INSTITUTO SERZEDELLO CORRÊA

Página de Liderança

MELHORES PRÁTICAS DE GERENCIAMENTO DE RISCOS

Autor:

Renata Miranda Passos Camargo

CAMARGO, Renata Miranda Parros. Melhores práticas de gerenciamento de risco. **Página de Liderança**, Brasília, 24 mai 2013. Disponível em: << http:// portal2.tcu.gov.br/ portal/page/portal/TCU/educacao_ corporativa/lideranca>>. Acesso em: (data da consulta)

Melhores práticas de gerencimento de riscos

Não há um perfil ideal de líder, mas estilos que são mais adequados às diferentes situações vivenciadas. Você já ouviu falar em Liderança Situacional? Como esse modelo de liderança pode apoiar a sua atuação como líder gestor em diferentes situações? Além disso, como esse modelo pode ajudá-lo a promover o desenvolvimento de sua equipe? A literatura não é unânime acerca da definição do conceito de "riscos", tendo em vista que este pode ser utilizado em vários contextos. Existem autores que o percebem com agregado de riscos, conjunto de riscos identificados e que podem requerer algum tipo de tratamento; como risco residual, que permanece após o tratamento dos demais; como riscos não sistemáticos; ou, ainda, como risco de perseguir de estratégias ineficazes (DOFF, 2008). No contexto deste artigo, todavia, adotaremos a definição do ISO/IEC Guide 73, para o qual, risco é uma combinação de probabilidade de ocorrência de eventos e suas consequências.

O *Institute of Risk Management* (THEIRM, 2002) define "gestão de riscos" como o processo mediante o qual as organizações endereçam, metodicamente, os riscos associados a suas atividades, visando o alcance de objetivos e a sustentabilidade de benefícios.

Em pesquisa realizada na base de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, em março de 2012, foi possível evidenciar (Figura 1) o aumento na quantidade de publicações sobre gestão de riscos corporativos (*corporate risk management),* sobretudo a partir do início do século XXI, período marcado por: escândalos (ex.: Enron, WorldCom); exposição excessiva a riscos; concessão exagerada de créditos, em especial a tomadores que não ofereciam garantias suficientes de pagamento; problemas no *subprime* americano; e, mais recentemente, crises de dívidas soberanas europeias.

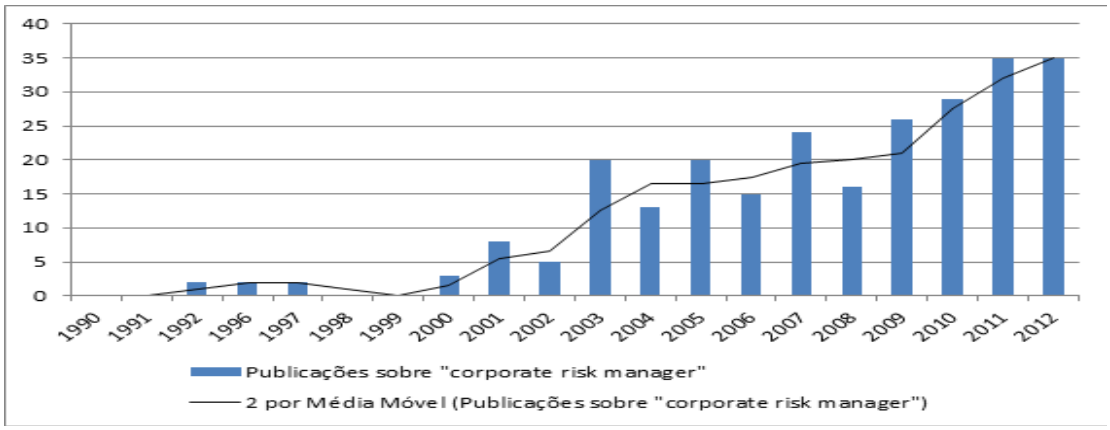

Figura 1: Publicações científicas sobre "*corporate risk*" disponíveis no portal da CAPES. Fonte: a autora

Modelos de gerenciamento de riscos

Nesse contexto, marcado por crises financeiras mundiais, foram desenvolvidos e aprimorados *frameworks* e padrões focados, entre outras coisas, no aprimoramento de técnicas de gerenciamento de riscos. De acordo com o IT Governance Institute – ITGI (2009), dentre os modelos mais aceitos estão: o ARMS:2002; o COSO-ERM:2004; o Risk IT Framwork:2009; e a ISO/FDIS 31000:2009.

