Metodologia de auditoria com foco em processo e risco

Antonio José Saraiva de Oliveira Júnior é servidor do Tribunal de Contas da União, bacharel em Economia pela Universidade de Brasília, com especialização em Análise de Políticas Públicas pela Fundação Getúlio Vargas (FGV).

Arnaldo Ribeiro Gomes é servidor do Tribunal de Contas da União, graduado em Ciências Contábeis pela Universidade de Brasília (UnB) e Certified in Control Self Assessment (CCSA®) pelo The Institute of Internal Auditors (IIA), dos Estados Unidos da América.

Guilherme de Vasconcellos Machado é servidor do Tribunal de Contas da União, graduado em Engenharia Mecatrônica pela Universidade de Brasília – UnB.

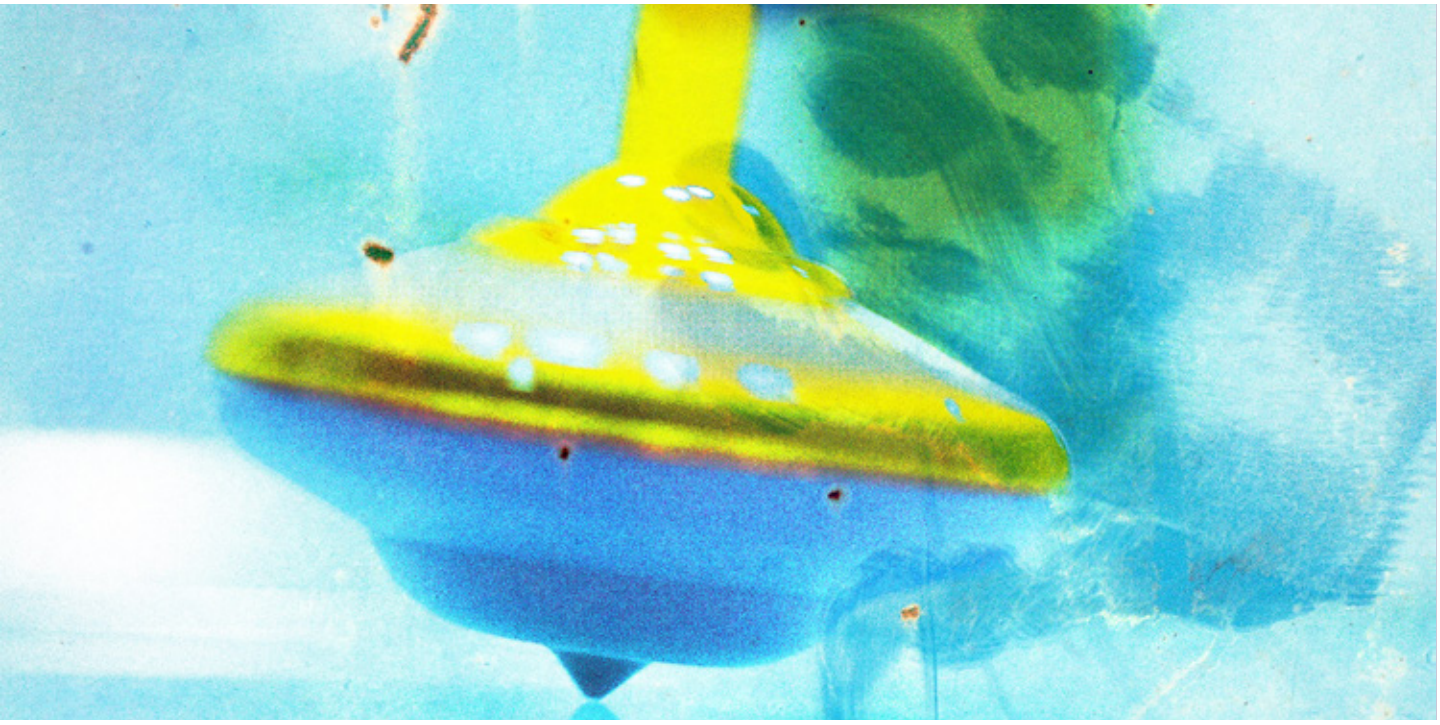
RESUMO

Este artigo apresenta as linhas gerais de metodologia de auditoria orientada para a avaliação de riscos e controles com foco em processos de trabalho, finalísticos ou de apoio, que suportam o objeto de fiscalização, por meio da aplicação de procedimentos e técnicas para mapear os processos envolvidos, seus objetivos, riscos e controles associados. O método apresentado possui flexibilidade para aplicação em fiscalizações do controle interno ou externo e tem o potencial de contribuir para a melhoria da governança, no tocante ao componente relacionado à gestão de riscos e controles internos e, consequentemente para o alcance dos objetivos organizacionais ou de políticas públicas.

Palavras-chave: Controle Externo. Governança Pública. Metodologia de Auditoria. Gestão de Riscos. Controles Internos.

1. FUNDAMENTOS TEÓRICOS

A gestão de riscos traduz um processo contínuo conduzido pela alta administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da instituição e possibilitar garantia razoável do cumprimento dos seus objetivos (COSO, 2004).



