INTOSAI GOV 9130

The International Standards of Supreme Audit Institutions, ISSAI, are issued by the International Organization of Supreme Audit Institutions, INTOSAI. For more information visit *www.issai.org*

INTOSAI

Diretrizes para Normas de Controle Interno do Setor Público - Informações Adicionais sobre Gestão de Risco nas Entidades

Tradução:

Antonio Alves de Carvalho Neto

Auditor Federal de Controle Externo do Tribunal de Contas da União: Fev. 2013

PSC-Secretariat
Rigsrevisionen • Landgreven 4 • P.O. Box 9009 • 1022 Copenhagen K • Denmark Tel.:+45 3392 8400 • Fax:+45 3311 0415 •E-mail: info@rigsrevisionen.dk

I N T O S A I

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

[INTOSAI GOV 9130]

ITEM 13

Diretrizes para Normas de Controle Interno do Setor Público

Informações adicionais sobre Gestão de Risco nas Entidades

INTOSAI PSC Subcomitê de Normas de Controle Interno

Janeiro de 2007

Sumário

Diretrizes para Normas de Controle Interno do Setor Público

Informações adicionais sobre Gestão de Riscos nas Entidades

Prefácio

As Diretrizes para Normas de Controle Interno da INTOSAI, de 1992, foram concebidas como um documento vivo, refletindo a visão de que tais normas deveriam promover a concepção, implementação e avaliação do controle interno. Essa visão implica um esforço contínuo para manter as diretrizes atualizadas.

O 17º INCOSAI (Seul, 2001) reconheceu uma forte necessidade de atualização das diretrizes de 1992 e acordou que a estrutura integrada para controle interno do Comitê de Organizações Patrocinadoras da Comissão Treadway's (COSO) deveria ser incorporada. Consulta subsequente resultou numa expansão maior para abordar os valores éticos e prover mais informações sobre os princípios gerais de controle de atividades relacionadas ao processamento de informações.

A versão atualizada das Diretrizes para Controle Interno foi emitida em 2004 e também deve ser vista como um documento vivo, que ao longo do tempo terá de ser aperfeiçoado e refinado para incorporar o impacto de novos desenvolvimentos, como a estrutura *COSO ERM - Gerenciamento de Riscos Corporativos* [1]. Assim, esta adição às Diretrizes foi produzida para abrigar o entendimento atual sobre a gestão de riscos, conforme estabelecido na estrutura COSO *ERM*. Como este documento é destinado primariamente para os leitores do setor público o termo "entidade" é usado no lugar de "Corporação", já que este tem uma associação particular com o setor privado.

As informações adicionais fornecidas aqui são o resultado do esforço conjunto dos membros do Comitê de Normas para Controle Interno da INTOSAI. Esta atualização foi coordenada por um grupo de trabalho criado entre os membros do comitê com representantes das EFS da França, Hungria, Lituânia, Holanda, Oman, Ucrânia, Romênia, Reino Unido, Estados Unidos da América e a Bélgica (presidente).

Introdução

A premissa subjacente à *Estrutura COSO - Gerenciamento de Riscos nas Entidades* é que cada entidade existe para proporcionar valor para suas partes interessadas. No setor público, a expectativa geral é que os funcionários públicos devem servir ao interesse público com equidade e gerenciar adequadamente os recursos públicos. As partes interessadas são efetivamente os cidadãos e seus representantes eleitos.

Todas as entidades enfrentam a incerteza e o desafio da gestão é determinar quanto de incerteza aceitar quando ela se empenha para obter o melhor valor para as partes interessadas. Também é importante notar que a incerteza apresenta tanto risco como oportunidade, com o potencial de corroer ou aumentar valor ou, em termos do setor público, prestar o serviço de interesse público mais ou menos bem. O objetivo da gestão de riscos nas entidades é permitir a administração lidar de modo eficaz com a incerteza e seus riscos e oportunidades associados, reforçando a capacidade de criar valor, para oferecer serviços mais eficientes, eficazes e econômicos, e para orientá-las tendo em conta valores como equidade e justiça.

As *Diretrizes da INTOSAI para normas de controle interno do Setor Público* veem o controle interno como uma estrutura conceitual por meio da qual uma entidade pode gerenciar o atingimento dos seus objetivos. A estrutura *COSO ERM* e outros modelos similares elevam essa visão a um estágio adicional, segundo o qual uma entidade pode ser dirigida com base na identificação de riscos e oportunidades futuros para refinar os objetivos e a concepção de controles internos, de maneira a minimizar riscos e maximizar oportunidades.

Assim como houve alargamento na definição das funções que abarcam o regime de governança corporativa, a gestão de riscos nas entidades requer uma mudança na maneira como as organizações pensam sobre o alcance de seus objetivos. Isso porque, para ser eficaz, a gestão de riscos nas entidades é um processo contínuo, aplicado na definição da estratégia, perpassando e afetando todos os níveis e cada unidade de negócio e concebido para identificar todos os eventos que possam afetar a capacidade da entidade para atingir os seus objetivos.

Este documento descreve uma estrutura recomendada para a aplicação dos princípios de gestão de risco nas entidades do setor público e fornece uma base contra a qual a gestão de riscos de uma entidade pode ser avaliada. No entanto, não se destina a substituir ou suplantar as *Diretrizes para Normas de Controle Interno do Setor Público,* mas, ao contrário, foi concebido para fornecer informações complementares e para ser usado junto com aquelas normas, onde os Estados membros considerarem ser apropriado fazê-lo. Também não se pretende limitar ou interferir no desenvolvimento da legislação pelas autoridades devidamente constituídas, relacionadas às regras de tomada de decisão ou outras políticas de decisão discricionárias em uma organização.

Em suma, deve-se ter claramente compreendido que este documento inclui diretrizes adicionais para os padrões de governança corporativa. As diretrizes não fornecem políticas detalhadas, procedimentos e práticas para uma implementação da melhor prática de um regime de governança corporativa, nem se espera que seja adequado para todas as organizações em todos os ambientes regulatórios. No entanto, o aditamento prevê um acréscimo à estrutura geral dentro da qual as entidades possam desenvolver regimes que melhor ajudem-nas a maximizar os serviços prestados às partes interessadas.

Como este documento está estruturado?

O suplemento está estruturado de forma semelhante às *Diretrizes para as Normas de Controle Interno do Setor Público*. No primeiro capítulo, o conceito de gestão de risco nas entidades é definido e seu escopo é delineado. No segundo capítulo, são apresentados os componentes do gerenciamento de riscos e destacadas suas conexões com as Normas de Controle Interno.