O ARMS:2002 é um modelo britânico, criado pela *Association of Insurance and Risk Managers* (AIRMIC) e pelo *National Forum for Risk Management* in the Public Sector (ALARM), que tem por objetivo: estabelecer uma terminologia comum; propor processos, definir estruturas organizacionais necessária e explicitar objetivos a serem alcançados com o gerenciamento de riscos (THEIRM, 2012). De acordo com este modelo, os riscos organizacionais podem resultar de fatores internos e externos e podem ser de diversas categorias: financeiro (ex. crédito, câmbio, taxas); estratégico (ex.: mudanças de mercado, demanda de clientes, modelo industrial); operacional (ex.: regulações, cultura, composição do board); e *hazard* (contratos, eventos naturais, fornecedores, ambiente). O processo de gerenciamento de riscos, neste modelo, consiste: na análise de objetos estratégicos da organização, no diagnóstico de riscos (análise – identificação, descrição e estimativa – e avaliação), no relato de riscos (ameaças e oportunidades), na tomada de decisão, no tratamento de riscos, no relato de riscos residuais e no monitoramento.

Com o objetivo de prover orientações sobre controles internos, gestão de riscos empresariais (*Enterprise Risk Management* – ERM) e prover estudos sobre fraudes, o *Committee of Sponsoring Organizations* - COSO desenvolveu um conjunto de publicações e recomendações direcionadas a companhias públicas e auditores independentes. Na perspectiva do COSO (2012), o valor de um investimento é maximizado quando: o administrador estabelece objetivos que visam a um equilíbrio ótimo entre crescimento, retorno esperado e riscos relacionados; e entrega recursos de forma eficiente e efetiva. Neste sentido, o gerenciamento de riscos deve se preocupar com: o alinhamento entre estratégia e apetite a risco; a melhoria nas decisões de resposta a riscos; a redução de surpresas e perdas operacionais; a identificação e gestão de riscos múltiplos envolvendo uma ou mais empresas; o aproveitamento de oportunidades.

No que se referem às técnicas para gerenciamento de riscos, o COSO (2012) sugere a análise combinada de três dimensões: objetivos organizacionais (estratégias, operações, relatórios e conformidade), estrutura organizacional e componentes de gerenciamento de riscos. Especificamente, no que tange a estes últimos, orienta: a análise do ambiente interno, o estabelecimento de objetivos, a identificação de eventos, o diagnóstico de risco, a resposta a risco, o controle, a geração e a comunicação de informação, e o monitoramento de riscos.

O *framework* de risco de TI, concebido no âmbito do *Information Technology Governance Institute* - ITGI, estabelece ligações com outros modelos, como COSO-ERM, AS/NZS 4360:2004 e ISO 31000, e sugere a observância de seis princípios gerais para o gerenciamento de riscos: conexão com os objetivos da organização; alinhamento do gerenciamento de riscos de TI com o gerenciamento de riscos de negócio; balanceamento da relação entre custos e benefícios; comunicação franca e aberta; definição de responsabilidades; tratamento contínuo de riscos de TI (ITGI, 2009). Em termos processuais, este modelo está estruturado em três domínios: governança, avaliação e resposta a riscos (ITGI, 2009). O primeiro engloba atividades relacionadas: ao estabelecimento e manutenção de visão comum de riscos; à integração com o gerenciamento de riscos empresariais (ERM); e à transformação da consciência sobre riscos em decisões de negócio. O segundo abrange a coleta de dados, a análise de riscos e a manutenção de perfil de riscos. Por fim, o terceiro, se preocupa com a reação a eventos, com a articulação de riscos e, mais especificamente, com a gestão de riscos.

O *International Organization for Standardization* publicou em 2009 as normas: ISO/FDIS 31000, que trata de princípios e orientações para gerenciamento de risco; e ISO 31010, que apresenta técnicas para

assessment (identificação, análise e avaliação) de riscos. O processo de gerenciamento de riscos, segundo este *framework*, envolve a aplicação sistemática de políticas, procedimentos e técnicas com vistas a: comunicar e consultar partes interessadas; estabelecer contextos (parâmetros internos e externos a serem levados em consideração); identificar fontes, eventos, causas e consequências potenciais de riscos; compreender e analisar a natureza e o nível de risco (incluindo estimativas); determinar e avaliar se o risco, ou sua magnitude, é aceitável/tolerável (tendo por base critérios estabelecidos); tratar e alterar riscos (mediante, por exemplo, a potencialização e/ou aproveitamento de oportunidade, a redução da probabilidade de ocorrência, a remoção da fonte, a transferência para outras partes interessadas); monitorar riscos, controles, processos e modelos (mediante a checagem, supervisão e observação crítica); e, por fim, revisá-los (quanto à adequação e a efetividade frente aos problemas potenciais e alcance de objetivos) (ISO, 2009).

De acordo como o ITGI (2012), os modelos supracitados têm em comum: a orientação a negócio; o provimento de uma estrutura de processo que inicia na identificação de riscos e culmina no monitoramento e *feedback*; a cobertura de diversas opções de tratamento de risco; e a apresentação de uma visão abrangente sobre gerenciamento de riscos, não limitada à técnicas e a ferramentas.

