GESTÃO DE RISCOS NA ADMINISTRAÇÃO PÚBLICA

AULA 01: Aula Demonstrativa

PROF. KLEBERSON ROBERTO DE SOUZA

2019

Conteúdo

1. INTRODUÇÃO 5

1. BASES CONCEITUAIS 9

1.1 Objetivos 8

1.2 Riscos 13

1.3 Controle Interno 17

1.4 Gestão de Riscos 24

1.5 Modelos de Referência 30

Primeiramente, gostaria de agradecer o interesse nesta aula demonstrativa. Após me apresentar brevemente a vocês, falaremos sobre como implementar, manter e monitorar uma adequada gestão de riscos, de forma prática e direta.

KLEBERSON SOUZA

- ✓ Auditor Federal de Finanças e Controle da **Controladoria-Geral da União** (CGU), lotado na CGU-Regional/MT.

- ✓ Especialista em Direito e Controle Externo da Administração Pública pela FGV e em Auditoria Contábil e Tributária pela UFMT, com certificação internacional pela *Internacional Organization for Standardization - ISO* em Gestão de Riscos (C31000);

- ✓ Coautor dos livros Como Combater à Corrupção em Licitações – Detecção e Prevenção de Fraudes e Como Combater o Desperdício no Setor Público – Gestão de Riscos na Prática, ambos lançados pela Editora Fórum em 2016 e 2019, respectivamente; autor dos livros de Avaliação de Controles Internos: Contratações Públicas e Implantação de Governança no Setor Público, lançados pela Editora Publicontas do TCE/MT em 2017 e 2019, respectivamente e autor do Guia de Integridade das Empresas Estatais Federias, publicado pela CGU em 2015.

- ✓ Professor de pós-graduação da UFMT com a disciplina Gestão de Riscos e Palestrante na área de auditoria governamental, detecção de fraudes em licitação e contratos, gestão de riscos e avaliação de controles internos.

1. INTRODUÇÃO

A gestão de riscos não é um modismo. A gestão de riscos não é uma prática "enlatada" exportada pelo mundo desenvolvido. A gestão de riscos não é apenas uma filosofia, um conjunto de boas ideias inexequíveis. A gestão de riscos não é uma solução mágica, que garantirá a resolução de todos os problemas da Administração Pública.

Segundo a ISO 31000/2018, Gestão de riscos é um conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a eventos incertos que podem afetar os objetivos. Entretanto, os gestores públicos não parecem bem preparados para lidar com riscos, de modo geral. Para reforçar essa tese, basta lembrar de um monte de notícias tratando de fraudes, prejuízos, superfaturamentos, desvios, fracassos, falhas, erros, desastres, tragédias.

Esse cenário triste e recorrente, meio cristalizado, meio generalizado, meio arraigado no setor público brasileiro decorre, em boa medida, da precariedade com que se organizam e desenvolvem sistemas de governança, gestão de riscos e controles internos nas organizações governamentais.

Essa precariedade, com traços marcantes de amadorismo, pitadas ainda generosas de patrimonialismo, nepotismo e anacronismo, afeta a capacidade das organizações públicas atingirem seus objetivos, produzindo consequências para toda a sociedade, especialmente para a parcela que mais depende dos serviços prestados pelo Estado. No setor público, em vez de lucros e dividendos, o cidadão, verdadeiro proprietário do empreendimento, quer resultados em termos de políticas sociais, esperando retorno efetivo dos impostos.

Isso cria um típico conflito de agência entre cidadão e governo, em que o cidadão, como principal, não tem certeza de que o gestor público, o agente, está maximizando o resultado esperado, em termos de bens e serviços para a sociedade, gerando, assim, assimetria informacional. O cidadão financia o Estado, o que lhe dá, tal como o sócio de uma empresa privada, direito à informação e a resultados adequados.

Resultados adequados é o que a Constituição Federal exige como fundamento da gestão pública: legalidade, impessoalidade, moralidade, publicidade e eficiência.

Assim, não é suficiente cumprir leis e regulamentos e agir com integridade. É imperativo atingir os objetivos, e fazê-lo buscando qualidade adequada dos bens e serviços ofertados, a partir dos recursos disponíveis, ao menor custo possível.

A literatura especializada sobre controles internos e gestão de riscos identifica clara correlação entre essa abordagem gerencial e a eficiência das organizações. A ISO 31000, por exemplo, defende que uma adequada gestão de riscos aumenta a possibilidade de atingir objetivos e melhora a eficácia e eficiência operacional. Assim, a eficiência proporcionada pela adoção da gestão de riscos e controles internos na entidade decorre da adequação entre riscos enfrentados e controles internos existentes para mitigá-los.

Organizações ao redor do mundo, inclusive do setor público em diversos países, vêm se adaptando ao ambiente de mudanças contínuas, vivenciado nos últimos anos, mediante a adoção de estruturas de governança e práticas administrativas fortemente voltadas para gerenciar riscos que possam impedir ou dificultar a realização de suas missões e o alcance de seus objetivos,

estabelecendo estruturas de controle interno capazes de responder adequadamente aos riscos identificados e, assim, garantir razoável certeza quanto ao alcance de seus objetivos, à consecução de suas missões e, por conseguinte, à continuidade e sustentabilidade de seus negócios

Consultando os julgados do Tribunal de Contas da União (TCU) de 2001 a 2018, encontramos 683 acórdãos tratando do tema "gestão de riscos", sendo 539 só de 2013 em diante, representando 80% do total.

Isso mostra o quanto a "Gestão de Riscos" tem se tornado central em um dos principais órgãos de controle do país. De forma cada vez mais frequente, o TCU tem determinado às entidades públicas que adotem um processo sistemático de gerenciamento de riscos.

O TCU passou a perceber que o gerenciamento de riscos é um processo fundamental para racionalizar a ação governamental, melhorar a tomada de decisão e avaliação de desempenho. A identificação, avaliação e tratamento de riscos de maneira lógica e sistemática proporciona uma visão ampla do custo-benefício do controle interno, lidando com o futuro, suas incertezas e oportunidades.

Por isso, para o Tribunal de Contas, a gestão de riscos é uma "poderosa ferramenta" para os gestores públicos.

Foi sobre essa "poderosa ferramenta" que Paulo Capivara, prefeito de Pantanal do Norte, município fictício do interior de Mato Grosso, ouviu falar. E ouviu muito, porque o controlador-geral, João Coruja, não perdia uma oportunidade de tocar no assunto. Em toda reunião, encontro, relatório, nota de auditoria, até na pausa do cafezinho estava lá o João falando de riscos.

Tanta insistência deu resultado. Especialmente depois de alguns casos graves de irregularidades e falhas na gestão municipal. Merenda estragada, comida que os alunos detestavam, falta de medicamentos, desvio de combustível, carro oficial usado em festa particular, sumiço de processos, funcionários fantasmas, fraudes em licitação, excesso de carimbo, formulários inúteis em cinco vias. Todos casos em que o controlador-geral apontou fragilidades no gerenciamento de riscos.

Até que enfim, o prefeito se convenceu de que precisava agir para combater o desperdício e evitar que mais problemas acontecessem. Não adiantava só lamentar. Era preciso prevenir. E o controlador sempre dizia que a melhor forma de prevenção era atuar sobre as causas e os fatores de risco, melhorando os controles internos.

Controles internos?

Todo mundo, inclusive o prefeito, achava que "controle interno" era o nome do setor que João Coruja chefiava. Ele e os auditores José Onça e Gilberto Tuiuiú entravam em algum departamento e o comentário geral era "lá vem aquele pessoal do controle interno...".

Foi preciso certo esforço da controladoria municipal e muitos dedos de prosa, mas, por fim, o pessoal se convenceu de que controle interno é um mecanismo de enfrentamento de riscos, de responsabilidade dos gestores. Às vezes é chamado de controle interno administrativo, controle interno da gestão ou controle interno primário para se diferenciar do controle interno avaliativo, a auditoria governamental.

Essa confusão acontecia em Pantanal do Norte e se repete em muitos lugares. Uma senha para entrar nos computadores é um controle interno. Uma etiqueta, um inventário e uma norma de registro no patrimônio, também. Um checklist, uma rotina de conferência, um sistema, um crachá, um manual, todos são controles internos instituídos pelos gestores para reduzir riscos. Mesmo que eles não saibam disso.