Capítulo 1: O que é Gestão de Risco

1.1 Definição

1.1.1 A Estrutura Integrada de Gerenciamento de Risco do COSO, declara que a gestão de riscos na entidade lida com riscos e oportunidades afetando a criação de valor ou a sua preservação, definindo-a da seguinte forma:

> "A gestão de risco é um processo efetuado pelo conselho de administração, gestores e outra 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 apetite a risco, para fornecer uma garantia razoável quanto à realização dos objetivos da entidade." (Modelo COSO ERM 2004).

1.1.2 No setor público os temos criação e preservação de valor não têm tanta relevância direta quanto no setor privado. No entanto, a definição é propositadamente ampla para cobrir, tanto quanto possível, os diversos setores e tipos de organizações. Assim, é possível substituir a criação de valor e sua preservação por criação de serviços e sua preservação para a definição ser plenamente aplicável às entidades do setor público.

1.2 Identificação da Missão

1.2.1 O ponto de partida para a gestão de riscos na entidade é o estabelecimento da sua missão ou visão. No âmbito desta missão, a gestão deve estabelecer os objetivos estratégicos, selecionar as estratégias para atingi-los e estabelecer objetivos de apoio alinhados e em cascata por toda a organização.

1.3 Fixação de objetivos

1.3.1 As Diretrizes da INTOSAI para Normas de controle Interno afirmam que os objetivos podem ser subdivididos em quatro categorias (embora a maioria dos objetivos pertencerão a mais do uma categoria).São elas:

- **Estratégico** - objetivos de alto nível, alinhados e dando suporte à missão das entidades.
- **Operacional** - execução ordenada, ética, econômica, eficiente e eficaz das operações; e salvaguarda dos recursos contra perda, mau uso e dano.
- **Informacional** - confiabilidade da informação, incluindo o cumprimento de obrigações de accountability.
- **Conformidade** - conformidade com leis e regulamentos aplicáveis e atuação de acordo com as políticas de Governo.

1.3.2 Objetivos nas duas primeiras categorias não estão totalmente dentro do controle da entidade, assim o sistema de gestão de risco só pode fornecer razoável garantia de que os riscos relacionados a eles estão sendo gerenciados de forma satisfatória, no entanto deverá ser capaz de informar à gestão, em tempo hábil, a extensão na qual esses objetivos estão sendo alcançados. Os objetivos relativos à confiabilidade da

informação e à conformidade estão dentro do controle da entidade, sendo esperado, portanto, que a gestão eficaz dos riscos ofereça uma garantia razoável de que estes objetivos estão sendo alcançados.

1.4 Identificação de Eventos – Riscos e Oportunidades

1.4.1 Uma vez definidos os objetivos, a gestão de riscos requer uma organização para identificar os eventos que possam ter um impacto sobre a realização desses objetivos. Os eventos podem ter um impacto negativo, um impacto positivo ou ambos. Eventos com impacto negativo representam riscos que podem prejudicar a capacidade da entidade para atingir os seus objetivos. Estes riscos podem surgir devido a fatores internos e externos. A Figura 1, adiante, apresenta muitos dos riscos que enfrentam as entidades do governo, contudo pode muito bem haver outros riscos relevantes para entidades em particular.

1.4.2 Eventos com impacto positivo podem compensar impactos negativos ou representar oportunidades. As oportunidades são a possibilidade de que um evento ocorra aumentando a capacidade da entidade para atingir seus objetivos ou permitir que a entidade os alcance com mais eficiência. Assim como a gestão busca mitigar os riscos, também deve formular planos para aproveitar as oportunidades.

1.5 Comunicação e Aprendizagem

1.5.1 Determinar se a gestão de risco de uma entidade é "efetiva" é uma parte fundamental do processo. A administração precisa fazer um julgamento sobre se os componentes da gestão de riscos estão presentes e funcionam de maneira eficaz, isto é, que não existem deficiências materiais e que todos os riscos foram trazidos para dentro de parâmetros aceitáveis, considerando o apetite a risco da entidade. Onde existe uma gestão de riscos eficaz a administração entende em que medida os objetivos em todas as quatro categorias estão alinhados com a missão e estão sendo alcançados. Uma efetiva comunicação de cima para baixo e de baixo para cima através de toda a entidade é fundamental para facilitar este processo.

1.6 Limitações

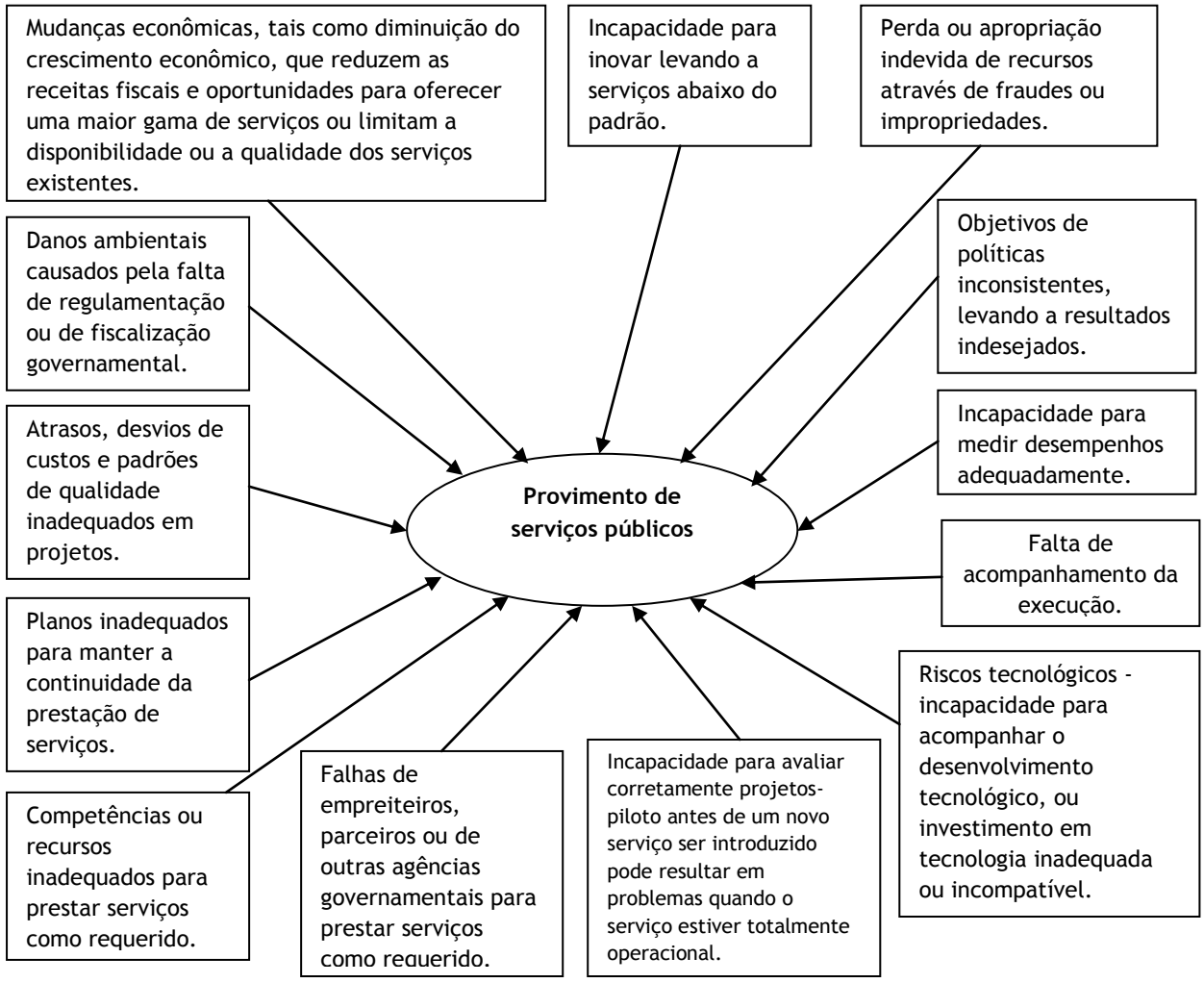
1.6.1 Não importa quão bem desenhado e operado seja o sistema, a gestão de risco de uma entidade não poderá fornecer à administração uma garantia absoluta quanto à realização dos objetivos em geral. Assim, este suplemento reconhece que somente um nível razoável de garantia pode ser obtido.