Ohtoshi (2008) realizou um estudo comparativo entre as principais metodologias e ferramentas que servem como instrumento de avaliação de risco e podem ser utilizadas por instituições da Administração Pública Federal Brasileira. Resultou desse trabalho um inventário de metodologias, ferramentas e quadros comparativos que explicitam qualidades e benefícios potenciais de cada um desses instrumentos, no qual percebeu a existência de um movimento de convergência e integração de metodologias e ferramentas. Para ele o surgimento da sigla GRC (Governance, Risk and Compliance) e da integração destas práticas evidencia esse fenômeno. Ohtoshi (2008) percebeu, ainda, que a ISO vem gradativamente incorporando aos seus modelos elementos constantes de metodologias e modelos americanos, europeus e australianos.

Semelhante a este autor, também percebemos este movimento de síntese de práticas e modelos, não apenas no contexto restrito dos processos de gerenciamento de riscos, mas também no contexto dos modelos de governança. Diversas práticas indicadas em modelos de governança são na verdade reprodução ou especializações de práticas descritas em modelos internacionais de gerenciamento de risco, em especial dos descritos na ISO/FDIS 31000:2009 e no COSO I e II.

É perceptível a preocupação dos estudiosos da governança com processos e estruturas que remetem ao controle e, aparentemente, o gerenciamento de riscos e de controles internos surge neste cenário como um arcabouço metodológico, suficientemente estável e robusto, que pode contribuir para melhoria da governança, seja ela corporativa, aplicada ao setor público ou de TI.

Gerenciamento de riscos e controle externo

O Plano Estratégico do TCU explicita dois objetivos diretamente relacionados ao tema Gerenciamento de Riscos (GR): "atuar de forma seletiva e sistêmica em áreas de risco e relevância" e "intensificar ações que promovam a melhoria da gestão de riscos e de controles internos da Administração Pública". No primeiro objetivo o foco está na utilização de práticas de GR para orientar as ações de controle. No segundo, busca-se induzir a utilização de práticas de GR na administração pública.

Tendo em vista esses objetivos, é interessante que as unidades do TCU:

- incorporem elementos de GR em seus planos institucionais;
- formem grupos de trabalho multidisciplinares e multissetoriais para definir e coordenar a implantação de melhores práticas de GR no contexto do TCU;
- implantem, efetivamente, processos e soluções que apoiem a integração de práticas de GR em nível institucional;
- controlem, por meio de indicadores, a eficiência, a eficácia e a efetividade dos processos de GR e de soluções propostas para tratamento de riscos;
- levem em consideração os dados disponibilizados pelo processo de GR quando da execução de atividades de tomada de decisão;
- utilizem práticas de GR não apenas para aferir riscos intraorganizacionais, mas também identificar eventos e diagnosticar riscos existentes em suas clientelas;

- proponham respostas a riscos e comuniquem tempestivamente às partes interessadas acerca dos riscos identificados e respostas planejadas e/ou executadas;

- controlem a execução de atividades necessárias e mantenham um monitoramento próximo de riscos considerados críticos.

Por fim, considerando que o TCU está em vias de iniciar um diagnóstico de Gestão de Riscos na Administração Pública Federal é importante preparar a Casa não apenas para avaliar, mas também para adotar melhores práticas de gerenciamento de riscos. Para apoiar essa atividade foi construído e disponibilizado, na Página de Liderança do Portal Corporativo do TCU, um instrumento de trabalho que pode auxiliar a aplicação de práticas de gerenciamento de riscos no contexto do controle externo.

Referências

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS - AICPA. COSO enterprise risk management - integrated framework. 2004 . Disponível em <http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990015/PC-990015.jsp>. Acessado em 31 mar. 2012.

DOFF, René. Defining and measuring business risk in an economic-capital framework. The Journal of Risk Finance. vol. 9 Iss: 4, 2008. pp. 317 – 333.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE – ITGI. The risk IT framework. USA, Rolling Meadows: ISACA, 2009.

_____. A spotlight on ISACA's new framework, Risk-IT. Disponível em <http://www.theirm.org/events/documents/StevenBabb-7710.pdf>. Acessado em 05 mar. 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. International standard ISO/FDIS 31000:2009 - Risk management: principles and guidelines. 2009. Disponível em:

<http://www.iso.org/iso/catalogue_detail?csnumber=43170>. Acessado em: 05 abr. 2012.

OHTOSHI, H. O. Análise comparativa de metodologias de gestão e de análise de riscos sob a ótica da norma NBR-ISO/IEC 27005. Disponível em: <http://academic.googlecode.com/svn/trunk/academic_jobs/monografias07_08/Monografia_Paulo_Ohtoshi.pdf>. Acessado em: 29 set. 2012

THE INSTITUTE OF RISK MANAGEMENT - THEIRM. A risk management standard. 2002. Disponível em <http://www.theirm.org/publications/documents/ARMS_2002_IRM.pdf>. Acessado em 31 mar. 2012.