Reflexões sobre a gestão com o foco em risco – impacto nas auditorias públicas

O gerenciamento de riscos não trata de decisões futuras, mas sim do futuro das decisões que tomamos hoje.
Salles Júnior, Carlos Alberto Corrêa et al

Abrão Blumen
Bacharel em Ciências Contábeis pela Universidade de São Paulo, Especialista em Gestão de Negócios Governamentais – FIPE/USP e mestre em Administração pela Universidade São Marcos. Professor universitário e palestrante. Ex-diretor da Escola de Contas do TCMSP

Resumo: O presente artigo pretende oferecer reflexões sobre algumas ferramentas e estratégias ainda pouco utilizadas pelos auditores em seus trabalhos de campo, tendo como referência teórica e aplicada o levantamento de auditoria realizado pelo TCU em 2013 em entidades da administração indireta federal.

Palavras-chave: Risco. Controle Interno. Gestão de Riscos. Auditoria Pública.

Abstract: This article seeks to offer reflections on some tools and strategies are still little used by auditors in their field work, taking as a reference of theoretical and applied the survey of audit performed by TCU in 2013 in entities federal indirect.

Keywords: Risk. Internal Control. Risk Management. Public Audit.

1 Introdução

Peter L. Bernstein (1997), em sua extraordinária obra "Desafio aos Deuses – a fascinante história do risco", coloca de forma clara e unívoca a ideia revolucionária da fronteira entre o passado e os tempos modernos – "é o domínio do risco: a noção de que o futuro é mais do que um capricho dos deuses e de que homens e mulheres não são passivos ante a natureza".

No entanto, o que a história do risco (em seu enfoque probabilístico) tem a ver com o impacto na auditoria, seja privada ou pública?

2 A essência da administração segundo Peter Bernstein

A essência da administração, segundo Bernstein (1997), está em "maximizar as áreas onde temos certo controle sobre o resultado, enquanto minimizamos as áreas onde não temos absolutamente nenhum controle sobre o resultado e onde o **vínculo entre efeito e causa está oculto de nós**" (grifo nosso).

3 O caso Titanic

Os autores Alencar e Schmitz (2012), em um dos capítulos do seu livro, trouxeram à luz, ***sob o enfoque de gestão de riscos***, um dos casos mais controvertidos de desastre naval – o naufrágio do Titanic em 1912. Apontam os autores, por meio de levantamento de evidências documentais e notícias da época, que caso os responsáveis pela construção do navio bem como o capitão e os oficiais a bordo tivessem elaborado adequados planos de contenção e contingência desde o planejamento e durante o transcorrer da viagem, e estabelecido, tempestivamente, cursos de ação capazes de minimizar os riscos, poderiam até ter evitado o desastre. Concluem a análise do caso com a seguinte assertiva: "o que torna a análise de risco uma atividade ímpar em sua natureza mais íntima é o fato dela estar sempre ligada à incerteza sobre a ocorrência de um ou mais eventos que podem prejudicar as chances de sucesso de um projeto".

4 Lei Sarbanes-Oxley

A Lei Sarbanes-Oxley, lei federal americana, comumente chamada SOX, foi editada em 2002 tendo em vista os inúmeros escândalos financeiros e contábeis que afetaram fortemente a credibilidade e a transparência das informações, especialmente, as do mercado americano. A lei tem por escopo supervisionar, disciplinar e regulamentar a atuação das empresas abertas, conselhos de administração, comitês de auditoria e de auditoria independente.

Dentre um dos resultados mais importantes da edição da SOX, criou-se um Conselho, o *Public Company Accounting Oversight Board* (PCAOB), revogando os modelos, até então, de autorregulação, com o objetivo de supervisionar e disciplinar as empresas de auditoria externa bem como proteger os interesses dos investidores por informações mais fidedignas e acuradas. A SOX aplica-se igualmente às empresas não norte-americanas que emitam títulos no mercado de capitais nos EUA (conhecidos como *ADRs – american depositary receipts*).

Outros importantes aprimoramentos da SOX:

- ateste por auditores independentes da efetividade dos controles internos relacionados com a divulgação de informações contábeis e financeiras;
- vedação de certos tipos de serviços aos clientes auditados;
- estabelecimento de comitês de auditoria independentes;
- vedação de empréstimos pessoais a diretores ou executivos (incluindo as companhias subsidiárias);
- certificação dos relatórios financeiros emitidos pelos CEOs e CFOs (tornando-os responsáveis e solidários junto ao contador!);
- multas por desobediência à lei (incluindo detenção e penas severas), aplicadas pela SEC (U.S. Securities and Exchange Commission);
- proteção aos denunciantes de fraudes e irregularidades (criação de canais de denúncia);
- estabelecimento de padrões de auditoria, controle de qualidade, código de conduta e de ética corporativo;

- recomendação para adoção dos padrões de controle interno estabelecidos pelo *The Committee of Sponsoring Organizations* (COSO), criado em 1985.

Borgerth (2007) conclui que:

> [...] a Lei Sarbanes-Oxley é bastante abrangente. As empresas que já estão sujeitas a ela terão que rever todos os seus **sistemas de controles internos**, adaptar **sistemas de informação** para que forneçam maior detalhamento, implementar um senso de responsabilidade para cada nível de criação da informação final, adotar um **código de ética** e reformular seus **princípios de governança corporativa**. (grifos nossos).

5 Normas e diretrizes brasileiras no âmbito do Controle Interno/ Contabilidade, Governança e Gestão de Riscos

Em 2007 (por meio da Res. CFC 1103 de 28.09.07), é criado o Comitê Gestor da Convergência no Brasil, congregando entidades como o Conselho Federal de Contabilidade (CFC), o IBRACON (Instituto de Auditores Independentes), a CVM (Comissão de Valores Mobiliários) e o BACEN (Banco Central do Brasil), objetivando a *reforma contábil* e de *auditoria*, bem como o aprimoramento das práticas profissionais, culminando com a convergência das normas brasileiras aos padrões internacionais.