1.6.2 Garantia razoável corresponde a um nível satisfatório de confiança de que os objetivos serão alcançados ou que a gestão tomará conhecimento em tempo hábil se os objetivos dificilmente serão alcançados. Determinar o quanto de garantia é necessário para atingir um nível satisfatório de confiança é uma questão de julgamento. No exercício desse julgamento a administração terá de considerar o apetite a risco da entidade e os eventos que possam impactar a realização dos objetivos.

1.6.3 Garantia razoável reflete a noção de incerteza e risco relacionados ao futuro, que ninguém pode prever com certeza. Além disso, fatores fora do controle de uma entidade ou da sua influência, tais como fatores políticos, podem ter impacto sobre sua capacidade para atingir seus objetivos. No setor público, fatores fora do controle da entidade podem até mesmo alterar objetivos fundamentais sem prévio aviso. Limitações

também resultam das seguintes realidades: erros na tomada de decisão podem ocorrer devido a julgamentos humanos; colapsos podem ocorrer devido a falhas humanas, como simples erros ou equívocos; decisões sobre como responder a riscos e estabelecer controles necessitam considerar os custos e benefícios envolvidos; controles podem ser contornados por conluio entre duas ou mais pessoas e a gestão pode passar por cima do sistema de controle. Essas limitações impedem a gestão de ter garantia absoluta de que os objetivos serão alcançados. A Figura 1 apresenta alguns dos riscos que tipicamente são enfrentados pelas entidades do governo. Ela pretende ser mais ilustrativa do que exaustiva.

Figura 1: Alguns riscos típicos que entidades governamentais enfrentam



1.7 Relação entre Controle Interno e Gestão de Riscos nas Entidades

1.7.1 Em muitos aspectos a gestão do riscos nas entidades pode ser considerada como uma evolução natural do modelo de controle interno. A maioria das organizações busca a aplicar completamente o modelo de controle interno antes de implementar os conceitos inerentes à de gestão de riscos. O controle interno é uma parte integrante da gestão de risco da entidade. A estrutura de gestão de risco abarca o controle interno e, além disso, forma uma conceituação mais robusta de como as decisões de negócio de uma entidade devem ser tomadas quanto a possíveis desvios de sua missão fundamental e objetivos associados, oferecendo uma ferramenta para ajudar a gestão a determinar qual a resposta correta para mitigar um determinado evento. O modelo ERM vai além das Diretrizes de Controle Interno da INTOSAI em certos aspectos, em particular os seguintes:

- as categorias de objetivos são mais amplas e também incluem informação mais completa, informações não financeiras, objetivos estratégicos;
- expande o componente de avaliação de riscos e introduz diferentes conceitos de risco, como apetite a risco, tolerância a risco e resposta a risco; e
- enfatiza a importância de conselheiros independentes no conselho e define seus papéis e responsabilidades.

Capítulo 2 - Componentes da Gestão de Risco nas Entidades

A gestão de risco nas entidades consiste de oito componentes inter-relacionados. Estes componentes foram derivados da maneira como uma administração toca um negócio e foram integrados com o processo de gestão. Os componentes são:

- Ambiente interno
- Fixação de objetivos
- Identificação de eventos
- Avaliação de riscos
- Resposta a riscos
- Atividades de controle
- Informação & comunicação
- Monitoramento

Na aplicação dos componentes ao gerenciamento de riscos a entidade deve considerar todo o escopo de suas atividades em todos os níveis da organização. A gestão também deve considerar a utilização da estrutura de gestão de risco em novas iniciativas e projetos.

Aplicando a Gestão de Risco em toda a Entidade

É necessário que administração adote uma perspectiva de portfólio de riscos. Com efeito, todos os níveis da gestão terão de considerar os eventos que podem ter impacto em suas áreas de atividades e reportá-los até nível superior. Esta avaliação pode ser qualitativa ou quantitativa. A administração superior deve utilizar estas avaliações que atravessam todos os níveis e áreas de negócio para elaborar a avaliação em nível de entidade do portfólio global de riscos da organização.

Importância das Pessoas

A gestão de risco nas entidades é implementada e efetivamente posta em prática pela administração e por outras pessoas. Ela é influenciada pelo que os indivíduos dentro de uma organização fazem e dizem. Do mesmo modo, a gestão de riscos afeta as ações das pessoas. Cada colaborador é um indivíduo com diferentes competências e níveis de compreensão. A gestão de risco visa proporcionar os mecanismos para que eles possam compreender o risco, no contexto dos objetivos a entidade.

Os gestores devem conhecer suas responsabilidades e os limites de sua autoridade. Assim, uma clara e concisa ligação deve existir entre os deveres dos indivíduos e o modo de realizá-los. A gestão superior primariamente executa a supervisão, no entanto, também fornece direção, aprova estratégias e certas operações e políticas, desempenhando um papel fundamental no fortalecimento da cultura organizacional.

