De modo geral, sua utilização é válida quando temos alterações nos objetivos e metas gerais, quando se notam alterações nos riscos aos quais a empresa está exposta, incluindo por fatores no ambiente interno ou externo, ou quando é preciso implementar um processo de adequação.

A partir do processo de gestão de riscos seguindo a ISO 31000, é possível desfrutar dos seguintes benefícios:

- operações mais eficientes;
- promoção de valores de governança corporativa;
- estímulo à credibilidade empresarial;
- combate à perdas e riscos;
- desempenho melhorado quanto à normas regulamentadoras;
- gestão proativa e empenhada;
- tomada de decisões otimizada e sólida.

Saiba Mais

ISO 31000 - Vamos conhecer?

Gestão de riscos - princípios e diretrizes

A ISO 31010

A ISO 31010 funciona como uma complementação à ISO 31000, apresentando orientações para a aplicação de técnicas de avaliação de riscos, e, tornando possível a tomada de decisões baseada em evidências e análises dos riscos que envolvem o negócio.

Para que isso ocorra é necessário um processo de avaliação de riscos. E o que ele compreende? Políticas, procedimentos e processos organizacionais (em todos os níveis da organização) que tracem uma estratégia a fim de decidir quando e como avaliar os riscos.

Essa estratégia deve conter:

- Comunicação e consulta eficazes com as partes interessadas para que elas contribuam com o processo de avaliação de riscos em consonância com as outras interfaces da gestão;
- Estabelecimento de contexto no qual está inserido o projeto para que sejam estabelecidos parâmetros (internos e/ou externos) básicos, relevantes para a organização como um todo, que auxiliam a criação de critérios para o resto da gestão;
- Processo de avaliação de riscos enquanto processo geral de identificação, análise e avaliação de riscos, suas causas e consequências;
- Tratamento de riscos que envolve a seleção e o acordo de uma ou mais soluções para lidar com a ocorrência do risco e seus efeitos;
- Monitoramento e análise crítica dos riscos para verificar os resultados.

Esses elementos podem ser concretizados por meio da identificação, da análise e da avaliação de riscos, bem como da aplicação do processo de avaliação de riscos durante as fases do projeto. Mas o que significa cada etapa?

A identificação do risco, de forma resumida, consiste no procedimento de encontrar, reconhecer e registrar os riscos. E por que isso é importante? Para que seja possível identificar as situações que poderiam afetar a concretização do objetivo do projeto.

A análise de riscos diz respeito ao entendimento destes, por meio da identificação de suas causas e fontes. Esse procedimento engloba diversas técnicas e abre portas para o processo de avaliação e, posterior tomada de decisão.

A referida avaliação de riscos consiste na comparação dos níveis e critérios de riscos estabelecidos no processo de contextualização do projeto, ou seja, determina a importância e o tipo de risco de cada hipótese.

E, por fim, a aplicação do processo de avaliação de riscos durante as fases do projeto, significa a utilização prática do processo de gestão, da definição inicial de conceitos, passando pela realização do projeto, e, por fim, sua conclusão.

Importante ressaltar, neste ponto, que cada etapa necessita de um tipo específico de técnica para gerar resultados eficazes.

Seção Saiba Mais

Técnicas para o processo de avaliação de riscos.

ISO 31010: O que usar ao invés da abordagem baseada em ativos para a identificação de riscos da ISO 27001.

O gerenciamento de riscos no setor público

A iniciativa de implantar a gestão de riscos no setor público é relativamente recente no Brasil, embora, em alguns países, tenha começado há mais tempo. No Reino Unido, no início dos anos 1990, foi implantada com a finalidade de aumentar o empreendedorismo no setor público e, desde então, vem se consolidando como parte integrante do processo de gestão. Atualmente, a Commonwealth1 conta com uma política de gestão de riscos para o setor público.

No contexto brasileiro, é importante lembrar a Emenda Constitucional nº 19, de 1998, que acrescentou o conceito da eficiência no rol dos princípios que regem toda a administração pública federal (CF, art. 37, caput). O objetivo principal da gestão de riscos é aumentar o grau de

certeza na consecução dos objetivos, o que tem impacto direto na eficiência.

O Ministério do Planejamento, Desenvolvimento e Gestão (MP), Ministério da Transparência e Controladoria-Geral da União (CGU) expediram, em 2016, a Instrução Normativa Conjunta nº 01, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. O MP lançou, em 2017, o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. Ainda em 2017, foi editado o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, que trata, entre outros temas, da gestão de riscos na administração pública. A seguir, falaremos um pouco mais sobre este decreto.

Decreto da política de governança 9203/2017

A necessidade de se fortalecer a confiança da sociedade nas instituições públicas; a busca por maior coordenação das iniciativas de aprimoramento institucional; e a utilidade de se estabelecer patamares mínimos de governança motivaram o Governo Federal a implementar diversas medidas em busca de alcançar esses objetivos.