A "controladoria" ou a "auditoria interna" não é responsável por esses mecanismos. Seu papel fundamental é avaliar se o controle instituído é adequado e se está efetivamente funcionando. E tudo isso tem a ver com a gestão de riscos. Controle interno é o principal mecanismo de gerenciamento de riscos. Ele existe para evitar, mitigar a ocorrência de um risco ou minimizar seu impacto, caso ele venha a acontecer. Mas, para gerenciar riscos e implantar controles, é preciso ter estrutura adequada e uma boa estratégia de atuação.

Sabendo disso, o prefeito de Pantanal do Norte decidiu instituir uma estrutura de gestão de riscos no município, ou seja, criou o comitê de gestão de riscos. Esse comitê ficou responsável por definir a política de gestão de riscos, fomentar a sua prática efetiva, monitorar a execução, estimular uma cultura de gestão de riscos na prefeitura, entre outras atividades.

Foi aí que a diretora de compras, Maria Carcará, que já vinha pensando sobre o gerenciamento de riscos há algum tempo, decidiu tomar a dianteira, depois que dois casos graves haviam sido detectados em seu setor pela controladoria, acrescentados à lentidão e retrabalho frequentes que ela tinha identificado sozinha. Se era para fazer a tal de gestão de riscos, Maria Carcará começaria logo. Até porque o pessoal da controladoria alertou que a área de compras é um excelente lugar para começar esse processo nas organizações públicas.

Diante dos episódios desagradáveis – a necessidade de adotar novas práticas gerenciais para criar e proteger valor na área de licitação e a determinação superior para implantar a política de gestão de riscos –, a diretora decidiu começar por seu processo mais crítico: a licitação.

Problemas nessa área são recorrentes, especialmente em razão de especificações e pesquisas de preços deficientes, recursos e impugnações contra editais e contra os resultados, falta de dotação orçamentária, fraudes e conluios, entre outros. Sendo assim, a diretora entendeu que ali havia muitos riscos a serem gerenciados.

Depois de pegar o jeito com as licitações, Maria Carcará também atuou sobre os riscos dos contratos.

Seus colegas de outros departamentos da prefeitura, também realizaram o mesmo processo. Os setores de gestão de pessoas, gestão financeira, gerenciamento de frotas, alimentação escolar, medicamentos, patrimônio e convênios identificaram, avaliaram e estabeleceram medidas de tratamento de riscos nas suas atividades mais relevantes.

Agora você, caro leitor, vai acompanhar passo a passo esse processo de mudanças na pujante e hospitaleira Pantanal do Norte, o que pode servir de exemplo para implantação da gestão de riscos em qualquer organização do setor público.

Tenha em mente que este curso traz exemplos de riscos de diversas atividades de uma organização, considerando entendimentos do Tribunal de Contas da União (TCU), Controladoria-

Geral da União (CGU) e a experiência do autor. É uma referência na identificação dos riscos de um órgão específico.

Porém, não pretende ser um conjunto exaustivo. Nem poderia, já que cada organização precisa identificar os seus próprios riscos, suas respectivas probabilidades e impactos. Esse é um dos princípio da gestão de riscos, ou seja, ela é personalizada, feita sob medida e leva em consideração fatores humanos e culturais da organização.

Sabendo isso, esperamos que o exemplo de Pantanal do Norte possa servir de ponto de partida para todos os gestores governamentais combaterem efetivamente o desperdício por meio da gestão de riscos, na busca por uma Administração Pública mais efetiva, integra, ágil e responsável.

Preparado? Vamos começar por conceitos...

1. BASES CONCEITUAIS

Qual é a relação entre objetivos, riscos e controles?

Qual é o significado de risco? Quais as classificações de risco adotadas?

Como gerenciar riscos na Administração Pública? Qual é a sua importância para a eficiência das organizações?

Existem modelos que podem ser utilizados como referência para gestão de riscos?

Para responder a essas e outras questões, estudaremos, nesta aula, os conceitos básicos do curso de gestão de riscos na Administração Pública.

Começaremos estudando o conceito de objetivo, risco e controle emitido pelos órgãos de controle como a Controladoria-Geral da União (CGU) e Tribunal de Contas da União (TCU). Em seguida, faremos a diferenciação entre risco inerente e risco residual e abordaremos os objetivos da gestão de riscos no setor público.

Finalizaremos a aula, apresentando os principais modelos de referência em gestão de riscos que podem ser adotados pela Administração Pública.

Os conceitos trabalhados nesta aula são fundamentais para a compreensão e realização da gestão de riscos que será detalhada nas aulas seguintes.

Pronto para começar?

Então, vamos.

1.1 CONCEITOS BÁSICOS

Todas as organizações desempenham atividades administrativas para o cumprimento de seus objetivos institucionais. Essas organizações enfrentam fatores decorrentes dos ambientes interno e externo que tornam incerto se irão atingir esses objetivos e quando isso irá ocorrer. O efeito que essa incerteza provoca nos objetivos é chamado de "risco" (ABNT, 2018).

Todas as organizações gerenciam o risco em maior ou menor grau, mesmo que ainda não o faça de modo estruturado, sistematizado e oportuno. Isso acontece quando a organização identifica, avalia e trata os riscos, adotando controles internos da gestão ou simplesmente "controles internos". A implantação, o efetivo funcionamento e a avaliação dos controles internos decorrem de mandamento constitucional.

A finalidade desses controles é garantir que o poder público atue em estrita observância aos princípios da legalidade, da moralidade e da eficiência, almejando a conformidade dos atos da gestão, o alcance dos seus objetivos, a melhor qualidade dos serviços públicos prestados à população e a boa governança pública.

Para gerenciar riscos na Administração Pública, é preciso ter clareza dos conceitos de **objetivos, riscos e controles** apresentados a seguir.

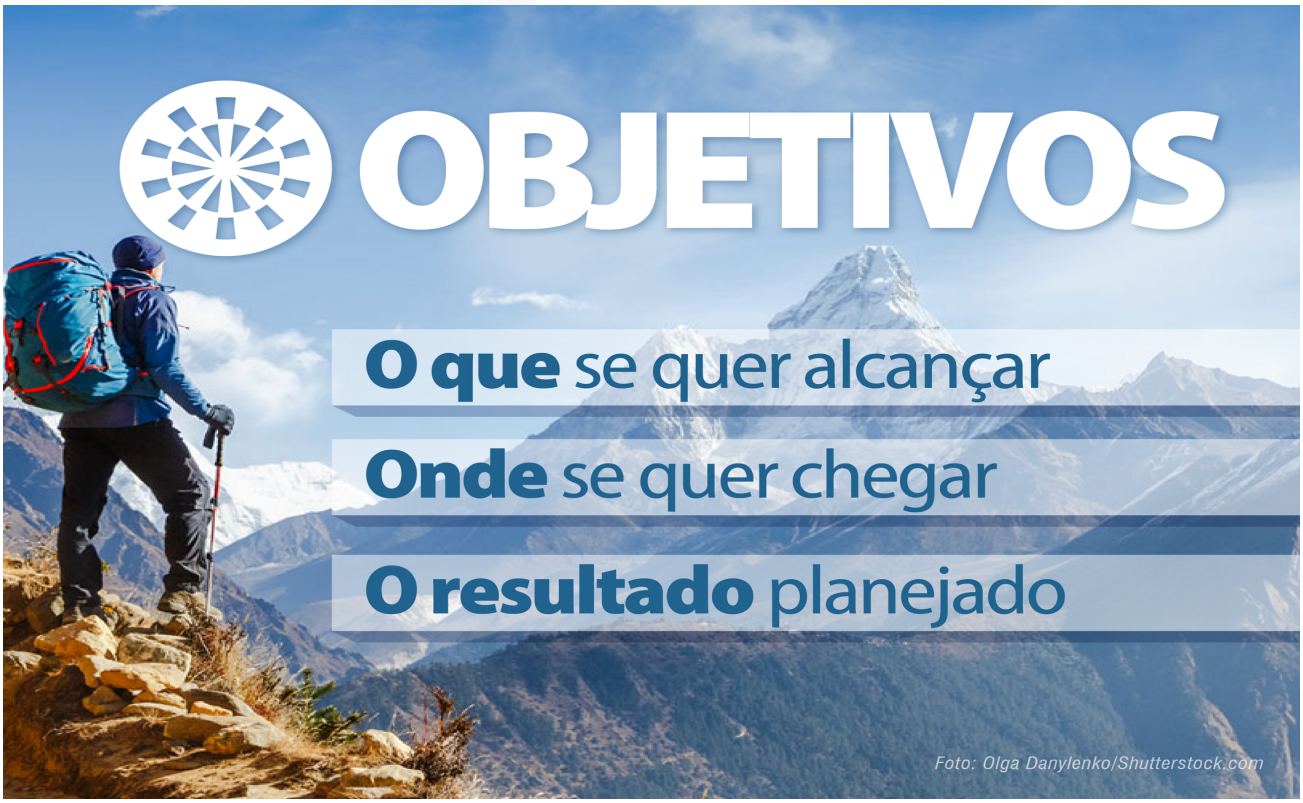
Figura 1: Conceitos de objetivos, riscos e controles