2.1 Relação entre Controle Interno e Gestão de Riscos nas Entidades

2.1.1 O ambiente/contexto de risco envolve o tom da organização, influenciando a consciência de riscos de todos as suas pessoas e é a base para todos os outros componentes da gestão de riscos, proporcionando disciplina e estrutura. Fatores

ambientais internos incluem a filosofia de gestão riscos da entidade; seu apetite a risco; supervisão do Conselho de Administração; integridade e valores éticos; competência do pessoal, bem como a maneira como a administração atribui autoridade e responsabilidade e organiza e desenvolve o pessoal.

Filosofia de gestão de riscos

2.1.2 A filosofia de gestão de riscos de uma entidade é o conjunto de crenças compartilhadas e atitudes que definem a forma como a entidade considera o risco em tudo o que faz, da definição da estratégia até o dia a dia das atividades operacionais. Ela influencia a cultura e o estilo de operação, incluindo a forma como os riscos são identificados, que tipos de riscos são aceitos e como eles são gerenciados. A filosofia de gestão de riscos deve estar presente em políticas estabelecidas, em comunicações orais ou escritas às partes interessadas e ao pessoal e no processo de tomada de decisões. Independentemente do método de comunicação, é de fundamental importância que a alta administração reforce a filosofia, não só através de políticas de comunicação, mas por meio de ações cotidianas.

Apetite a risco

2.1.3 Apetite a risco é a quantidade de risco em nível amplo que uma entidade está disposta a aceitar na busca para atingir seus objetivos. Ela reflete a filosofia de gestão de riscos e, por sua vez, influencia a cultura da entidade e o seu estilo operacional. O apetite a risco pode ser considerado quantitativa ou qualitativamente. Ele deve ser considerado na definição da estratégia, onde o retorno desejado de uma estratégia deve estar alinhado com o apetite a risco, que é a predisposição de aceitar ou tolerar riscos.

2.1.4 Além disso, ao identificar o ambiente de risco para selecionar um apetite a risco adequado, as entidades do setor público devem considerar a organização de maneira ampla, envolvendo todo o seu contexto. As opiniões e expectativas das organizações que são partes interessadas, sejam elas outras entidades públicas ou detentoras de poder de regulamentação, e das organizações parceiras podem dar uma clara direção quanto à adequação da uma filosofia de gestão de riscos e de apetite a risco.

Supervisão do Conselho

2.1.5 A alta administração da entidade é uma parte crítica do ambiente interno e influencia significativamente os seus elementos. É uma verdade que a cultura organizacional pode ser definida ou ser fatalmente minada pelo “tom do topo". A independência da administração superior da gestão executiva, a experiência e a respeitabilidade de seus membros, o seu grau de envolvimento e supervisão, e o adequado desempenho de suas atividades, todos desempenham um importante papel. Membros do alto escalão executivo podem fazer parte da administração superior, mas para o ambiente interno ser eficaz, é aconselhável que a equipe da administração superior contenha alguns membros independentes de fora. Isto porque a administração superior deve estar preparada para tomar contas da administração executiva, mediante questionamento e escrutínio de suas atividades e para apresentar visões alternativas.

Integridade e valores éticos

2.1.6 A integridade e os valores éticos da administração influenciam a maneira como a estratégia e os objetivos são implementados. Devido ao fato de a boa reputação da

entidade ser algo tão valioso, os padrões de comportamento devem ir além do mero cumprimento mínimo de normas legais. Comportamento ético e integridade de gestão derivam da cultura organizacional, que inclui normas éticas e comportamentais e a maneira como elas são comunicadas e reforçadas. A alta administração desempenha um papel fundamental na determinação da cultura organizacional. Ênfase indevida em resultados de curto prazo, em oposição à realização da missão global pode promover um ambiente interno inadequado.

2.1.7 Códigos formais de conduta são importantes como fundamento para a promoção de um tom ético apropriado. Canais de comunicação para cima (ou procedimentos formais de denúncia), por meio dos quais os funcionários se sintam confortáveis para trazer informações relevantes para o Conselho também são importantes. No entanto, um código de conduta escrito não garante por si só que os procedimentos estão sendo seguidos, é importante que todos os empregados tenham que demonstrar que estão cientes dos comportamentos que deles se espera. Igualmente importante para o seu cumprimento são as sanções resultantes para os empregados que violarem o código. As mensagens transmitidas pelos membros da alta gestão rapidamente se incorporam na cultura organizacional, portanto "fazer a coisa certa" quando confrontados com decisões de negócio difíceis, transmite uma mensagem poderosa que é assimilada rapidamente por toda a entidade.

Competência

2.1.8 A competência reflete os conhecimentos e habilidades necessários para executar as atribuições. Ela precisa ser suportada por apropriadas práticas de recursos humanos ao recrutamento e à promoção de pessoas adequadas, ao incentivo, à formação e para lidar com o mau desempenho. A gestão precisa definir os níveis de competência que são necessários para o desempenho de tarefas específicas e traduzi-los em descrições de cargos adequadas para cada posto de trabalho. É importante reconhecer que pode existir uma compensação entre competência e custo.

Estrutura organizacional

2.1.9 A estrutura organizacional de uma entidade fornece a base para o planejamento, a execução, o controle e monitoramento de suas atividades. A estrutura organizacional adotada deverá ser adequada às necessidades da organização. Algumas estruturas são centralizadas, outras descentralizadas, algumas organizadas por localização geográfica e outras por função. Qualquer que seja a estrutura, a entidade deve ser organizada para favorecer uma efetiva gestão de riscos e realizar suas atividades de modo a atingir seus objetivos.

Atribuição de autoridade e responsabilidade

2.1.10 A atribuição de autoridade e responsabilidade envolve estabelecer o grau em que os indivíduos e as equipes estão autorizados e são incentivados a usar a sua iniciativa para tratar de questões e resolver problemas, bem como os limites à sua autoridade. Os desafios chave são assegurar que todo o pessoal compreenda os objetivos da entidade e como as suas ações contribuem para a realização desses objetivos e somente delegar na extensão que for necessária para alcançá-los. A responsabilidade é tão importante como a autoridade. O ambiente interno é fortemente influenciado pelo grau em que os indivíduos reconhecem que eles serão responsabilizados. Isto é válido para todos, até para o executivo chefe.