Especialmente importantes aos auditores afetos à avaliação do sistema de gerenciamento de riscos, as seguintes normas editadas pelo CFC:

NBC TA 265 – Comunicação das deficiências de Controle Interno;

NBC TA 330 – Resposta do auditor aos riscos avaliados;

NBC TA 530 – Amostragem em Auditoria.

Para o setor público, o CFC, aprova, em 2008, as Normas NBC T16.1 a 16.10 (em 2011, a NBC T16.11). Cumpre observar que a NBC T 16.6 foi alterada para NBC T16.6. R1(exclusão da Demonstração do Resultado Econômico e inclusão da Demonstração das Mutações do Patrimônio Líquido e Notas Explicativas pela Res. CFC 1437/13) – Demonstrações Contábeis.

Duas dessas normas são importantes ao auditor do setor público:

NBC T 16.8 – Controle Interno;

NBC T 16.11 – Informação de Custos do Setor Público.

O Conselho Federal de Contabilidade colocou em Audiência Pública (até 10.08.2016), a Minuta NBC TSP Estrutura conceitual para a elaboração e divulgação de informação contábil de propósito geral pelas entidades do setor público. Uma vez referendada a minuta, entendemos oportuno mencionar o inciso 1.8A pela sua abrangência de aplicabilidade:

> Aplicabilidade da Estrutura Conceitual e das NBC TSP
>
> [...]
>
> 1.8A A Estrutura Conceitual se aplica à elaboração e divulgação dos RCPG, estando compreendidos no conceito de entidades do setor público: os governos nacionais, estaduais, distritais e municipais, bem como seus respectivos Poderes (abrangidos os **Tribunais de Contas**, Defensorias e o Ministério Público), órgãos, secretarias, departamentos, agências, autarquias, fundações (instituídas e mantidas pelo poder público) e outras repartições públicas congêneres das administrações direta e indireta, além das empresas estatais dependentes (grifo nosso).

Encontra-se igualmente disponível no site do CFC o Manual das Normas Internacionais de Contabilidade para o Setor Público - IPSAS, editado em 2010 pelo IFAC (*International Federation of Accountants*) e traduzido para o portu-

guês, de extrema valia aos auditores públicos.

Nos últimos 10 a 15 anos, houve um crescimento exponencial de normas e regulamentos, resoluções, comunicados técnicos e diretrizes que orientam o exercício profissional dos contadores e auditores, tanto nas entidades privadas quanto nos entes públicos. Sem o objetivo de esgotar o assunto, destacamos como vitais ao conhecimento do auditor público:

1. Lei Complementar nº 101/2000 – Lei de Responsabilidade na gestão fiscal.
2. Guia de orientação para gerenciamento de riscos corporativos – IBGC, 2007.
3. Diretrizes para as Normas de Controle Interno do Setor Público – Intosai/TCE -BA (2007).
4. Normas de Auditoria Governamental (NAGs) aplicáveis ao Controle Externo – IRB/Atricon (2010).
5. Lei nº 12.527/2011 – Lei de Acesso à Informação.
6. Lei nº 12.846/2013 – Lei anticorrupção.
7. Decreto nº 8.420 de 18.03.2015 – regulamenta a Lei no 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências.
8. Portaria CGU nº 750 de 20.04.2016 – institui o Programa de Integridade da Controladoria Geral da União.
9. Instrução Normativa Conjunta CGU/MP nº001 de 10.05.2016 – dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

6 Governança

O Código das Melhores Práticas de Governança Corporativa do IBGC (2015) assim conceitua Governança:

> Governança corporativa é o ***sistema*** pelo qual as empresas e demais organizações são ***dirigidas***, ***monitoradas*** e incentivadas, envolvendo os ***relacionamentos*** entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o ***valor econômico de longo prazo*** da organização, facilitando seu ***acesso a recursos*** e contribuindo para a qualidade da gestão da organização, sua ***longevidade*** e o bem comum. (grifos nossos).

Analisando o conceito emitido pelo IBGC, abordaremos com maior minudência o significado de cada um dos itens grifados no texto acima, oportunizando ao auditor uma maior reflexão dos objetivos do Código:

Sistema: é um conjunto de partes coordenadas/interligadas que concorrem para a realização de um conjunto de objetivos. O modelo físico universalmente utilizado para representar um sistema é o da entrada (*input*) de recursos, materiais, equipamentos e informações; seguido pelo processamento/operação/execução e saída (*output*) de relatórios, planilhas preenchidas, pesquisas, ensaios/testes realizados, produtos e serviços entregues.

Direção da sociedade: Gestão/Administração/Alta Direção, estrutura de comando e liderança, políticas e diretrizes organizacionais, filosofia para o gerenciamento de riscos, código de ética.

Monitoração: processo de acompanhamento da gestão por meio de indicadores/métricas, índices de maturidade do sistema de segurança informacional e tratamento analítico e estatístico dos índices econômico-financeiro-sociais.

Relacionamento com os *stakeholders* (partes interessadas): relação com a sociedade/comunidade/contribuintes/clientes e prestadores

de serviços/fornecedores, com as agências de fomento, bancos e outros órgãos públicos, como tribunais de contas, judiciário e legislativo, criação de portais da transparência (e-governo) e adesão ao modelo de contratualização de resultados (contratos de gestão).

Aumento de valor econômico de longo prazo: entrega de mais valor à sociedade (EVA)/aumento do resultado econômico, investimentos em infraestrutura e logística, elaboração do balanço ambiental e social, replicação de externalidades positivas etc.