1.1.1 Objetivos

Para gerenciar risco é preciso de apenas uma coisa: ter objetivos definidos. Em linhas gerais, "objetivo" é um fim que se quer atingir, um propósito que se deseja alcançar. De acordo com o **COSO (Committee of Sponsoring Organizations of the Treadway Commission)** entidade mundialmente reconhecida em Gestão de Riscos e Controles Internos:

> *os objetivos são fixados no âmbito estratégico, estabelecendo-se uma base para os objetivos operacionais, de comunicações (relatórios) e de conformidade. Toda organização enfrenta uma variedade de riscos oriundos de fontes internas e externas, sendo o estabelecimento de objetivos, condição prévia para a identificação de eventos, avaliação de riscos e resposta a riscos* (COSO, 2006).

Figura 2: Definição de objetivos



A definição de objetivos faz parte de nossas vidas, seja no âmbito pessoal, profissional ou nas relações sociais. Quando você planeja comprar uma casa, um carro, fazer uma faculdade, se casar, ter filhos, você está definindo objetivos. Mesmo que não o faça de maneira formal, escrita ou sistematizada. Acontece naturalmente.

Assim como as pessoas, organizações do setor público possuem objetivos, com a diferença de que costumam ser declarados, definidos e detalhados formalmente, em vários níveis, primeiro na Constituição, depois em leis, regulamentos, planos estratégicos, táticos e operacionais. Esses objetivos se desdobram em indicadores e metas, que representam o caminho e o destino que a organização percorre e persegue para atingir suas finalidades.

O objetivo primordial, entretanto, é um só: entregar valor à sociedade, promovendo o interesse público. Infelizmente, nem sempre isso é lembrado com a frequência e a intensidade merecida.

O Ministério do Planejamento recomenda que uma gestão pública de excelência contemple a formulação e implementação da estratégia, pensando o futuro de modo integrado ao processo decisório (BRASIL, 2014).

Para o TCU, toda organização deve formular suas estratégias a partir de sua visão de futuro, da sua missão institucional e da análise dos ambientes interno e externo.

As estratégias devem ser desdobradas em planos de ação. E faz parte do processo acompanhar a implementação dos planos, "*oferecendo os meios necessários ao alcance dos objetivos institucionais e à maximização dos resultados"* (Brasil, 2014).

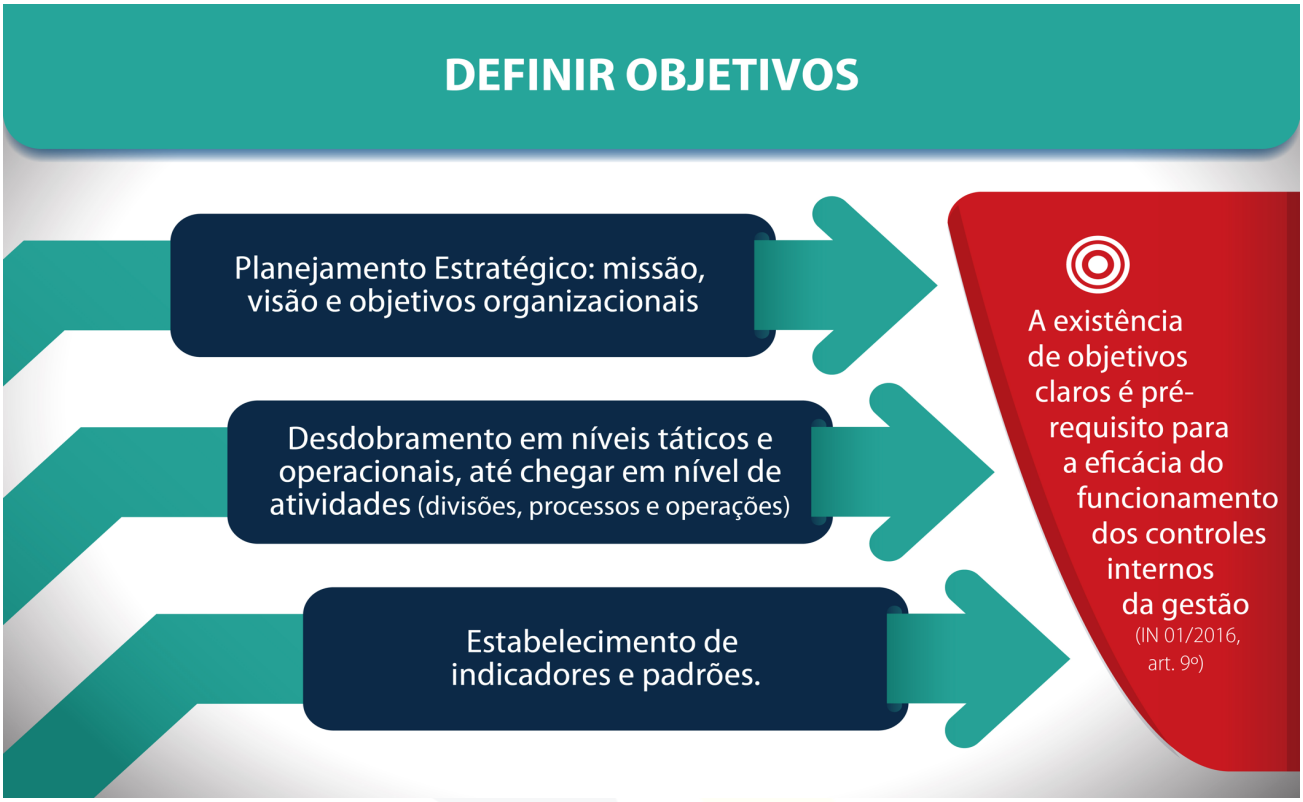
Nesse sentido, toda organização deve ter clareza de seus objetivos mais elevados. Assim, todos os colaboradores podem visualizar a contribuição dos resultados de seu trabalho para o resultado organizacional, bem como compreender de que forma ações de gestão de riscos, tomadas localmente, podem contribuir para a mitigação de riscos-chave em nível de entidade.

É buscando a excelência em cada pequena parte da engrenagem da organização que se garante o cumprimento da missão para a qual ela existe.

Quando os objetivos das áreas são estabelecidos de modo a maximizar suas contribuições para o resultado organizacional, pode-se dizer que conhecer os objetivos e prioridades da unidade em que se trabalha é tão ou mais importante do que estar informado sobre os objetivos estratégicos da organização.

Dessa forma, as entidades devem definir objetivos, podendo adotar as seguintes ações:

Figura 3: Ações na definição dos objetivos



Além disso, a organização deve acompanhar o cumprimento dos objetivos, dos indicadores, das metas e dos resultados alcançados, com medidas de aperfeiçoamento eventualmente estabelecidas para a melhoria dos resultados.

Sobre o último ponto, é importante que a entidade divulgue os indicadores, metas e resultados esperados entre servidores, usuários do serviço público e sociedade em geral, de modo a propiciar o gerenciamento das ações implementadas e estimular o exercício do saudável e necessário controle social.

A jurisprudência do TCU é pacífica quanto a importância do planejamento estratégico (Acórdãos n.º 1.521/2003, 1.558/2003, 2.094/2004, 786/2006, 1.603/2008 e 2.585/2012, todos de Plenário).

Como exemplo, transcrevemos trecho do Acórdão nº 1.233/2012-TCU-Plenário:

(...) 9.1.1 em atenção Decreto-Lei nº 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos:

9.1.1.1 Elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

9.1.1.2 Aprovação, pela mais alta autoridade da organização, do plano estratégico institucional;

9.1.1.3 Desdobramento do plano estratégico pelas unidades executoras;

9.1.1.4 Divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.1.5 Acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.1.6 Divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado. (...)