2.2 Fixação de objetivos

2.2.1 Objetivos são definidos no nível estratégico, estabelecendo uma base para os objetivos de apoio, das categorias operacional, informacional e de conformidade. Cada entidade enfrenta uma série de riscos procedentes de fontes externas e internas e uma pré-condição para a eficaz identificação e avaliação de riscos e de respostas pertinentes é o estabelecimento de objetivos. Os objetivos devem ser previamente estabelecidos para que a gestão possa identificar e avaliar os riscos para a sua realização e tomar as medidas necessárias para mitigar esses riscos. Objetivos tem que ser alinhados com o apetite a risco da entidade, que por sua vez é orientado pelos níveis de tolerância a riscos da entidade.

2.2.2 A missão de uma entidade apresenta, em termos gerais, o que ela aspira alcançar. A gestão define objetivos estratégicos, formula a estratégia e estabelece as operações relacionadas. Os objetivos estratégicos são metas de alto nível, alinhados com e dando suporte à missão da entidade. A estratégia implementada e os objetivos de apoio para realizar a missão tendem a ser mais dinâmicos do que a missão e terão que ser ajustados para levar em conta as mudanças de condições.

2.2.3 Nada obstante a diversidade de objetivos entre as entidades, há certas categorias gerais que podem ser aplicadas. Todos os objetivos se classificam em uma ou mais das seguintes categorias:

Objetivos Operacionais - Dizem respeito à eficácia e eficiência das operações da entidade, incluindo metas de desempenho e salvaguarda de recursos contra perdas. No âmbito do setor público uma definição ampliada de "salvaguarda dos recursos/ativos" pode ser usada: lidar com a prevenção ou detecção e correção de desvios de recursos públicos. Os objetivos operacionais precisam refletir o ambiente particular no qual a entidade funciona. Como os objetivos operacionais são o ponto focal para direcionar a alocação de recursos, se eles não forem claros ou não forem bem concebidos, os recursos podem ser mal direcionados.

Objetivos Informacionais - Dizem respeito à confiabilidade das informações e podem envolver tanto dados financeiros como não-financeiros. Embora os objetivos informacionais também se relacionem com informação preparada para partes externas, o objetivo principal é prover informações precisas e completas à gestão, adequadas para a finalidade pretendida. Sem informações precisas e completas é muito difícil a gestão tomar boas decisões.

Objetivos de Conformidade - referem-se ao cumprimento de leis e regulamentos aplicáveis. As exigências podem referir-se aos mercados, ao meio ambiente, ao bem-estar dos funcionários etc. Algumas entidades também necessitam cumprir objetivos de conformidade internacionais.

2.2.4 Uma gestão de riscos eficaz proporciona uma garantia razoável de que os objetivos - operacionais, informacionais e de conformidade - da entidade estão sendo alcançados.

2.2.5 O apetite a risco, instituído pela gestão e pelo Conselho de Administração, é um indicativo para definir a estratégia e avaliar a importância relativa dos objetivos. Efetivamente, o apetite a risco é o nível de risco que uma entidade está disposta a aceitar na geração de valor (sob a forma de serviços públicos) para as partes

interessados. Usualmente, são inumeráveis as diferentes estratégias que podem ser concebidas para a realização da missão, cada uma com diferentes riscos. A gestão deve selecionar a estratégia e os objetivos de apoio que melhor se encaixem no apetite a risco.

2.2.6 Tolerâncias a risco são os níveis aceitáveis de variação em relação à realização dos objetivos. Elas podem ser medidas através de metas de desempenho. Muitas vezes as metas de desempenho são mais bem mensuradas quando se utiliza as mesmas unidades de medida dos objetivos correspondentes. Operar dentro de tolerâncias a risco proporciona uma maior garantia para a gestão de que a entidade está dentro de seu apetite a risco e alcançará seus objetivos.

2.3 Identificação de eventos

2.3.1 A gestão identifica eventos potenciais que, se ocorrerem, afetarão a entidade. Eles devem ser classificados para saber se representam oportunidades ou se poderiam afetar adversamente a capacidade da entidade para executar com sucesso a estratégia e alcançar seus objetivos (riscos). Ao identificar eventos, a gestão considera uma variedade de fatores internos e externos que poderiam dar origem a riscos e oportunidades, no contexto de todo o âmbito da entidade.

2.3.2 Um evento é um incidente ou ocorrência proveniente de fontes internas ou externas que afeta a implementação da estratégia ou a realização de objetivos. Eventos podem ter um impacto positivo ou negativo, ou ambos. Eventos vão desde o óbvio até o obscuro e os efeitos vão desde o inconsequente até o altamente significativo. No entanto, para evitar uma consideração excessiva de eventos, o processo de identificação é mais bem executado se for feito separadamente da avaliação da probabilidade de ocorrência do evento e seu impacto.

2.3.3 A gestão precisa compreender os principais tipos de fatores internos e externos que conduzem aos eventos. Fatores externos podem incluir, mas não estão limitados, aqueles decorrentes de mudanças no ambiente político, social e tecnológico, bem como problemas econômicos que afetam a própria entidade ou seus fornecedores. Fatores internos derivam de escolhas que a própria gestão faz relacionadas às operações. Isso pode incluir a infraestrutura da entidade, como os muitos locais em que atua; as habilidades e competências do pessoal e como sistemas de informação de negócio operam.

2.3.4 As técnicas de identificação de eventos têm um olhar tanto no passado como no futuro. Técnicas que focam sobre os eventos passados podem considerar fatores tais como relatórios e contas anuais, padrão histórico de gastos e relatórios internos. Técnicas que focam sobre eventos futuros podem considerar fatores como mudanças demográficas, novas condições de mercado e expectativas sobre mudanças no ambiente político. Técnicas variam muito em seu nível de sofisticação e automação e podem ser focadas em uma perspectiva descendente ou ascendente de eventos.

2.3.5 Eventos não ocorrem frequentemente de maneira isolada. Um evento pode provocar outro e eventos podem ocorrer simultaneamente. A gestão deve compreender como os eventos se relacionam. Ao avaliar essas relações pode ser possível determinar onde os esforços da gestão de riscos devem ser mais bem direcionados.

2.3.6 Também pode ser útil agrupar eventos potenciais em categorias. Ao agrupar os eventos horizontalmente através da entidade e verticalmente dentro das unidades operacionais, a gestão pode ganhar uma compreensão das relações entre eles. O agrupamento de eventos também pode trazer alguma orientação sobre quais poderiam ser as melhores respostas em termos de custo/efetividade. Embora cada entidade desenvolva seu próprio método de agrupamento de eventos, existem ferramentas padrão como a Análise de Mercado PEST [2] que podem servir como base.