Facilitação ao acesso a recursos: ampliação de fontes de recursos, linhas de empréstimos (*funding*) em organismos internacionais, emissão de títulos governamentais, cogestão/parcerias público-privadas, linhas de fomento, consórcios públicos etc.

Longevidade (continuidade estratégica/tática/operacional): plano de metas, responsabilidades social, política e ambiental, programas de desenvolvimento e capacitação profissional, investimento em formação de mão de obra e qualificação profissional, valorização do capital intelectual, inclusão digital, aprimoramento da gestão pública, gestão da transparência, projetos de médio e longo prazo etc.

Valmor Slomski, pioneiro na aplicação do conceito de governança no setor público e elaboração do balanço do resultado econômico, expõe em seu livro (2005), os princípios que inspiram o código das melhores práticas de governança corporativa no setor público:

a) **Transparência** (*disclosure*): mais que a obrigação de informar, a administração deve pretender o "desejo de informar". A comunicação não deve restringir-se às informações econômico-financeiras, mas deve alcançar os fatores/ativos intangíveis que conduzem à criação de valor à ação pública.
b) **Equidade** (*fairness*): tratamento justo e igualitário de todos os grupos, englobando clientes, colaboradores, credores, fornecedores entre outros (todos os *stakeholders* em sua acepção mais ampla).
c) ***Accountability***: também tratada como prestação de contas com ampla responsabilização dos gestores. Os cidadãos desejam, e necessitam, saber se as verbas do governo estão sendo devidamente administradas e em conformidade com a legislação e as regulamentações. Desejam e necessitam também saber se as organizações, programas e serviços governamentais estão atingindo seus objetivos e se estas organizações, programas e serviços estão funcionando de forma econômica e eficiente. O autor nos chama atenção para algo pouco discutido em relatórios de gestão pública: "fazer com que o cidadão possa fazer comparações com resultados privados e, assim, sentir-se confortável ao ver que a gestão pública está sendo eficiente no gasto dos recursos públicos".
d) **Responsabilidade corporativa**: incorporação de considerações de ordem social e ambiental na definição de negócios e operações. Trata-se de uma visão ampla da estratégia da organização ao cuidar de todos os relacionamentos com a comunidade em que a sociedade atua. Incluem-se neste item todas as preocupações com a qualificação do trabalho/trabalhador, estímulo ao desenvolvimento técnico-científico, melhoria da qualidade de vida, ações educativas, assistenciais e defesa do meio ambiente. Acrescentaria às ponderações do autor, o estímulo às ações associativas no modelo de cooperativismo/associativismo e fomento ao emprego formal (empreendedorismo).

7 *Compliance* e Riscos

O termo *compliance* origina-se do verbo em inglês *to comply*, que significa cumprir, execu-

tar, satisfazer, realizar algo imposto. *Compliance* é o ato de cumprir, de estar em conformidade e executar regulamentos internos e externos, impostos às atividades da instituição, buscando mitigar o risco atrelado à reputação, imagem e ao regulatório/legal.

As autoras Célia Lima e Juliana de Fátima (2014) comentam como o *compliance* ainda é implementado com dificuldade e resistência cultural nas organizações, repercutindo em diversos desafios que deverão ser vencidos como: "(a) – abrangência da função de *compliance*; (b) – compreensão da importância do *compliance*; (c) – dificuldade para diferenciar os conceitos de *compliance*, controles internos e auditoria e finalmente, (d) – barreiras impostas pelas diversas áreas das organizações para implantar programas de *compliance*."

8 Controle Interno e o modelo COSO

8.1 Controle Interno

Os autores Gil, Arima e Nakamura (2013) assim se expressam com relação à gestão de riscos e auditoria de gestão do controle interno:

O **risco** como entidade associada às mudanças do controle interno tem o evento contingente (decisão e demais eventos organizacionais futuros associados) como foco.

A gestão e a auditoria da gestão são realizadas com o sistema de controle interno, ou seja, o conjunto de documentação que descreve e determina o exercício do processo/produto das diversas linhas de negócio e áreas organizacionais de natureza:

1 – normas e regulamentos organizacionais;
2 – planos com estratégias organizacionais definidas;
3 – documentação de sistemas de informações com TI;
4 – contratos com organizações parceiras;
5 – documentação de projetos organizacionais;
6 – legislação federal, estadual, municipal;
7 – regulamentações profissionais.

A gestão e a operação organizacional necessitam de comportamento profissional de excelência de seus executivos, gestores e chefes com foco no:

- Amplo conhecimento do controle interno a cada momento histórico do negócio; e
- Cálculo do risco para a hierarquia com a escolha das decisões e demais contingências inerentes ao processo/produto do negócio.

A metodologia de gestão deve ser estruturada e ter inserida a formalização do processo / produto organizacional objeto do controle interno com as práticas e os resultados do exercício das atividades de linhas e áreas de negócio, contemplando as visões qualitativa e quantitativa de natureza:

1 – Visão Qualitativa.

- Formatar os recursos integrantes dos eventos organizacionais hierarquizados para efeito planejamento, execução e controle de seu ciclo de vida.
- Identificar causas e efeitos, como constatar ou especular a participação desses recursos prioritários em situações de falhas ou com necessidade de melhor desempenho, os quais serão objeto de decisão/ação/projeto para o alcance de melhores patamares tecnológicos funcionais do negócio.
- Classificar a lógica da gestão do evento organizacional e de seus recursos integrantes na perspectiva "4 E's; produtividade; segurança; regulamentações" com objetivo de tratar e alimentar o sistema de informações "Decisão" para efeito de comprovação da lógica para maior qualidade à gestão do negócio.

2 – Visão Quantitativa.