Além da jurisprudência do TCU, diversos normativos estabelecem diretrizes para o planejamento estratégico e avaliação institucional, tais como a Resolução CNJ nº 198/2014 e o Decreto nº 7.133/2010.

Destaca-se, ainda, que o Tribunal de Contas do Estado de Mato Grosso – TCE/MT instituiu em 2012 o Programa de Desenvolvimento Institucional Integrado – PDI, com objetivo de disseminar a cultura de **Planejamento Estratégico** nos Jurisdicionados, por meio do fornecimento de ferramentas tecnológicas e orientação técnica das equipes municipais e estaduais, para a sua elaboração, execução, acompanhamento e avaliação, estimulando, assim, o desenvolvimento institucional e melhoria da qualidade dos serviços prestados pelas organizações públicas de Mato Grosso.

Como exemplos de objetivos em atividades específicas do setor público, podemos citar a licitação, que visa a isonomia, a proposta mais vantajosa e a promoção do desenvolvimento nacional sustentável (art. 3º da Lei nº 8.666/93).

Na alimentação escolar, o programa tem como objetivo promover o crescimento, desenvolvimento, aprendizagem, melhoraria do rendimento escolar e formação de práticas alimentares saudáveis nos alunos. Não se trata, portanto, de “fornecer comida aos alunos”.

Já a assistência farmacêutica, preza pelo uso racional dos medicamentos, levando a melhor qualidade de vida. Veja que o objetivo não é simplesmente “entregar remédio ao cidadão”. Vai muito além disso.

Mas conhecer os objetivos, onde se quer chegar, embora fundamental, não garante o sucesso da empreitada. É o primeiro passo. Para que os resultados apareçam é preciso que haja execução adequada, com o devido acompanhamento e gerenciamentos dos riscos que podem impactar os objetivos.

Riscos, o que é isso? É sobre esse assunto que vamos tratar no próximo tópico.

1.1.2 Riscos

Na obra "*Desafio aos Deuses: a fascinante história do risco*", Bernstein (1997) destaca o fator que distingue a pré-história dos tempos modernos. Para o autor, não é o progresso da ciência, nem a tecnologia, nem o capitalismo ou a democracia. A verdadeira diferença estaria na **capacidade de administrar os riscos**.

> *A ideia revolucionária que define a fronteira entre os tempos modernos e o passado é o **domínio do risco**: a noção que o futuro é mais que um capricho dos deuses e de que homens e mulheres não são passivos ante a natureza. Até os seres humanos descobrirem como transpor essa fronteira, o futuro era um espelho do passado ou o domínio obscuro de oráculos e adivinhos que detinham o monopólio sobre o conhecimento dos eventos previstos.*
> (Bernstein, 1997, grifos nossos)

Para Bernstein, economista e professor consagrado de Harvard, ao compreender o risco, medi-lo e avaliar suas consequências, o homem converteu o ato de correr riscos em um dos **principais catalisadores** que impelem a sociedade ocidental moderna.

RISCO: OPÇÃO OU DESTINO?

A palavra "risco" deriva do italiano *risicare*, que significa "ousar". Nesse contexto, risco é uma opção e não um destino (Bernstein, 1997).

Sem domínio da teoria das probabilidades e outros instrumentos de gestão do risco, os engenheiros jamais teriam projetado grandes pontes, os lares ainda seriam aquecidos por lareiras ou fogareiros, as usinas elétricas não existiriam, não haveria aviões e as viagens espaciais seriam apenas um sonho.

Sem os seguros em suas múltiplas variedades, a morte do pai de família reduziria os filhos jovens à penúria ou caridade, a assistência médica seria possível a um número reduzido de pessoas e somente os ricos teriam casa própria. Se os agricultores não pudessem vender suas safras a um preço estabelecido antes da colheita, produziriam muito menos alimento (Bernstein, 1997).

Conviver com o risco é um velho dilema da sociedade: "Proteger-se contra todos os riscos é impossível, porque qualquer oportunidade invariavelmente acarreta riscos." É o que afirma Aaron Wildavsky (1979, p.32):

> *O risco é uma precondição essencial para o desenvolvimento humano; se parássemos de assumir riscos, inovações técnicas e sociais necessárias para solucionar muitos dos problemas mundiais desapareceriam. De fato, muitos dos riscos existentes na sociedade moderna resultam de benefícios gerados por inovações sociais e tecnológicas. Por outro lado, a imprudência insensata também não é uma boa ideia. Em vez disso, precisamos definir um caminho intermediário no qual o acaso – com*

suas incertezas e ambiguidades inerentes – seja levado em consideração de maneira objetiva, racional e eficiente.

Em 1921, o economista Frank Knight observou, de forma pioneira, que risco e incerteza são manifestações da aleatoriedade, associadas a situações de escolha. Diferenciava incerteza mensurável, o risco propriamente dito, da incerteza não mensurável (Bergamini Junior, 2005). Essa distinção é fundamental na tomada de decisões sob condições de incerteza: nem toda incerteza merece tratamento.

Assim, *riscos* são *eventos incertos*, ocorridos na prática da operação das organizações e que impactam seus objetivos, e *não qualquer coisa que pode acontecer ou dar errado*.

Podem ser destacados como riscos no setor público situações como falta de medicamentos, falhas nos serviços prestados, diminuição do crescimento econômico, demanda de serviço maior que a oferta, atraso nos cronogramas dos projetos, queda na arrecadação, descontinuidade administrativa, restrição indevida de uma licitação, pagamento por serviços não prestados, desvios de recursos, sobrepreço, superfaturamento, conluio entre licitantes, fraudes, evasão escolar, etc. Eventos incertos, porém mensuráveis, que merecem tratamento.

Por outro lado, eventos de ocorrência improvável, ainda que possível, como tsunamis, terremotos, guerras, atentados terroristas e epidemias, devem ser foco de técnicas com melhor poder preditivo e não objeto específico de gerenciamento de riscos.

Com base nessa perspectiva, estabeleceu-se uma definição formal para risco. Para a ISO 31000/2018, por exemplo, "risco é o efeito da incerteza nos objetivos".

No Brasil, o Tribunal de Contas da União definiu risco como "a possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades" (Art. 1º, V, da Instrução Normativa TCU nº 63/2010).

RISCO é a possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos (COSO, 2006).

Esse conceito é muito similar ao adotado na Instrução Normativa Conjunta CGU/MP nº 01/2016, trocando-se "algo" por "evento" e "consequências" por "impactos".

Figura 4: Definição normativa de risco

Ficou fácil perceber que os riscos permeiam toda a nossa vida e os enfrentamos o tempo todo, em qualquer atividade na vida pessoal, profissional ou no dia a dia das organizações. Não dá para viver sem riscos. O desafio é lidar com os riscos de forma consciente, sistemática e equilibrada.

E qual é a principal classificação de risco definida pelos modelos de referência?

1.1.2.1 Classificação de Riscos

Para o modelo de referência COSO ERM (Gerenciamento de Riscos Corporativos), há dois tipos de riscos: **inerente** e **residual**.

Risco inerente é o que existe independentemente de controles para sua mitigação. Residual é o risco que permanece após a resposta da administração (COSO, 2006).

A figura a seguir exemplifica muito bem essa classificação:

Figura 5: Classificação do risco

Fonte: Elaboração própria

O entendimento conceitual dessa classificação é fundamental para o adequado gerenciamento de riscos. Quando se deseja medir a efetividade da estrutura de controle existente, realiza-se a avaliação do risco inerente e residual, permitindo a identificação de possíveis falhas ou excessos na estrutura de controles internos – por exemplo, se existem muitos ou dispendiosos controles para mitigar um risco que inerentemente já é baixo.

É o caso de uma organização que decida investir pesado para mitigar o risco de segurança de pessoas, bens e informações. Para isso, ela decide contratar diversos postos de vigilância armada, investe em porta giratória com detector de metal, catracas, instala circuito interno de TV por todo o prédio.

Entretanto, se poucas pessoas visitam essa organização, se a entidade não trabalha com informações sigilosas ou possui bens de grande valor, o risco de violação da segurança é muito baixo

e os controles instituídos podem estar em excesso, representando desperdício de tempo e recursos. Uma adequada gestão de riscos resultará na eliminação de controles desnecessários, sem expor a organização a riscos indesejados.