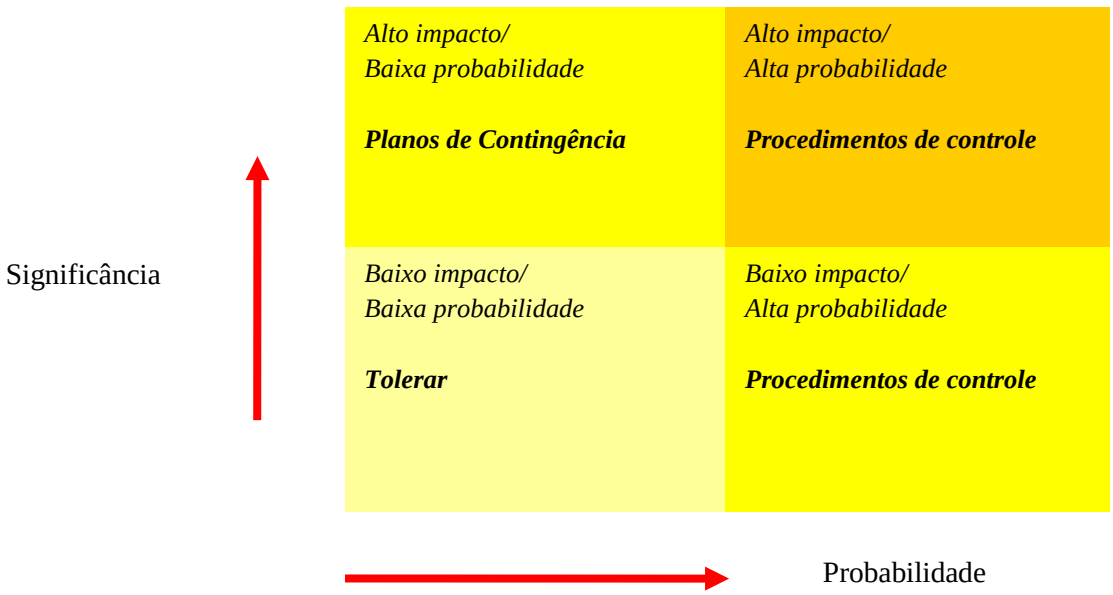
2.4 Avaliação de riscos

2.4.1 A avaliação de riscos permite a uma entidade considerar a extensão na qual os eventos têm um potencial impacto sobre a realização dos objetivos. A gestão deve avaliar os eventos em duas perspectivas - impacto e probabilidade - usando uma combinação de técnicas quantitativas e qualitativas. Os impactos positivos e negativos dos eventos podem ser avaliados individualmente ou por categoria, por seu impacto em toda a entidade. Riscos devem ser avaliados em ambas as bases, inerente e residual.

2.4.2 Embora o termo "avaliação de riscos" algumas vezes seja usado de maneira conjugada com uma atividade pontual, no contexto da gestão de risco, o componente de avaliação de riscos é uma interação contínua e iterativa das ações que ocorrem em toda a entidade. O objetivo da avaliação de riscos é identificar quais eventos são bastante importantes e significativos o suficiente para serem o foco de atenção da gestão.

2.4.3 A incerteza dos potenciais eventos precisa ser avaliada a partir das perspectivas de probabilidade e impacto. Probabilidade representa a possibilidade de que um evento irá ocorrer em um determinado período de tempo, enquanto o impacto representa a dimensão do efeito que o evento terá na capacidade da entidade para atingir seus objetivos. O período de tempo durante o qual a gestão avalia a probabilidade deve ser consistente com o horizonte temporal da estratégia e dos objetivos relacionados. Os riscos mais importantes são aqueles com alta probabilidade de ocorrência e alto impacto. Por outro lado, os riscos menos importantes são aqueles com uma baixa probabilidade de ocorrência e baixo impacto. O foco da gestão deve ser dirigido para os riscos de alta probabilidade e alto impacto (ver a Figura 2, adiante). O resultado final do processo será o de atribuir a cada risco uma classificação, tanto para a probabilidade como para impacto. Algumas entidades usam uma escala alto-baixo, outras um sistema "semáforo" de vermelho, laranja e verde, e outras uma medida quantitativa, como uma pontuação percentual.

Figura 2: Matriz simples de avaliação e resposta a riscos



2.4.4 A metodologia de avaliação de riscos pode ser quantitativa ou qualitativa e pode ser baseada em métodos objetivos e subjetivos. Nenhuma entidade precisa empregar técnicas de avaliação comum a todas as áreas de negócio. No entanto, a gestão precisa estar ciente do viés humano ao avaliar riscos e necessita assegurar-se de que todos os membros relevantes da equipe tenham um entendimento comum do que significa a terminologia de classificação para avaliar riscos. Se isso não for feito, será difícil para a alta administração avaliar a importância relativa dos diferentes riscos.

2.4.5 Uma vez que os riscos foram avaliados, as prioridades de risco para a entidade devem emergir. Se a exposição ao risco é inaceitável, dado o apetite de risco da entidade, o risco deve ser classificado como de alta prioridade ou "risco-chave". Os riscos chave devem ter uma atenção contínua do mais alto escalão da entidade. Prioridades específicas de risco mudam ao longo do tempo, quando os objetivos da entidade alteram, o ambiente de riscos muda e os riscos chave são tratados.

2.4.6 A avaliação de riscos, conforme descrita anteriormente, se refere ao "risco inerente". Risco inerente é o risco que enfrenta uma atividade na ausência de quaisquer ações da gestão para modificar a probabilidade ou impacto de eventos. Risco residual é o risco que permanece depois que a gestão desenvolve suas atividades de resposta a riscos, que é delineada no próximo parágrafo. A vantagem desse método é que ele permite às entidades identificar riscos que estão tomando tempo da gestão que poderia ser mais bem aplicado em outras questões (e.g. porque o risco inerente tem uma baixa probabilidade de ocorrência).

2.5 Resposta a riscos

2.5.1 Tendo avaliado os riscos relevantes, a gestão decide como irá respondê-los. Formas de abordar riscos identificados incluem transferir, tratar, encerrar atividades e tolerar o risco. Ao considerar sua resposta, a gestão avalia seu efeito sobre a

probabilidade e o impacto do risco, bem como os custos e benefícios de cada resposta, para selecionar uma resposta que traga o risco residual para dentro da tolerância a risco desejada. A gestão deve também identificar eventuais oportunidades que estão disponíveis e assumir uma perspectiva ampla da entidade, uma visão de portfólio de risco.