- Trabalhar o ciclo de vida de indicadores/métricas para *benchmark* do nível da quali-

dade das operações e benefícios do processo/produto organizacional entre áreas ou linhas de negócio no horizonte "passado/ presente/futuro".

- Apurar o risco da qualidade do negócio com o tratar a vertente "contingência; incerteza; risco" para maior garantia e melhor visão dos cenários futuros organizacionais pretendidos/ buscados.

8.2 COSO

O Tribunal de Contas do Estado de Mato Grosso, por meio da Resolução Normativa nº26/2014-TP, ao aprovar os requisitos e estrutura de referência do sistema de controle interno dos fiscalizados, assim se expressa em seus artigos 10 e 11, ao referendar a estrutura integrada de controle interno ao modelo COSO II:

> Art. 10. Aprovar os requisitos mínimos para a estruturação e o funcionamento dos sistemas de controle interno dos poderes executivos dos municípios matogrossenses, constantes do Anexo III desta Resolução, os quais serão considerados para fins de medição da meta 5.1. do Plano Estratégico 2012-2017 deste Tribunal (***Garantir o atendimento de 100% dos requisitos de controle interno de cada fiscalizado, até dezembro de 2017***).
>
> Parágrafo único. Além de observar os requisitos prescritos no Anexo III desta Resolução, o sistema de controle interno dos fiscalizados deve ser implementado em observância ao ***modelo de estrutura integrada de controle interno publicado pelo COSO*** (*Committee of Sponsoring Organizations of the Treadway Commission*), de forma a garantir a presença e o funcionamento de todos os seus elementos e componentes.
>
> Art. 11. Determinar aos Prefeitos Municipais que na implementação do sistema de controle interno do Poder Executivo devem ser atendidos 100% dos requisitos prescritos no Anexo III desta Resolução, os quais serão considerados para efeito de apreciação das respectivas contas anuais.
>
> Parágrafo único. Determinar aos Presidentes das Câmaras Municipais que, na implementação dos respectivos sistemas de controle interno, devem ser atendidos, no que couber, os requisitos a que se refere o *caput* deste artigo. (grifos nossos).

Em função das fraudes corporativas e escândalos financeiros, criou-se nos Estados Unidos, em 1975, uma Comissão Nacional independente (*National Commission on Fraudulent Financial Reporting*), agregando várias associações profissionais e com o objetivo explícito de aperfeiçoamento dos relatórios financeiros e dos sistemas de controle interno, sendo transformada, posteriormente, em Comitê (*The Comitee of Sponsoring Organization of the Treadway Commission – COSO*).

Em 1992, publica a estrutura (*framework*) de um modelo integrado de controle interno – COSO I, tornando-se referência mundial. Em 2004, amplia o modelo anterior e o transforma em COSO II – Gerenciamento de Riscos Corporativos – Estrutura Integrada, abordando de forma mais completa, a gestão de riscos.

O modelo COSO II abrange os seguintes tópicos: ambiente interno, fixação de objetivos, identificação de eventos, avaliação de riscos, resposta aos riscos, atividades de controle, informação e comunicação e monitoramento.

Cumpre observar as limitações descritas no próprio Manual do COSO/PWC (2007) sobre o gerenciamento de riscos corporativos, a saber:

> Para alguns observadores, o gerenciamento de riscos corporativos, como controles internos implantados, assegura que a organização não fracassará – isto é, ela sempre atingirá seus objetivos. Essa opinião é ***falaciosa***.
>
> Considerando as limitações do gerenciamento de riscos corporativos, três conceitos distintos devem ser reconhecidos:
>
> - Primeiro, o risco está relacionado ao futuro, o qual é intrinsecamente incerto.
> - Segundo, o gerenciamento de riscos cor-

porativos – mesmo que eficaz – opera em diferentes níveis com relação a diferentes objetivos. No caso de objetivos estratégicos e operacionais, o gerenciamento de riscos corporativos pode contribuir para assegurar que a administração e o conselho de administração em seu papel de supervisão estão oportunamente cientes apenas da evolução da organização no cumprimento desses objetivos. Mas não são capazes de fornecer nem uma garantia razoável de que as próprias metas serão atingidas.

- Terceiro, o gerenciamento de riscos corporativos não é capaz de oferecer uma garantia absoluta em relação a qualquer uma das categorias de objetivos (grifo nosso).

9 Gestão de Riscos

Em março de 2013, a Segep (Secretaria de Gestão Pública), em cooperação com os Ministérios das Relações Exteriores do Reino Unido e do Planejamento, Orçamento e Gestão do Brasil e o IFCI (Instituto para o fortalecimento das capacidades institucionais), lança o Guia de Orientação para o Gerenciamento de Riscos, baseado no documento "*The Orange Book Management of Risk - Principles and Concepts*" (Gerenciamento de Riscos – Princípios e Conceitos) produzido e publicado pelo *HM Treasury* do Governo Britânico.

A missão das organizações, segundo o Guia, é entregar serviços (ou produtos) de qualidade ao cidadão. Para tanto, o gerenciamento de riscos conduz à otimização na utilização dos recursos (menos custos e instituição de programas de contingenciamento e contenção de falhas operacionais), no planejamento mais adequado e integrado bem como no melhor gerenciamento dos programas de governo, melhorando a eficácia, a eficiência e a efetividade da gestão.