Imagine que em *Pantanal do Norte* há um depósito de bens inservíveis. Coisa que ninguém mais usa e ninguém teve tempo ou disposição para se desfazer. Digamos que todo esse patrimônio seja avaliado em R$ 1 mil. Agora imagine que se decida contratar vigilância ininterrupta do depósito, para proteger os bens. E que para isso sejam gastos R$ 10 mil por mês.

O que você diria desse controle, em relação ao risco? O que um cidadão, se soubesse disso, diria do uso do dinheiro suado que ele investiu no governo municipal? Se você fosse o dono de uma empresa e o seu gerente tomasse essa decisão, como você reagiria ao destino que o seu dinheiro está tomando?

Se você parou para refletir sobre isso, deve estar entendendo porque estamos chamando este curso de "gestão de riscos". Controlar bem não é o mesmo que controlar muito.

Outra situação que justifica medir a efetividade da estrutura de controle existente ocorre quando o controle implementado não está funcionando efetivamente para mitigar determinado risco priorizado. Nesse caso, a organização precisa aprimorar ou implementar novos controles, pois o controle existente não está cumprindo seu papel de reduzir o risco.

Imagine que aquele depósito agora passou a abrigar medicamentos. O estoque ali dentro vale R$ 1 milhão. E há apenas uma câmera de vigilância, cujo gravador está estragado, servindo de proteção a esse patrimônio.

E agora, como você se sentiria em relação aos riscos? Protegido? Confortável? Preocupado? Desesperado? Bem-vindo ao mundo da gestão de riscos.

E já que estamos falando em controles internos, vamos conhecer as principais definições apresentadas para esse tema?

1.1.3 Controles Internos

Controle interno é qualquer medida instituída intencionalmente para modificar o risco. Na vida pessoal, por exemplo, adotamos diversos controles. Para evitar atrasos, utilizamos o despertador para acordar. Para não errar o caminho ou se perder, usamos o GPS. Ao atravessar a rua, olhamos para os lados. Ser atropelado é um risco ao seu grande objetivo de continuar vivo e ser feliz. Mesmo inconscientemente, de modo intuitivo, até por reflexo ou por hábito, adotamos controles para mitigar riscos.

Essas ações instituídas para evitar que os riscos se materializem ou para mitigar seus efeitos é o que chamamos de controle interno.

Para o *Instituto Americano de Contadores Públicos Certificados*, por meio de Relatório Especial da Comissão de Procedimentos de Auditoria, controle interno é definido como:

> *o plano da organização e todos os métodos e medidas coordenados, aplicados a uma empresa, a fim de proteger seus bens, conferir a exatidão e a fidelidade de seus dados contábeis, promover a eficiência e estimular a obediência às diretrizes administrativas estabelecidas.*

Com a publicação do Modelo COSO I – Controle Interno – Estrutura Integrada, em 1992, o nível de abrangência dos controles internos foi ampliado, constituindo um processo, implementado pela alta administração, envolvendo diretores, gerentes e funcionários, com a finalidade de prover razoável garantia quanto à realização dos objetivos, nas seguintes categorias:

i) conceder efetividade e eficiência às operações;

ii) obter confiabilidade no processo de comunicação, especialmente por meio das demonstrações contábeis; e

iii) assegurar a conformidade com as leis e os regulamentos.

Na mesma linha, as Diretrizes Internacionais para as Normas de Controle Interno do Setor Público, adotaram definição similar:

> *Controle Interno é um processo integrado efetuado pela direção e corpo de funcionários, estruturado para enfrentar os riscos e fornecer razoável segurança de que na consecução da missão da entidade os seguintes objetivos gerais serão alcançados: - execução ordenada, ética, econômica, eficiente e eficaz das operações; - cumprimento das obrigações de accountability; - cumprimento das leis e regulamentos aplicáveis; - salvaguarda dos recursos para evitar perdas, mau uso e dano.* (INTOSAI, 2004)

De igual modo, em suas Normas de Auditoria, o TCU reviu sua definição de Controle Interno, adotando a seguinte:

> ***processo efetuado pela administração e por todo o corpo funcional**, **integrado** ao processo de gestão **em todas as áreas e todos os níveis** de órgãos e entidades públicos, estruturado **para enfrentar riscos e fornecer razoável segurança** de que, na consecução da missão, dos objetivos e das metas institucionais, os princípios constitucionais da administração pública serão obedecidos e os seguintes objetivos gerais de controle serão atendidos:*
>
> *- eficiência, eficácia e efetividade operacional, mediante execução ordenada, ética e econômica das operações;*
>
> *- integridade e confiabilidade da informação produzida e sua disponibilidade para a tomada de decisões e para o cumprimento de obrigações de accountability;*
>
> *- conformidade com leis e regulamentos aplicáveis, incluindo normas, políticas,*

programas, planos e procedimentos de governo e da própria instituição;

- adequada salvaguarda e proteção de bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

Ainda está muito teórico. Dá para dar um exemplo? Vamos lá.

Suponha que a prefeitura de Pantanal do Norte tenha realizado licitação a fim de adquirir medicamentos para distribuição à população. As atividades desenvolvidas seriam as seguintes:

Figura 6: Etapas de um processo de aquisição de medicamentos

Etapa 01 – Prefeitura faz pregão para registro de preços de medicamentos. Ao final, vencedores assinam a Ata de Registro de Preços com as condições pré-definidas.

Etapa 02 – Para repor os estoques, o **farmacêutico,** responsável pelo Almoxarifado Central, envia memorando à Secretaria de Saúde, encarregada pelo gerenciamento da Ata, com a relação de produtos necessários.

Etapa 03 –- Servidor responsável pelo gerenciamento da Ata envia "Ordem de Fornecimento" ou "Nota de Empenho" para o fornecedor, com a quantidade pretendida e condições de entrega.

Etapa 04 – Fornecedor envia os medicamentos demandados, sendo recebidos por comissão de servidores designados para a atividade. Após conferência de quantidades, especificações, marca, validade e outros fatores, comissão "atesta" o recebimento, mediante carimbo e assinatura na Nota Fiscal.

Etapa 05 – Fornecedor encaminha Nota Fiscal atestada à Secretaria de Saúde. Com a requisição, ordem de fornecimento, empenho e nota fiscal, abre-se um processo de pagamento. Consulta-se a regularidade fiscal da empresa e anexa-se o resultado ao processo de pagamento.

Etapa 06 – Se tudo estiver bem, o pagamento é autorizado pelo gestor financeiro e pelo ordenador de despesa, emitindo a ordem de pagamento para quitação da obrigação.

Com esse exemplo, vamos agora explicar cada parte da definição de controles internos.

PROCESSO INTEGRADO

O controle interno não é apenas um documento, uma norma, um sistema, um registro, um fato ou circunstância isolada. É um conjunto de ações interligadas que permeiam todas as atividades, todas operações, de modo contínuo e coerente (Brasil, 2012).

Diversos procedimentos integrados de controle foram executados em nosso exemplo, dos quais podemos destacar: a solicitação pelo almoxarifado central; a notificação da empresa para entrega dos medicamentos; o recebimento dos produtos pela comissão, conferindo as condições de entrega; a conferência da regularidade fiscal e processamento do pagamento.

EXECUTADO POR PESSOAS

Controle interno não se refere apenas a implantar manual de políticas e procedimentos, sistemas e formulários, mas diz respeito, principalmente, às pessoas e às ações que elas tomam em cada nível da organização para executar suas tarefas. Nenhum manual, checklist ou sistema informatizado substitui as pessoas (Brasil, 2012).

No exemplo, quem emite a demanda (etapa 2), notifica o fornecedor (etapa 3), recebe os produtos (etapa 4) e efetua o pagamento (etapa 6) são servidores da prefeitura. Dessa forma, todos em uma organização executam controles internos, implicando que esses controles são diretamente afetados pela natureza humana.

AUXILIA O ALCANCE DOS OBJETIVOS

Já vimos que controles internos são conduzidos para atingir objetivos em uma ou mais categorias – estratégico, operacional, comunicação e conformidade, podendo ser objetivos fixados para toda a organização ou estabelecidos para atividades, processos ou operações específicas.