2.5.2 Respostas a riscos abrangem as seguintes categorias:

- ***Compartilhar/Transferir risco*** - redução da probabilidade ou do impacto do risco pela transferência ou pelo compartilhamento de uma parte do risco. Isso pode ser feito por meio da contratação de seguros ou de pagamento a um terceiro para assumir o risco de outra maneira. Esta opção é particularmente útil para mitigar riscos financeiros, riscos de ativos e para atividades subcontratadas. Contudo, a maioria dos riscos não pode ser inteiramente transferida. Em particular, geralmente não é possível transferir o risco reputacional, ainda que a entrega de um serviço seja contratada externamente.
- ***Reduzir/Tratar risco*** - De longe, o maior número de riscos serão tratados desta forma. Ações são tomadas para reduzir a probabilidade ou o impacto do risco, ou ambos. Isso normalmente envolve uma miríade de decisões de negócio todos os dias, incluindo atividades de controle discutidas em mais detalhes na seção 2.6 e em Controles Internos - Estrutura Integrada.
- ***Evitar/Encerrar atividade*** - Saindo das atividades que geram riscos. Embora as entidades do setor público possam raramente eximir-se de executar um elemento essencial de um programa, evitar pode ser uma resposta útil ao decidir sobre se um novo método de entrega de serviços é adequado ou ao estudar a possibilidade de continuar com um projeto específico.
- ***Aceitar/Tolerar risco*** - Nenhuma ação é tomada para reduzir a probabilidade ou o impacto do risco. Esta resposta sugere que nenhuma resposta eficaz para reduzir o impacto e a probabilidade a um nível aceitável, com um custo razoável, foi identificada, ou ainda, que o risco inerente já está dentro das tolerâncias a risco. Tolerar risco pode, evidentemente, se complementar com planos de contingência para lidar com os impactos que surgirão se o risco for concretizado.

2.5.3 O modelo ERM não apenas enfatiza a antecipação e manejo dos riscos, mas também, dentro da mesma abordagem, a identificação de oportunidades. Em qualquer situação a gestão deve atentar para considerar as oportunidades ou os eventos com impacto positivo e não apenas considerar riscos ou eventos com impacto negativo. Isso envolve dois aspectos: primeiro, ao mitigar uma ameaça, pode surgir uma oportunidade para explorar um impacto positivo; segundo, considerar se as circunstâncias que surgiram, embora não gerando ameaças, oferecem oportunidades positivas.

2.5.4 A gestão deve avaliar os efeitos das diferentes respostas, para então decidir a melhor forma de administrar o risco, a seleção de uma resposta ou combinação de respostas visa trazer tanto a probabilidade como o impacto do risco para dentro das tolerâncias a risco. A resposta selecionada não precisa necessariamente gerar a quantidade mínima de risco residual, mas se gerar um risco residual acima dos limites de tolerância, a gestão terá que reconsiderar a resposta ou os limites de tolerância a risco.

2.5.5 Avaliar respostas alternativas ao risco inerente requer consideração sobre os riscos adicionais que possam resultar de uma resposta. Aqui, é útil a administração superior considerar as respostas a partir de uma perspectiva de portfólio, que lhe dê uma visão geral do perfil de uma resposta e lhe permita analisar se a natureza e os tipos de riscos residuais que remanescem se encaixam com a missão global e o apetite a risco.

2.5.6 Uma vez que a gestão seleciona o método preferencial para abordar o risco, é necessário desenvolver um plano de implementação para executá-lo. Uma parte crítica de todo plano de implementação é o estabelecimento de atividades de controle para assegurar que a resposta ao risco seja realizada de forma eficaz.

2.6 Atividades de controle

2.6.1 Atividades de controle são as políticas e os procedimentos que ajudam a assegurar que as respostas a risco da gestão sejam executadas. Essas atividades de controle ocorrem em toda a organização, em todos os níveis e em todas as funções. As *Diretrizes para Normas de Controle Interno do Setor Público* contêm informações detalhadas para estabelecer controles eficazes. Este adendo não pretende fazer nada mais do que colocar os controles internos no contexto da gestão riscos nas entidades.

2.6.2 A gestão de riscos vê as atividades de controle como uma parte importante do processo pelo qual uma entidade procura atingir os seus objetivos de negócio. As atividades de controle não são realizados simplesmente para seu próprio bem, ou porque parece que é a "coisa certa a fazer", mas sim servir como mecanismos de gestão na realização dos objetivos de negócio.

2.6.3 Conquanto as atividades de controle sejam geralmente estabelecidas para assegurar que as respostas a riscos sejam conduzidas de maneira adequada, em relação a certos objetivos, as atividades de controle são em si mesmas a resposta a risco. A seleção ou a revisão de atividades de controle precisa incluir considerações sobre a sua relevância e adequação à resposta aos riscos e aos objetivos relacionados.

2.6.4 Devido ao fato de que cada entidade tem seu próprio conjunto de objetivos e sua própria abordagem de implementação, haverá diferenças nas respostas a riscos e nas atividades de controle relacionadas. Ainda que duas entidades com os mesmos objetivos tomem decisões semelhantes sobre como eles devem ser alcançados, as atividades de controle resultantes serão provavelmente diferentes. Isso ocorre porque as diferentes equipes de gestão terão diferentes limites de apetite e tolerância a risco.

2.6.5 No entanto, no contexto da gestão de riscos todos as atividades de controle se encaixam em quatro grandes categorias:

- **Controles preventivos** – concebidos para limitar a possibilidade de um risco se materializar e um resultado indesejável se concretizar. Quanto maior for o impacto do risco na capacidade da entidade para alcançar os seus objetivos, maior será a importância de se implementar adequados controles preventivos.
- **Controles Diretivos** – concebidos para assegurar que um determinado resultado seja alcançado. Esses controles são particularmente importantes quando é crítico que um evento indesejável (como uma violação de segurança) seja evitado, por isso são muitas vezes utilizados para apoiar a realização de objetivos de conformidade.

- **Controles Detectivos** – concebidos para identificar se resultados indesejáveis ocorreram "depois de um evento". Não obstante, a presença de adequados controles detectivos também pode mitigar o risco de que resultados indesejáveis ocorram pela criação de um efeito de dissuasão (N.T. expectativa de controle).
- **Controles Corretivos** – concebidos para corrigir resultados indesejáveis que tenham se realizados. Eles também podem agir como uma contingência para se conseguir alguma recuperação, quer de recursos ou de reabilitação contra perdas ou danos.

2.7 Informação e Comunicação

2.7.1 Há pouca diferença entre os requisitos de qualidade dos dados utilizados para apoiar os objetivos de controle interno e os requisitos de qualidade dos dados utilizados para apoiar gestão de riscos da entidade. As *Diretrizes para Normas de Controle Interno do Setor Público* contêm informações detalhadas sobre requisitos de informação e comunicação. Este adendo não pretende fazer nada mais do que colocar esses requisitos no âmbito gestão de riscos das entidades.