Em atenção à recente IN Conjunta CGU/MP nº001/2016, os órgãos e entidades do Poder Executivo Federal, num prazo de até 12 meses a contar da publicação da instrução, devem especificar em sua política de gestão de riscos (art.17), entre outras diretrizes, as seguintes, que destaco como pertinentes ao teor da presente reflexão:

> [...]
> c) como será **medido** o desempenho da gestão de riscos;
> [...]
> e) a utilização de **metodologia** e **ferramentas** de apoio à gestão de riscos ... (grifos nossos).
> Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado.
> Na mesma instrução, assevera que a política de gestão de riscos deve observar os seguintes princípios (art. 14):
> I – gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;
> II – estabelecimento de níveis de exposição a riscos adequados;
> III – estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;
> IV – utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico; e
> V – utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

Em seu art.16, propugna a utilização do *framework* COSO II (2004) na estruturação do modelo de gestão de riscos, abrangendo todos os seus oito componentes.

E, em seu art. 22, estabelece como devem ser geridos - governança, riscos e controles internos (a saber, o modelo GRC):.

> Art. 22. Riscos e controles internos devem ser geridos de forma integrada, objetivando o esta-

belecimento de um ambiente de controle e gestão de riscos que respeite os valores, interesses e expectativas da organização e dos agentes que a compõem e, também, o de todas as partes interessadas tendo o cidadão e a sociedade como principais vetores.

10 Governança, Risco e *Compliance* (GRC)

Pelo acrônimo GRC, compreende-se um modelo único e integrado de G (governança), R (risco) e C (*compliance*). No mercado encontram-se disponíveis aplicativos e sistemas informatizados, com abordagens holísticas e integradas de armazenamento, triagem, correlação e comunicação de informações, propiciando o mapeamento da organização de acordo com a sua política de governança e gestão de riscos bem como ajustando os controles ao fluxo de trabalho e rotinas organizacionais.

O objetivo principal com a implantação do GRC é garantir a *compliance* (conformidade) com as normas legais e procedimentais, por meio de auditorias contínuas[1], consolidando-se, assim, os padrões de operação dentro de um único modelo (plataforma operacional) e conciliando os conflitos de interesse que naturalmente emergem entre as diferentes áreas e processos da organização.

11 Apresentação do indicador de maturidade de gestão de riscos apurado no Levantamento de Auditoria relatado no Acórdão TCU 2.467 de 11.09.2013

Trataremos, nesta parte, do Acórdão do TCU e respectivo Relatório, emitido em 11.09.2013, pela Ministra Relatora Ana Arraes. O minucioso Relatório (30 páginas) cuida do levantamento de auditoria com o objetivo de elaborar um indicador que reflita a maturidade do sistema de controles internos e da gestão de riscos dos órgãos e entidades públicas (inserido no Programa Estratégico do TCU em 2012 - Plano de Ação TMS 10.1: Governança, gestão de riscos e controles internos).

O Relatório consagra o conceito de gestão de risco já anteriormente adotado:

> Riscos são eventos ou circunstâncias que têm potencial para comprometer, no todo ou em parte, a consecução dos objetivos ou dos resultados desejados. A gestão de riscos contribui para a boa governança corporativa ao aumentar a chance de que os resultados pretendidos sejam atingidos.

É importante destacar o que consta no quesito 8 do Relatório, uma afirmação que merece profunda reflexão dos órgãos fiscalizadores, no sentido de estimularem a implantação e examinarem mais a fundo, quando existentes, os programas de gestão de riscos dos entes públicos:

> 8. No Brasil, ***ainda não há um referencial que oriente a estruturação da gestão de riscos*** na administração pública federal. O mais próximo disso é o *Gespública*, que consiste em conjunto de orientações e parâmetros para avaliação da gestão, embora esse modelo de gestão não tenha enfoque específico para gerenciamento de riscos. (grifo nosso).

O levantamento de dados para a construção do indicador de gestão de riscos obedeceu, sucintamente, aos seguintes passos:

1. Treinamento da equipe ministrado por um consultor internacional (18 horas).
2. Identificação e análise de diversos modelos de gestão de riscos aplicáveis ao setor público (Secretaria do Tesouro do Reino Unido, COSO, ISO, Secretaria do Tesouro do Governo do Canadá, GAO, modelo de avaliação do Ministério do Planejamento – GES-

PUBLICA e o IGOV.TI elaborado pelo SEFTI).

3. Definição das dimensões da gestão de riscos incorporadas ao indicador em construção.
4. Definição de fatores matemáticos de ponderação para que as avaliações de cada dimensão pudessem ser expressas conjuntamente em um único número que representasse a maturidade organizacional da gestão de riscos, dentro de uma escala de avaliação. Utilizou-se, para tanto, a técnica de hierarquização de fatores denominada *Analytic Hierarchy Process (AHP)*.
5. Desenvolvimento do questionário eletrônico com questões avaliativas e aplicado a 66 entidades da administração indireta federal (incluindo autarquias, fundações, empresas públicas e sociedades de economia mista).
6. A análise de dados permitiu avaliar a maturidade da gestão de riscos nessas organizações.

11.1 Modelo adotado para avaliação da Gestão de Riscos e Controles Internos

Foi selecionado o modelo do Reino Unido – *Risk Management Assessment Framework: a Tool for Departments* (2009) como base conceitual da construção do indicador de gestão de riscos. Modelo derivado do EFQM – 2012, *The EFQM Excellence Model*, utilizado por mais de 30 mil organizações, especialmente, na Europa e estruturado em 7(sete) componentes: a) liderança; b) pessoas; c) política e estratégias para riscos; d) parcerias; e) processo de gestão de riscos; f) eficácia da gestão de riscos e g) resultados.

Optou-se, igualmente, por realizar pequenas adaptações no modelo do Reino Unido com a utilização do COSO, GRC e ISO 31.000/09 e dos demais modelos mencionados no corpo do Relatório. Na dimensão – Ambiente Interno – do COSO/GRC, foram englobadas as dimensões citadas do modelo do Reino Unido: Liderança, Políticas e Estratégias e Pessoas.