Em nosso exemplo, os controles internos auxiliam, dentre outros, os seguintes objetivos da atividade de aquisição de medicamentos:

a) Assegurar que as demandas sejam elaboradas após estudos técnicos preliminares e analisadas e aprovadas pela autoridade competente;

b) Garantir que o fornecedor tenha sido selecionado, respeitando a isonomia e a proposta mais vantajosa;

c) Permitir que o pedido de compra seja adequado às necessidades;

d) Garantir que o fornecedor atenda ao pedido de compra no tempo e conforme as condições esperadas; e

e) Assegurar que o fornecedor receba o pagamento no prazo acordado, desde que tenha cumprido suas obrigações.

OFERECE SEGURANÇA RAZOÁVEL

O controle interno é capaz de proporcionar segurança razoável, mas nunca absoluta, para a estrutura de governança e alta administração de uma entidade governamental. Não importa quão bem planejado ou executado seja, o controle interno não pode dar segurança ilimitada à organização, em relação ao alcance dos objetivos e a mitigação de todos os riscos existentes nas atividades (Brasil, 2012).

A nova definição adotada pelo TCU, alinhada ao conceito do COSO e INTOSAI, apresenta alguns elementos fundamentais para o controle interno, mencionando tanto a "segurança razoável" quanto a consecução dos objetivos.

A segurança razoável reflete a noção sobre a incerteza e os riscos futuros que não podem ser previstos e controlados de forma absoluta. Existem fatores que estão fora do controle ou da influência da organização e que podem afetar sua capacidade de alcançar os objetivos.

As limitações decorrem também do julgamento humano, passível de erro ou engano; ninguém é capaz de prever, com exatidão, o futuro; a administração lida com incertezas que, nem sempre, estão sob seu domínio; controles podem ser suprimidos por agentes mal-intencionados, geralmente em conluio; gestores, com objetivos obscuros, podem anular controles; descuido, cansaço físico, distração.

Essas limitações impedem que a alta administração, servidores e sociedade em geral tenham certeza absoluta sobre o alcance dos objetivos (Brasil, 2012).

Um exemplo bem claro disso aconteceu com a Petrobras. Mesmo tendo um dos mais elevados níveis de governança, a operação Lava Jato, iniciada em 2014, revelou fraquezas materiais que evidenciaram que os controles internos sobre os relatórios financeiros não foram efetivos, levando a empresa de auditoria *PricewaterhouseCoopers* (PwC) a se recusar a referendar o Balanço Patrimonial da Companhia referente ao ano de 2014.

Dessa forma, para implementar controles internos em uma organização é preciso **primeiro estabelecer objetivos, identificar e avaliar os riscos e tratá-los,** definindo quais devem ser modificados por alguma forma de **controle.**

Essa trinca "objetivo, risco e controle fica mais fácil de entender com uma imagem:

Figura 7: Relação entre objetivos, riscos e controles

Se você ainda tem dúvidas de que esse negócio de controles internos é importante, que tal saber que uma pesquisa sobre *a fraude no Brasil,* realizada pela KPMG em 2009, constatou que, para os empresários do setor privado, o que mais facilita a fraude são sistemas de controles internos insuficientes. Os mesmos empresários acham que a vacina para a fraude é melhorar os controles internos.

Figura 7: Medidas indicadas para evitar a fraude

Agora que conhecemos a trindade de objetivo, risco e controle, está na hora de conceituar a mistura.

1.1.4 Gestão de Riscos

Existem duas maneiras de lidar com riscos: ser surpreendido por eventos que podem impactar adversamente o alcance dos objetivos da organização e então reagir a eles, o que caracteriza a cultura de "apagar incêndios"; ou antecipar-se a eles, adotando medidas conscientes que mantenham ou reduzam a probabilidade ou o impacto dos eventos nos objetivos. Apenas a segunda maneira pode ser chamada de gestão de riscos (TCU, 2018).

Qualquer organização, seja ela pública ou privada, existe para atender às necessidades e expectativas das partes interessadas, ou seja, todas as pessoas afetadas, direta ou indiretamente, pelas atividades da organização.

No caso do setor público, atender expectativas de servidores públicos, organizações públicas, instituições privadas, cidadãos, grupos de interesse, associações e a sociedade como um todo visa aprimorar relações de qualidade e assegurar o desenvolvimento da organização.

Todas as organizações enfrentam incertezas e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza, assim como definir como essa incerteza pode interferir no esforço para gerar valor às partes interessadas (COSO, 2006).

A gestão de riscos corporativos diz respeito aos riscos e às oportunidades de criar ou preservar valor, e é definida pelo COSO da seguinte forma:

> *O gerenciamento de riscos corporativos é o processo conduzido em uma organização pelo Conselho de Administração, pela diretoria executiva e pelos demais funcionários, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetar a referida organização, e administrar os riscos para mantê-los compatíveis com o seu apetite a risco e possibilitar garantia razoável de cumprimento dos objetivos da entidade* (COSO, 2006).

Para a INTOSAI, lidar com as incertezas é fundamental para prestar serviços de qualidade:

> *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. (INTOSAI, 2007).

Na esteira dessas definições legais, a gestão de risco, em qualquer dos modelos adotados nos setores público e privado, nacional e internacional (COSO ERM, ISO 31000/2018), é abordagem que privilegia o alcance de resultados.

Ao buscar-se o gerenciamento dos riscos por meio de controles internos adequados, proporcionais aos riscos, o efeito será maior segurança de que os resultados serão atingidos, o que significa maior eficácia da atuação do gestor governamental.

Aumentar a segurança das operações, reduzir incertezas, ampliar a chance de atingir os resultados é, sobretudo, combater o desperdício, seja de esforços, recursos, dinheiro ou tempo. Menos desperdício representa mais entrega para a sociedade.

A gestão de riscos contribui para a boa governança corporativa ao aumentar a chance de que os resultados pretendidos sejam atingidos. De fato, o processo de gestão de riscos desenvolve o ambiente de controle, o qual, por sua vez, fornece maior garantia de que os objetivos organizacionais sejam alcançados dentro de um grau aceitável de risco residual (KNIGHT, 2003).

Além disso, baseado em experiências globais no mercado de gestão de projetos, a gestão adequada dos riscos pode reduzir em até 20% os custos de um projeto (Mulcahy, 2010).

Segundo a ISO 31000/2018, a gestão de riscos pode ser aplicada a toda uma organização, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos.

Em alguns países, a gestão de riscos já é prática consolidada no setor público há bastante tempo. A Secretaria do Tesouro do Canadá adotou oficialmente modelo de gestão de riscos em 2001, o qual vinha sendo a referência na administração direta daquele país. Em 2010, promoveu revisão ampla do tema, e editou novos documentos de referência (*Framework for the Management of Risk*), mas mantendo a continuidade da adoção da gestão de riscos no setor público canadense (Acórdão TCU nº 2467/2013 – Plenário).

O Reino Unido também tem adotado gestão de riscos no setor público há alguns anos, por meio da ferramenta voltada para a avaliação da gestão de risco nos diversos setores do governo (*Risk Management assessment framework: a tool for departments*).

Nos EUA, o Escritório de Accountability Governamental publicou a Ferramenta de Gestão e Avaliação de Controle Interno (GAO, 2001), com o objetivo de auxiliar os órgãos governamentais daquele país a manter e implementar um controle interno efetivo e, quando necessário, ajudá-los a

determinar o que, onde e como melhorias podem ser implementadas. Embora seja voltado para controle interno, esta é uma das principais formas de gerenciar riscos (Brasil, 2013). Entidades como o Banco Mundial, BID e Intosai adotam o modelo COSO como referencial para gestão de riscos.

No Brasil, até maio de 2016 não havia aplicação de uma abordagem de controles internos de forma estruturada, sistemática e disciplinada.

Seguindo recomendações do TCU, a CGU e o Ministério do Planejamento determinaram uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança, por meio da edição da Instrução Normativa Conjunta CGU/MP nº 01/2016, definindo que o modelo de avaliação de controles internos e gestão de riscos a ser implementado na Administração Pública Federal terá como base os princípios e a estrutura estabelecidos pelo COSO 2013. Nessa mesma linha é o Decreto Federal nº 9.203/2017, que estabelece a política de governança no Poder Executivo Federal.

A IN CGU/MP nº 01/2016 exigiu que cada órgão e entidade do Poder Executivo federal instituísse, até maio de 2017, sua própria política de gestão de riscos.

Também foi determinada a criação de comitê de governança, riscos e controles em cada organização federal.