Informação

2.7.2 A gestão de riscos requer especificamente que uma entidade capture uma ampla gama de informações que são necessárias para atingir os objetivos de controle interno, por exemplo, o foco nos objetivos estratégicos exige mais informações sobre produtos e resultados. Além disso, a utilização que se dá a esses dados é ligeiramente diferente. Dados históricos permitem à entidade para acompanhar o desempenho real de metas, planos e expectativas e pode fornecer alertas tempestivos de eventos potenciais que requerem a atenção da gestão. Dados atuais permitem a gestão ter uma visão em tempo real dos riscos existentes dentro de uma unidade de negócio ou de um processo e identificar variações frente a expectativas. Isso pode permitir a entidade determinar se ela está operando dentro das tolerâncias a risco estabelecidas.

2.7.3 Informações pertinentes devem ser identificadas, capturadas e comunicadas em forma e prazos que permitam as pessoas desempenhar suas responsabilidades. A comunicação eficaz também ocorre ao fluir de cima para baixo, através e de baixo para cima em todos os níveis da entidade. Todo o pessoal deve receber uma mensagem clara da alta gestão de que as responsabilidades de gerenciamento de riscos na entidade devem ser levadas a sério. Eles precisam entender o seu papel individual no processo de gestão de riscos da entidade, bem como ele se relaciona com o trabalho dos outros. O pessoal deve dispor de meios para comunicar informações significativas dos escalões inferiores para um nível adequado da gestão. Também há a necessidade de se ter uma comunicação eficaz com as partes interessadas externas.

2.7.4 Ter as pessoas certas, com a informação certa, no tempo e no lugar certo, é essencial para efetuar a gestão de riscos da entidade .

Comunicação

2.7.5 A comunicação é inerente aos sistemas de informação. Além de fornecer informações que permitam ao pessoal realizar adequadamente suas atribuições, a comunicação também deve ter um sentido mais amplo, divulgando a cultura corporativa, lidando com as expectativas, cobrindo as responsabilidades dos indivíduos e grupos e outros assuntos relevantes.

2.7.6 A administração deve prover uma comunicação interna específica e dirigida que trate as expectativas comportamentais e as responsabilidades do pessoal. Isto deve incluir uma exposição clara da filosofia e abordagem da gestão do risco na entidade. Comunicações sobre processos e procedimentos devem alinhar e consolidar a cultura desejada. A comunicação deve transmitir:

- ✓ A importância e relevância da gestão de risco na entidade
- ✓ Os objetivos da entidade
- ✓ O apetite e as tolerâncias a risco da entidade
- ✓ Uma linguagem comum para a identificação e avaliação de riscos
- ✓ Os papéis e as responsabilidades do pessoal na efetivação e apoio aos componentes da gestão de riscos.

2.7.7 Também há necessidade de se ter métodos para os empregados comunicar informações baseadas em risco para a sua gestão de linha e para toda a organização. Funcionários da linha de frente, que lidam diariamente com questões operacionais críticas, estão em melhores condições para reconhecer os problemas que podem surgir. Para que essas informações sejam comunicadas, deve haver canais de comunicação abertos e uma clara vontade de ouvir. Se a cultura organizacional for de "atirar no mensageiro", os funcionários não irão comunicar problemas a seus superiores e os riscos poderão não ser identificados em tempo hábil.

2.7.8 Na maioria dos casos as linhas normais de reporte são adequados canais de comunicação ascendentes. No entanto, existem algumas circunstâncias em que canais alternativos de comunicação (como algum tipo de linha de denúncia) são necessários. Devido à sua importância, a gestão eficaz de riscos na entidade requer a existência de um canal alternativo de comunicação direto com o gestor máximo disponível para todos os funcionários utilizarem sem medo de repercussão.

2.7.9 Existe a necessidade de uma comunicação adequada não só dentro da entidade, mas também com o exterior. É importante comunicar externamente às partes interessadas sobre a maneira pela qual a entidade está gerenciando os riscos para lhes dar garantias de que vai entregar o que dela se espera e para administrar as expectativas do que pode ser entregue. Isto é particularmente importante em relação aos riscos que afetem o público e onde o público depende de seu governo para administrar os riscos para eles. A seriedade com que são tratadas as comunicações com as partes externas e a honestidade dessa comunicação também enviam importantes mensagens para toda a entidade e pode ter um impacto significativo na cultura organizacional.

2.8 Monitoramento

2.8.1 A gestão de riscos na entidade deve ser monitorada para avaliar o funcionamento de seus componentes ao longo do tempo. Isto pode ser realizado por meio de atividades de monitoramento contínuo, avaliações em separado, ou uma combinação das duas. Deficiências no sistema de gestão de riscos da entidade necessitam ser comunicadas a um nível apropriado da gestão. As questões sérias devem ser relatadas à alta administração ou ao Conselho a fim de que a entidade possa melhorar seus processos.

2.8.2 Os objetivos de uma entidade podem mudar ao longo do tempo. O portfólio de riscos enfrentados e sua importância relativa também são passíveis de mudanças ao longo do tempo. Respostas a riscos, que antes eram eficazes, podem se tornar irrelevantes ou impossíveis de implementar e as atividades de controle podem se tornar menos eficazes ou caducar por completo. A gestão precisa monitorar constantemente a eficácia do seu sistema de gestão de riscos, a fim de determinar se ainda é adequado e eficaz.

2.8.3 As avaliações da eficácia da gestão de riscos varia de alcance e frequência, dependendo da importância dos grupos de riscos e da importância das respostas e controles relacionados com a gestão desses riscos. Quando a administração toma a decisão de proceder a uma avaliação global da estrutura de gestão de riscos, a atenção deve ser direcionada para abordar todos os aspectos do processo, incluindo a definição da estratégia. No entanto, as atividades regulares de gestão, como a atualização dos registos de riscos e verificações organizacionais ou funcionais, também são parte do monitoramento do processo de gestão de riscos.

Bibliografia

Australian Standard® for risk management (Standards Australia, 2004)

Entity Risk Management - Integrated Framework (COSO, 2004)

Integrated Risk Management Framework (Treasury Board of Canada Secretariat, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM & ALARM, 2002)

The Orange Book: Management of Risk - Principles and Concepts (HM Treasury, 2004)

---

[1] Enterprise Risk Management - Integrated Framework (COSO - Setembro de 2004)

[2] A análise PEST é uma ferramenta útil para a compreensão e avaliação do impacto de fatores externos sobre a realização dos objetivos da entidade. PEST é um acrônimo para fatores Políticos, Económicos, Sociais e Tecnológicas.