Finalmente, foi considerado importante incorporar as contribuições do Instrumento para Avaliação da Gestão Pública – ciclo 2010 e adotados os oito critérios em que o GESPÚBLICA se estrutura, com as pontuações máximas citadas entre parênteses, a saber: liderança (110 pontos), Estratégias e Planos (60 pontos), Cidadãos (60 pontos), Sociedade (60 pontos), Informações e Conhecimento (60 pontos), Pessoas (90 pontos), Processos (110 pontos) e Resultados (450 pontos).

11.2 Elaboração do Questionário Avaliativo

Para cada dimensão da gestão de riscos definida no modelo, a equipe formulou perguntas avaliativas, a partir do conteúdo dos documentos analisados. O teste piloto foi realizado na Eletronorte. Analisadas e incorporadas as sugestões e críticas, resultou um questionário com 64 perguntas (55 perguntas fechadas e 9 abertas) cobrindo 75 itens, reagrupadas agora em quatro dimensões: ambiente de gestão de riscos (englobando os subitens lideranças, políticas e estratégias e pessoas), processos de gestão de riscos, gestão de riscos em parcerias e resultados.

As perguntas fechadas (Ambiente, Parcerias e Resultados) foram construídas para serem respondidas em escala de concordância de cinco pontos (De 1 – discordo totalmente [...] ao extremo [...] 5 – concordo totalmente). Somente as duas perguntas que tratam da existência e composição de política de gestão de riscos tiveram respostas dicotômicas (sim/não).

Destacou-se, como fundamental, no relatório o seguinte aspecto: a importância

de que o dirigente máximo da entidade (ou outro membro da alta administração) reunisse pessoas que conhecessem bem a organização para debaterem e escolherem as respostas que melhor refletissem a situação da gestão de riscos na entidade.

11.3 Cálculo do Índice de Maturidade

Para a escala de 5 pontos (escala de concordância) utilizou-se a correspondência mostrada na tabela (1):

Tabela 1 – Critério de correspondência das escalas de cinco pontos para efeito de cálculo da maturidade em gestão de riscos

Ponto da Escala de Concordância	Pontuação correspondente
1	0
2	1
3	2
4	3
5	4

Fonte: Acórdão TCU 2467/13

Metodologia do Cálculo - citou-se no Relatório o seguinte exemplo prático. Caso a entidade obtivesse 40 pontos dos 76 pontos possíveis na dimensão Ambiente (dezenove perguntas, cada uma delas valendo até quatro pontos), então o índice de maturidade em Ambiente seria de, respectivamente, 52,6% (40/76 x 100 %).

Calculados os índices de maturidade nas quatro dimensões, aplicou-se a média ponderada com base nos seguintes pesos: Ambiente – 30%, Processos – 40%, Parcerias – 10% e Resultados – 20% (pesos selecionados utilizando a técnica AHP[2]). O índice global derivado desse cálculo permite classificar o nível de maturidade alcançado de acordo com a Tabela 2:

Tabela 2 – Níveis de maturidade organizacional em gestão de riscos segundo o índice apurado

Nível de maturidade	Índice apurado
Inicial	De 0% a 20%
Básico	De 20,1% a 40%
Intermediário	De 40,1% a 60%
Aprimorado	De 60,1% a 80%
Avançado	De 80,1% a 100%

Fonte: Acórdão TCU 2467/13

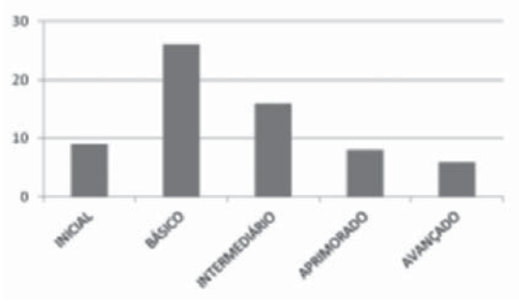
11.4 Avaliação da Gestão de Riscos na Administração Indireta

O Questionário foi encaminhado a 66 entidades da entidade indireta, obtendo-se um excelente retorno (65 respostas). Composição abrangida pelo levantamento: Autarquias (26), Fundação (2), Empresa Pública (20) e Sociedade de Economia Mista (17).

11.5 Resultados encontrados

Observando-se a distribuição das entidades participantes do levantamento, verifica-se que ***dois terços*** das organizações estão nos níveis básico e intermediário e que apenas 9% da amostra alcançou o nível avançado de maturidade de gestão de riscos (gráfico 1). (grifo nosso).

Gráfico 1 – Número de entidades segundo o nível de maturidade em gestão de riscos



Fonte: Acórdão TCU 2467/13

11.6 Oportunidades de Melhorias apontadas no Relatório do TCU

Para aquelas entidades públicas que se encontram no nível ***básico*** de maturidade:

a) obter o envolvimento ativo da alta administração com a institucionalização da gestão de riscos;
b) utilizar informações produzidas por auditorias internas e externas para o aperfeiçoamento da estrutura e do processo de gestão de riscos;
c) manter servidores informados dos objetivos e prioridades da organização e de suas unidades, assim como dos riscos enfrentados;
d) orientar e estimular os servidores a encaminhar assuntos relacionados a risco às instâncias decisórias adequadas;
e) aprimorar a avaliação de riscos, incluindo a estimativa da probabilidade de ocorrência de riscos e das consequências da materialização desses riscos sobre os objetivos organizacionais;
f) estruturar e operacionalizar as etapas de tratamento, monitoramento e comunicação de riscos;
g) estruturar e operacionalizar a gestão de riscos em parcerias.