Esse comitê deve ser composto pelo dirigente máximo e pelos gestores das unidades a ele diretamente subordinados, ou seja, pela alta administração da organização. A obrigatoriedade de se constituir um comitê de governança decorre também do Decreto Federal nº 9.203/2017.

Esse comitê deve ser responsável por: aprovar a política de gestão de riscos; institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos; promover o desenvolvimento contínuo dos agentes públicos; e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos.

Embora essa normatização seja de aplicação obrigatória apenas ao Poder Executivo federal, nada impede que estados e municípios e outras instâncias governamentais passem a dispor de um modelo referencial para implantação e avaliação de gestão de riscos e controles internos em suas unidades. Basta os dirigentes se convencerem que isso é uma medida relevante para melhorar os resultados e modernização das práticas e ferramentas de controle interno.

Aliás, foi o que aconteceu no Distrito Federal, com o Decreto nº 37.302, de 29 de abril de 2016, estabelecendo os modelos de boas práticas gerenciais em Gestão de Riscos e Controle Interno na Administração Pública distrital.

Em Pernambuco, o Decreto nº 46.855, de 7 de dezembro de 2018 instituiu a política de governança da administração pública estadual.

Outros estados, como Rondônia, Minas Gerais, Goiás e Ceará têm criado legislação própria, buscando instilar nas estruturas de governo locais as diretrizes da boa governança, gestão de riscos e

cultura da integridade, o que demonstra a tendência de crescimento e generalização desses conceitos na gestão pública brasileira.

Entretanto, o caminho para a excelência ainda é longo. Em 2013, o TCU (Acórdão 2467/2013-Plenário), avaliou o nível de maturidade da gestão de riscos nas empresas estatais e agências reguladoras federais. O objetivo era construir e divulgar indicador que estimulasse o aperfeiçoamento da gestão de riscos no setor público e que fornecesse subsídios para planejamento das suas ações de controle.

Como resultado, o levantamento permitiu identificar o índice de maturidade da gestão de riscos das entidades da Administração Federal Indireta.

Mesmo o setor financeiro, que tem o risco como essência do seu negócio, não andava tão bem, alcançando apenas 65% de maturidade em gestão de riscos.

E se a coisa andava fraca para as estatais e agências reguladoras em 2013, cinco anos depois vamos encontrar as universidades federais em situação ainda menos avançada. Pesquisando 60 instituições em junho de 2018, Bruno Affonso apontou que 24% delas ainda não tinham instituído o Comitê de Governança, Riscos e Controles previsto na Instrução Normativa Conjunta MP/CGU nº 01/2016. E apenas 38% tinham implantado Política de Gestão de Riscos. O autor concluiu que apenas 15% das universidades federais haviam cumprido a norma na forma e no prazo estabelecidos. (AFFONSO, 2018)

Esses diagnósticos evidenciam que a gestão de riscos ainda é muito incipiente na Administração Pública brasileira, havendo necessidade de aperfeiçoamento, fato que possibilitará benefícios para a sociedade em geral, tanto em termos de melhorias qualitativas nos serviços públicos prestados aos cidadãos quanto na garantia da boa e regular aplicação dos recursos públicos.

Foi pensando nisso que o controlador-geral de *Pantanal do Norte*, João Coruja, insistiu tanto para que o prefeito Paulo Capivara entendesse os conceitos básicos de objetivo, risco e controle e o poder que a sua gestão apropriada tem de ampliar as chances de sucesso das políticas públicas.

Lendo os manuais do TCU, a norma da CGU, os livros de referência no tema, João Coruja primeiro se convenceu que o risco é uma variável fundamental na equação de qualquer empreendimento. Ignorado, acontece e causa danos o tempo todo. E quem está despreparado costuma culpar o destino, o azar, chamar de fatalidade, acaso ou tragédia o que, na verdade, em muitos casos, poderia ser evitado ou pelo menos ter seus efeitos reduzidos.

Depois que se convenceu, o controlador municipal adotou outra postura em sua rotina de trabalho. Suas auditorias, planos, projetos e atividades passaram a ser executados com o olhar voltado, primeiro, para os objetivos, os resultados esperados e as ações necessárias para seu atingimento. Em paralelo, João mantinha o olho vivo nos eventos incertos que poderiam atrapalhar, impedir ou dificultar os objetivos. E quais desses eventos valia a pena controlar. E quais era melhor aceitar.

João percebeu que aquilo ajudava bastante a melhorar seus resultados e os da sua equipe. Ele se antecipava a armadilhas, tomava medidas preventivas e preparava alguns mecanismos compensatórios em caso de os riscos acontecerem. E, principalmente, avaliava sistematicamente o

que controlar e o que deixar para lá, porque sabia que os controles devem ser proporcionais ao risco.

Com essa cultura de riscos incorporada à sua própria rotina, João saiu tentando disseminar a ideia na prefeitura. E para isso ele usou o que aprendeu antes: os modelos de referência para implementação da gestão de riscos nas organizações. **Que tal conhecê-los também?**

1.1.5 Modelos de Referência

Os "modelos de referência" são mundialmente conhecidos como estruturas, padrões ou frameworks. Estas nomenclaturas são comumente utilizadas para fazer alusão às construções teóricas realizadas por diversas organizações internacionais, sobretudo na área de gestão de riscos e controles internos que as entidades podem adotar para implantação e avaliação de gestão de riscos.

Esses frameworks de gestão de riscos consolidam um conjunto de técnicas, atividades e boas práticas que efetivamente contribuem para o processo de gestão de riscos, contemplando as atividades de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos corporativos.

Como já explicado, a principal abordagem no tratamento dos riscos decorre da implantação de controles internos. Entretanto, se essa implantação não observar as orientações presentes nos modelos de referência consagrados mundialmente, as organizações podem estruturar um conjunto de controles puramente formais, burocráticos, cujo custo econômico e social seja evidentemente superior ao risco, passando a impressão da existência de um eficaz sistema de gerenciamento de riscos, quando, na verdade, não garante efetivamente os benefícios esperados, resultando, assim, em desperdício de tempo e recursos.

Dessa forma, os principais modelos de referência em gestão de riscos utilizados pelas organizações são: ISO 31000/2018 e COSO ERM (Enterprise Risk Management).

Apresentamos a seguir as principais características de cada modelo:

1.1.5.1 ISO 31000/2018

A abordagem descrita na ISO 31000 propõe-se a fornecer princípios e diretrizes para gerenciar qualquer forma de risco de uma maneira sistemática, transparente e confiável, dentro de qualquer escopo e contexto.

A norma indica que convém que o processo de gestão de riscos seja parte integrante da gestão, seja incorporado na cultura e nas práticas da organização, e seja adaptado aos processos de

negócio.

Dentre outros benefícios, o referencial tem por finalidade ajudar a organização a aumentar a probabilidade de atingir seus objetivos, melhorar sua governança e estabelecer base confiável para tomada de decisões.

Em 2018, a ISO 31000 foi atualizada. A revisão da norma mantém a mesma arquitetura de gestão de riscos (princípios, estrutura e processo) da norma de 2009, mas oferece um guia mais claro, mais curto e mais conciso que ajudará as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

1.1.5.2 COSO ERM

Trata-se do modelo de gestão de riscos predominante no cenário corporativo internacional, especialmente na América do Norte. COSO é a sigla de *Committee of Sponsoring Organizations da National Commission* (Comitê das Organizações Patrocinadoras da Comissão Treadway), também conhecida como *Treadway Comission*.

Criada em 1985 nos Estados Unidos, constitui uma entidade do setor privado, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros por meio de éticas profissionais, implementação de controles internos e governança corporativa (Brasil, 2013).

Em 1992, o COSO publicou a obra Controle Interno – Estrutura Integrada (*Internal Control – Integrated Framework*), que obteve grande aceitação em todo o mundo e tem sido aplicada amplamente. É reconhecida como uma estrutura modelo para desenvolvimento, implementação e condução do controle interno, bem como para a avaliação de sua eficácia.

Embora tenha havido ampla adesão ao modelo COSO I, isso não foi suficiente para evitar escândalos econômico-financeiros e contábeis envolvendo entidades de grande porte. O COSO, então, intensificou a preocupação com gerenciamento de riscos – em decorrência de uma série de escândalos e quebras de negócios de grande repercussão – e o desenvolvimento de uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o próprio gerenciamento de riscos. O resultado foi a publicação, em 2004, do modelo Gerenciamento de Riscos Corporativos – Estrutura Integrada, também conhecida como COSO ERM ou COSO II (Brasil, 2013).