Nesse contexto, foi publicado o Decreto nº 9.203/2017, que instituiu a Política de Governança do Poder Executivo Federal e criou o Comitê Interministerial de Governança (CIG). O CIG é a base institucional do Governo e tem a responsabilidade de promover a boa coordenação e a articulação da Governança Pública na administração pública federal, tendo, em seu primeiro ano de trabalho, gerado inúmeros resultados, a exemplo dos Guias que foram aprovados.

O fortalecimento da Política de Governança Pública também passa pela adoção de instrumentos de promoção de processo decisório

baseado em evidências, tais como: a análise do impacto regulatório e a avaliação de política pública.

Assim, dentro do menu "Governança Pública" é possível encontrar materiais de referência sobre o tema, recomendações e aprovações do CIG, conteúdos relacionados ao fortalecimento do Sistema Regulatório Brasileiro e as iniciativas para o fomento de boas práticas regulatórias, bem como materiais que visam auxiliar o processo de harmonização e coordenação das avaliações de políticas públicas dentro do Poder Executivo Federal.

Pretende-se contribuir para que as organizações públicas possam criar o seu próprio modelo de Governança Pública como fonte de consulta a informações relevantes para os usuários, o que contribui para melhorar seu nível de conhecimento sobre as questões relacionadas à governança pública, que servirão como fontes de inspiração. Outrossim, objetiva-se auxiliar o dirigente público na tomada de decisões, servindo como mecanismos de prevenção de desvios de condutas e evitando apontamentos de irregularidades pelos órgãos de controle, com consequente responsabilização dos agentes.

Seus principais objetivos são:

- Tornar os dados públicos sobre governança mais acessíveis, compreensíveis e úteis e
- Conferir maior segurança jurídica ao tomador de decisões

A ideia de concretizar uma política de governança surgiu da percepção de que era necessária uma condução integrada e coerente das diversas iniciativas setoriais isoladas de aprimoramento da governança, em razão da cooperação dos órgãos centrais de governo com o Tribunal de Contas da União.

Para dar sustentação e unidade à política, foram utilizadas recomendações da literatura especializada e de organizações internacionais, notadamente da Organização para Cooperação e Desenvolvimento Econômico (OCDE), que sintetizam as melhores práticas de governança. Tudo isso levando em consideração as principais fragilidades dos modelos de governança adotados no âmbito da administração pública federal.

Com a missão de estabelecer um conjunto de boas práticas de governança que subsidiariam e direcionariam a atuação estatal, uma equipe de técnicos da Casa Civil, do Ministério do Planejamento, do Ministério da Fazenda e do Ministério da Transparência e Controladoria-Geral da União prepararam dois atos normativos: o Decreto nº 9.203, de 2017, e o Projeto de Lei nº 9.163, de 2017.

O Decreto nº 9.203, de 22 de novembro de 2017, serve como ponto de partida para a formação de um consenso mínimo acerca do que é governança – com a indicação de um conjunto inicial de referências de boas práticas e a delimitação de um objetivo trata a governança pública como um "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade".

Também apresenta uma lista sintética de princípios e diretrizes de governança, definida a partir: i) das recomendações mais atuais de organizações internacionais especializadas no tema, em especial a OCDE e o Banco Mundial; ii) de referenciais de governança do Tribunal de Contas da União; e iii) de uma revisão da literatura especializada.

A aplicação coordenada e contextualizada desses princípios é fundamental para uma boa governança. As diretrizes do decreto, por sua

vez, servem como uma fonte mínima de inspiração para atitudes concretas.

Os princípios que representam o norte da política de governança pública

- Capacidade de resposta
- Integridade
- Confiabilidade
- Melhoria regulatória
- Prestação de contas e responsabilidade
- Transparência

Seção Saiba Mais

Instrução normativa conjunta mP/CGU Parte 1 e Parte 2

Apresentação inicial e modernização do Estado

Governança pública

Considerações finais

A identificação de riscos é uma atividade complexa, dependendo de muitos elementos para se atingir resultados úteis. Pela identificação apropriada de ferramentas que podem tirar vantagem da situação e informações disponíveis, sua organização pode se concentrar nos riscos que realmente importam para o seu negócio e resultados, aplicando recursos de uma forma mais eficiente.

Referências

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. Disponível em: < https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf>. Acesso em: janeiro, 2022.

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: janeiro, 2022.

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: janeiro, 2022

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: janeiro, 2022

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: janeiro, 2022

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. **Controle Interno: Estrutura Integrada: Sumário Executivo e Estrutura.** Tradução: Price Watherhouse Coopers 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: janeiro, 2022.

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: janeiro, 2022.

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