Para as entidades públicas que se encontram nos níveis *intermediário* e *aprimorado*, as principais medidas para fortalecer a gestão de riscos são as seguintes:

a) obter o envolvimento ativo da alta administração com o fortalecimento da gestão de riscos;
b) manter servidores informados dos objetivos e prioridades da organização e de suas unidades, assim como dos riscos enfrentados;
c) orientar e estimular os servidores a encaminhar assuntos relacionados a risco às instâncias decisórias adequadas;
d) aprimorar a estimativa da probabilidade de ocorrência de riscos e das consequências da materialização desses riscos sobre os objetivos organizacionais;
e) definir parâmetros para a escolha das ações de aceitar, transferir, evitar ou mitigar os riscos analisados;
f) definir e revisar periodicamente medidas de contingência para garantir a continuidade dos serviços;
g) estruturar e operacionalizar a etapa de monitoramento e comunicação de riscos;
h) estruturar e operacionalizar a gestão de riscos em parcerias.

12 Tribunal de Contas do Município de São Paulo – ferramentas de auditoria

Com a contínua evolução das estratégias de auditoria no mundo moderno, em especial, com a utilização de análises estatísticas complexas (ferramentas de extração de dados como a ACL e Workbench/Deloitte, entre outras), técnicas de auditoria assistida por computador - CAATs, auditorias contínuas, de riscos/*compliance*, de recuperação de desastres (*disaster recovery audit*) e de continuidade de negócios, auditoria de avaliação de governança em TI e *digital audit* (auditoria digital), tem exigido do auditor maior compromisso com seu aperfeiçoamento técnico, estimulando, inclusive, a procura pela autoinstrução.

Neste diapasão, o Tribunal de Contas do Município de São Paulo (TCMSP) tem acompanhado o aperfeiçoamento das técnicas de auditoria com o desenvolvimento interno pelos próprios servidores do Tribunal de *softwares* e sistemas como o Panorama (2007), Prisma (2008), Sigma (2008), Ábaco (2011), Radar (2009) e Átomo-Radar (2013), Portal (2012) e Diálogo (2015 – Contas RAF 2014)[3], em contínuo processo de integração de dados e informações.

Esses sistemas, segundo informações da

Subsecretaria de Fiscalização e Controle do TCMSP, se adequam a necessidade de permanente evolução das ferramentas de auditoria, gerando informações úteis, relevantes e tempestivas e permitindo, igualmente, detectar pontos de falha/risco, analisar suas causas potenciais, elaborar relatórios com maior qualidade e precisão bem como obter estatísticas sobre a atuação do Tribunal de Contas.

Em memorando recente do Gabinete do Conselheiro Domingos Dissei (Memo GABDD nº289/2016) do TCMSP, foi criado um instrumento de medição de resultado – indicador de resultado de zeladoria, fruto de pesquisas e estudos de treze atividades de zeladoria do Município de São Paulo, o que propiciará, com o seu monitoramento, segundo o memorando, ganho de qualidade e economia de recursos públicos nas contratações de serviços públicos (publicado no DOC de 27.07.2016, p.101 a 104).

Fatos esses que entendemos como alvissareiros, pois conjugados com a atuação da Escola de Contas do TCMSP que, desde a sua criação em 1996, tem oferecido programas continuados de treinamento e reciclagem, patrocinando, entre muitas atividades, cursos de curta duração presenciais e EAD, programas de pós-graduação *lato sensu*, palestras, artigos científicos, *workshops*, ciclos de debates institucionais e mais recentemente oportunizando a possibilidade de interação e participação, por meio de mídias sociais, integrando conteúdos e construção de informações.

13 Comentários finais

O sucesso do desenvolvimento de um indicador de risco não deve ser considerado como critério único e exclusivo, ao contrário, o seu objetivo principal é o de constituir-se em uma ferramenta exploratória para se mapear e avaliar onde devem estar concentradas as análises das falhas de desempenho e de gestão, com vistas a mitigar as fragilidades mais críticas. Quanto mais robusta a metodologia de criação do indicador de maturidade de gestão de riscos e, consequentemente, com a sua utilização nos levantamentos de auditoria, mais relevantes e úteis deverão ser os achados de auditoria, evidenciando-se com maior acurácia os controles existentes e oferecendo um importante subsídio ao gestor para aplicar procedimentos e técnicas mais adequadas de monitoramento, construindo, destarte, padrões normativos mais rígidos para enfrentamento das crises e riscos potenciais nas áreas mais vulneráveis da organização.

Identificar, mapear e inventariar riscos, sem dúvida, marcam importantes passos no desenvolvimento de um plano de contenção de riscos, porém, mais vital às organizações é a implementação e o constante aprimoramento das estratégias de recuperação de perdas e desastres, especialmente ativadas quando da concretização dos riscos e de seus reflexos adversos.

Com a adesão das ferramentas e técnicas apontadas no corpo do Relatório do TCU, espera-se obter valiosas contribuições ao planejamento de uma auditoria mais eficiente e eficaz, contribuindo, desse modo, para incentivar programas e mecanismos de controle com maior qualidade, fortalecendo a transparência na aplicação dos recursos públicos, a efetividade dos resultados alcançados e incentivando as boas práticas de governança nas organizações públicas.

Marcus Braga, analista de finanças e controle da CGU/RJ, em seu excelente artigo "Lógica de riscos nas atividades de auditoria governamental: um promotor da qualidade na gestão pública? (2013)" conclui, de forma peremptória, por que se deve estimular o gerenciamento de risco pela auditoria pública e pelos órgãos de controle:

> Em um país cartorial como o nosso, com grandes resquícios de patrimonialismo na gestão pública, a introdução de conceitos de risco nas

atividades de auditoria governamental, em um momento de pujança dos órgãos de controle, possibilitará resultados no campo da efetividade e um melhor diálogo com o gestor. Contribuirá, ainda, com o ***fortalecimento do papel do controle como um promotor da qualidade na gestão***, um desafio para os órgãos de controle nas próximas décadas (grifo nosso).