Incorporando e ampliando o COSO I, o modelo de gerenciamento de riscos corporativos do COSO ERM definiu quatro categorias de objetivos, que seriam comuns a praticamente todas as organizações, e identificou oito componentes como partes integrantes da estrutura de controles internos e do gerenciamento de riscos.

Segundo o COSO ERM (2004), o modelo é orientado para alcançar os objetivos de uma organização, que podem ser divididos nas seguintes categorias:

a) **estratégicos** – relacionados à sobrevivência, continuidade e sustentabilidade da organização. Consistem em metas gerais, alinhadas e dando suporte à missão da organização;

b) **operações** – diz respeito à eficácia e eficiência na utilização dos recursos;

c) **comunicação** – confiabilidade de relatórios, isto é, da informação produzida e sua disponibilidade para a tomada de decisão e para fins de prestação de contas; e

d) **conformidade** – cumprimento de leis e regulamentos aplicáveis à organização.

Por sua vez, os oito **componentes do gerenciamento de riscos** corporativos considerados indispensáveis para sua eficácia são:

1) **ambiente interno** – representa o tom da organização e fornece a base pela qual os riscos são identificados e abordados. Inclui a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do ambiente que os cerca;

2) **fixação de objetivos** – os objetivos devem ser fixados antes que a administração identifique os eventos em potencial que poderão afetar o alcance destes. Os objetivos estabelecidos devem estar alinhados com a missão da organização e precisam ser compatíveis com seu apetite a risco;

3) **identificação de eventos** – os eventos em potencial, oriundos de fontes internas ou externas, que podem afetar a realização dos objetivos da organização, devem ser identificados. Durante o processo de identificação os eventos poderão ser classificados em riscos, oportunidades, ou ambos;

4) **avaliação de riscos** – os riscos identificados devem ser analisados com o fim de determinar o modo como serão administrados e, em seguida, associados aos objetivos que podem afetar. Os riscos são avaliados considerando seus efeitos inerentes ou residuais, assim como sua probabilidade e seu impacto;

5) **resposta a risco** – as respostas aos riscos podem ser: evitar, aceitar, reduzir/mitigar ou transferir/compartilhar. Compete à administração selecionar o conjunto de ações destinadas a alinhar os riscos à tolerância e ao apetite a risco da organização;

6) **atividades de controle** – consistem em políticas e procedimentos estabelecidos e implementados com vistas a assegurar que as respostas aos riscos selecionadas pela administração sejam executadas

com eficácia;

7) **informações e comunicações** – a comunicação é considerada eficaz quando flui na organização em todas as direções e quando os funcionários recebem informações claras sobre suas funções e responsabilidades. A forma e tempestividade com que informações relevantes são identificadas, colhidas e comunicadas permite que os agentes cumpram com suas atribuições. Assim, para identificar, avaliar e oferecer resposta ao risco, a organização necessita de informações em todos os níveis hierárquicos.

8) **monitoramento** – a integridade do processo de gerenciamento de riscos deve ser monitorada para que as modificações necessárias sejam realizadas e a organização possa reagir ativamente segundo as circunstâncias. O monitoramento pode ser feito por meio de atividades gerenciais contínuas, por avaliações independentes, ou por uma combinação de ambos.

Esses oito componentes são **inter-relacionados** e estão **integrados ao processo de gestão**, ou seja, estão voltados para o alcance dos resultados da organização. Para o COSO (2004), existe um relacionamento direto entre os objetivos da organização e os componentes do gerenciamento de riscos corporativos, que representam o que é necessário para a concretização desses objetivos.

Esse relacionamento é apresentado no "cubo de COSO":

Figura 10: Cubo de COSO

Fonte: COSO ERM

Os objetivos da organização são representados pelas colunas verticais, enquanto os oito

componentes são mostrados nas linhas horizontais.

Na terceira dimensão aparecem as unidades da organização, demonstrando que o gerenciamento de riscos abrange todos os níveis organizacionais (em nível setorial: divisão, unidade, departamento, projeto, seção ou em nível de atividades: macroprocessos, processos, subprocessos, atividades).

Em 2017, essa estrutura do modelo de referência COSO ERM foi atualizada, estabelecendo uma ligação mais clara e direta entre o gerenciamento de riscos corporativos e as expectativas das partes relacionadas.

Além disso, posiciona o risco no contexto da performance da organização e não apenas como foco de um raciocínio isolado.

A nova estrutura ficou da seguinte forma:

Figura 11: Framework COSO ERM Revisado - 2017

Fonte: COSO ERM – Enterprise Risk Management, integrating with Strategy and Performance Executive Summary, 2017

Como já foi comentado, a Instrução Normativa CGU/MP nº 01/2016 definiu que o modelo de gestão de riscos a ser implementado na Administração Pública Federal tem os mesmos componentes do modelo COSO (art. 16).

Além disso, o TCU vem recomendando aos órgãos e entidades da Administração Pública Federal que realizem ações visando ao aprimoramento dos controles internos da gestão, com a devida avaliação de riscos, para adoção de procedimentos de forma a minimizar os problemas enfrentados, utilizando como referência modelos consagrados, a exemplo do COSO ERM, com vistas a mitigar os impactos negativos de eventos potencialmente danosos à sua gestão (Acórdão nº 2.754/2014 – Plenário).

Nesse mesmo sentido são os Acórdãos nº 7.128/2013 e 2.429/2015, ambos da 2ª Câmara, nº 1.062/2014, 4.599/2016 e 5.169/2016, todos da 1ª Câmara.

Considerando a ampla utilização do modelo conceitual COSO ERM no setor público em

nível nacional e internacional, passaremos a demonstrar como o município hipotético de *Pantanal do Norte* implementou o gerenciamento de riscos com base nas prescrições desse consagrado referencial, levando em conta, também, os elementos relevantes de outros modelos de referência, a exemplo da ISO 31000/2018, tendo em vista a complementariedade de ambos os *frameworks*.

ASSISTA AO VÍDEO

Na biblioteca do curso encontra-se disponível vídeo resumo do Caso Enron, um dos maiores escândalos financeiros e que motivou o foco em riscos do modelo de referência COSO. Veja também um vídeo sobre riscos do gestor, que existem mesmo que o gestor não esteja consciente. E um terceiro vídeo que mostra que não existe bola de cristal para gerenciar riscos, mas é possível fazer isso de modo inteligente. Confiram!

SAIBA MAIS

Para saber mais sobre a pesquisa realizada pela KPMG sobre "A Fraude no Brasil", leia o artigo completo disponível na biblioteca do curso. Além desse artigo, encontram-se disponíveis também as obras "10 passos para a Gestão de Riscos" e "Referencial Básico de Gestão de Riscos", ambas lançadas pelo TCU.

SÍNTESE DA AULA

Nesta aula, vimos que risco é a possibilidade de algo acontecer e afetar negativamente o alcance dos objetivos de uma organização e que o papel do controle interno é oferecer razoável segurança contra esses riscos, prevenindo sua ocorrência ou detectando sua materialização.

Vimos que para implementar controles internos em uma organização é preciso, primeiro, estabelecer **objetivos** (da entidade ou das atividades, processos, operações, setores, etc.), identificar e avaliar os **riscos** e tratá-los, definindo quais devem ser modificados por alguma forma de **controle**, evidenciando uma clara relação entre objetivos, riscos e controles.

Também aprendemos que a gestão de riscos contribui para a boa governança corporativa ao aumentar a chance de que os resultados pretendidos sejam atingidos, o que significa maior eficácia da atuação do gestor governamental.

A organização pública que incorpora a gestão de riscos à sua cultura e às suas atividades obtém aumentos graduais na sua capacidade de gerar, preservar ou entregar valor público com desempenho otimizado, o que se traduz em melhores resultados na implementação de políticas públicas e na prestação de serviços de interesse da sociedade.

Finalmente, estudamos os modelos de referência mais reconhecidos internacionalmente para a gestão de riscos em uma organização. Percebemos que esses modelos são o ponto de partida para auxiliar na definição de estruturas customizadas para o estabelecimento de controles internos, evitando que se adote um conjunto descoordenado de controles, que não garantam efetivamente os benefícios esperados.

Na próxima aula, aprofundaremos nosso conhecimento sobre como fazer gestão de riscos na prática, conhecendo o passo a passo para se implementar essa ferramenta gerencial moderna no setor público.