Referências

ALENCAR, Antonio Juarez, SCHMITZ, Eber Assis. **Análise de risco em gerência de projetos**: com exemplos em @Risk. 3. ed. Rio de Janeiro: Brasport, 2012.

BANCO CENTRAL DO BRASIL. Resolução Nº 3056, de 19 de dezembro de 2002. Dispõe sobre a auditoria interna das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?tipo=Resolu%C3%A7%C3%A3o&data=2002&numero=3056>. Acesso em 15.07.2016.

BERNSTEIN, Peter L. **Desafio aos deuses**: a fascinante história do risco. Rio de Janeiro: Elsevier, 1997.

BLUMEN, Abrão. **Controle Interno como suporte estratégico de governança no setor público**. Coordenação: Valmir Leôncio da Silva e Eurípedes Sales. Belo Horizonte: Fórum, 2015.

BORGERTH, Vania Maria da Costa. **SOX**: entendendo a Lei Sarbanes-Oxley: um caminho para a informação transparente. São Paulo: Thomson Learning, 2007.

BRAGA, Marcus. **Lógica de riscos nas atividades de auditoria governamental**: um promotor da qualidade na gestão pública? Disponível em: <https://periodicos.tce.pe.gov.br/seer/ojs-2.3.6/index.php/Revista_TCE-PE/article/viewFile/1175/1090>. Acesso em 10 jun. 2016.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Gerenciamento de riscos corporativos: estrutura integrada**. Price WatherhouseCoopers, COSO, Audibra, 2007. Disponível em: <http://www.coso.org/documents/coso_erm_executivesummary_portuguese.pdf>. Acesso em 20 maio 2016.

_____. **Improving Organizational Performance and Governance**. How the COSO Frameworks can help. COSO. February 2014

CONSELHO FEDERAL DE CONTABILIDADE. NBC T 16.8 - Controle Interno. Disponível em: <http://www1.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2008/001135>. Acesso em 17 jul. 2016.

CONTROLADORIA GERAL DA PREFEITURA DO MUNICÍPIO DO RIO DE JANEIRO. **Planejamento Estratégico em Auditoria**. Auditoria baseada em Risco. Rio de Janeiro, 2004. Disponivel em: <http://www.rio.rj.gov.br/dlstatic/10112/2904248/DLFE244422.pdf/auditoriabaseadaemrisco.pdf>. Acesso em 19 jul. 2016.

GIL, Antonio de Loureiro, ARIMA, Carlos Hideo, NAKAMURA, Wilson Toshiro. **Gestão: controle interno, risco e auditoria**. São Paulo: Saraiva, 2013.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5.ed. Instituto Brasileiro de Governança Corporativa. São Paulo: IBGC, 2015.

INTERNACIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). Working Group of Information Technology (WGITA). **Get.it: governance evaluation techniques for information technology**: a WGITA

guide for supreme audit institutions. Brasília: Federal Court of Accounts of Brazil, 2016.

INTERNATIONAL FEDERATION OF ACCOUNTANTS – IFAC. Disponível em: <http://portalcfc.org.br/wordpress/wp-content/uploads/2013/01/ipsas2010_web.pdf>. Acesso em: 19 jul. 2016.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO E A CONTROLADORIA-GERAL DA UNIÃO. **Instrução Normativa Conjunta** CGU/MP nº001, de 10.05.2016. Disponível em: <http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf>. Acesso em 01 jul. 2016.

NEGRÃO, Célia Regina P. Lima; PONTELO, Juliana de Fátima. **Compliance, controles internos e riscos: a importância da área de gestão de pessoas**. Brasília: Senac, 2014.

REINO UNIDO. **The Orange Book Management of Risk**: Principles and Concepts. HM Treasury, 2004. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf>. Acesso em 19 jul. 2016.

SALLES JÚNIOR, Carlos Alberto Corrêa et al. Gerenciamento de riscos em projetos. Rio de Janeiro: FGV, 2007.

SLOMSKI, Valmor. **Controladoria e governança na gestão pública**. São Paulo: Atlas, 2005.

TRIBUNAL DE CONTAS DA UNIÃO. Acórdão TCU 2467 de 11.09.2013. Ministra Relatora Ana Arraes (p.612-642). Disponível em: <http://www.tcu.gov.br/consultas/juris/docs/conses/tcu_ata_0_n_2013_35.pdf>. Acesso em 17 jul. 2016.

TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO. **Resolução Normativa nº 26/2014-TP**. Disponível em: <http://www.tce.mt.gov.br/arquivos/downloads/00049214/026-2014.pdf:. Acesso em 15 maio 2016.

YU, Abraham Sin Oih (coord.). **Tomada de Decisão nas Organizações: uma visão multidisciplinar**. São Paulo: Saraiva, 2011.

[1] O TCU e a Auditoria Contínua e Preditiva, Ministro Aroldo Cedraz, Presidente do TCU. Disponível em: □http://pt.slideshare.net/tecsifeausp/12-contecsi-34thwcars-o-tribunal-de-contas-da-unio-e-a-auditoria-contnua□. Acesso em 15.06.2016.

[2] Um dos métodos multicritério de apoio à decisão é o AHP (Analytic Hierarchy Process), desenvolvido pelo Prof. Thomas L. Saaty, na década de 70. Neste método, a atribuição de pesos é baseada na comparação de critérios oferecidos por especialistas por meio de questionários/perguntas, objetivando a apreciação da melhor alternativa ao processo de tomada de decisão. Fonte: Abraham Sin Oih Yu (2011).

[3] Informações gentilmente oferecidas pela Coordenadoria VII da Subsecretaria de Fiscalização e Controle do TCMSP.