O risco é o efeito da incerteza sobre os objetivos da organização (ABNT, 2009). Abrange eventos positivos, com o potencial de agregar valor, e negativos, com a capacidade de destruir valor. O desafio da governança nas organizações do setor público é determinar quanto risco aceitar na busca do melhor valor para os cidadãos e demais partes interessadas, o que significa prestar serviço de interesse público da melhor maneira possível (BRASIL, 2014). Os controles internos, por sua vez, são os instrumentos do processo de gestão de riscos da organização e atuam na mitigação dos eventos indesejáveis.

É nesse contexto que se propõe metodologia objetiva aplicável a trabalhos de fiscalização do controle externo e interno da Administração Pública. Conforme se verá adiante, também tem aplicabilidade às instituições privadas, sem alterações significativas, dada a versatilidade dos instrumentos de auditoria, embora não seja o enfoque deste artigo.

O método pressupõe a construção de matrizes de risco para avaliação de probabilidades e impactos em relação às etapas de operacionalização de quaisquer processos de gestão, os quais podem ser compreendidos como grandes conjuntos de atividades pelos quais a organização cumpre sua missão (BRASIL, 2013).

Os processos finalísticos são de grande interesse para os controles externo e interno, pois se referem à essência da organização, caracterizam sua atuação, estão diretamente relacionados aos seus objetivos estratégicos e recebem apoio de outros processos internos, gerando produtos e serviços seus clientes interno e externo (BRASIL, 2013).

Como produto da aplicação das técnicas e procedimentos, obtém-se uma avaliação qualitativa e quantitativa da gestão de riscos de uma organização ou política pública. O diferencial da metodologia é a capacidade de objetivação dos resultados, como se verá adiante.

No Brasil, são poucos os órgãos e entidades públicas que possuem política ou práticas de gestão de riscos formalmente estabelecida. Essa lacuna torna a aplicação da metodologia ainda mais profícua e pedagógica, pois possibilita evidenciar práticas inconscientes ou informais de administração do risco. Ainda que as instituições não possuam políticas de gestão de riscos formalmente instituídas, dispõem de elementos de resposta a risco (controles internos) que, identificados e avaliados, consoante metodologia proposta, podem ser aperfeiçoados, contribuindo assim para a melhoria da governança e para o alcance dos objetivos organizacionais.

2. NORMAS GERAIS DE AUDITORIA E CONCEITOS APLICADOS

As Normas de Auditoria do Tribunal de Contas da União – NAT (BRASIL, 2010) e as Normas Internacionais para a Prática Profissional de Auditoria Interna (IIA, 2012) prescrevem o estabelecimento de objetivos

para cada trabalho de auditoria. Segundo essas diretrizes, é preciso realizar uma avaliação preliminar de objetivos e riscos relevantes relacionados ao objeto da auditoria, cujos resultados deverão estar refletidos nos objetivos estabelecidos para a fiscalização. No desenvolvimento dos objetivos deve-se considerar, além das exposições significativas a riscos, a probabilidade de erros, irregularidades e descumprimentos a princípios, normas legais e regulamentações aplicáveis.

Na fase de planejamento, para determinar a extensão e o alcance da auditoria, o auditor ou unidade de auditoria deve dispor de informações sobre os objetivos relacionados ao objeto que será auditado e aos riscos relevantes associados a esses objetivos, bem como à confiabilidade dos controles para tratar os eventos indesejáveis.

Quando na auditoria a ser proposta as informações relativas aos objetivos, riscos e controles do objeto auditado não estiverem disponíveis, tais informações deverão ser obtidas na fase de planejamento do trabalho. A necessidade e a profundidade dos procedimentos para a obtenção desses dados variam de acordo com os objetivos e o escopo da auditoria em questão.

Caso o objeto e o escopo do trabalho sejam amplos, deve ser avaliada a conveniência de se realizar ação de controle prévia e específica para se obter conhecimento sobre o objeto auditado, devendo-se considerar seus resultados no planejamento e na aplicação dos procedimentos da auditoria com foco em riscos.

A metodologia proposta viabiliza a avaliação de riscos e controles e tem como referência o modelo ERM (*Enterprise Risk Management*), do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nas demonstrações contábeis das empresas. O modelo considera que a gestão de riscos das instituições deve ser avaliada segundo oito componentes (dimensões) que lhe são intrínsecos (COSO, 2004).

Nessa linha, a presente metodologia se propõe a avaliar os cinco elementos centrais do modelo, os quais podem ser traduzidos em perguntas que, didaticamente, facilitam o entendimento dos pontos:

a. **Fixação de Objetivos:** a unidade fixou objetivos para o processo ou para a política pública?

b. **Identificação de Eventos:** quais eventos podem representar risco aos objetivos do processo ou da política pública?

c. **Avaliação de Riscos:** qual é a significância dos riscos identificados em termos de probabilidade e impacto de ocorrência?

d. **Resposta a Riscos:** a organização implementou controles em resposta aos riscos identificados?

e. **Atividades de Controle:** qual é a qualidade dos controles internos estabelecidos e em que medida eles asseguram que os riscos relacionados sejam mitigados a um nível aceitável?

A opção por apenas cinco elementos do modelo ERM não retira ou reduz a importância atribuída aos demais (ambiente de controle, informação e comunicação, monitoramento). Eventual prolongamento da metodologia permite que o auditor facilmente avalie os demais componentes do modelo.

No que tange aos conceitos aplicados à metodologia, tem-se os seguintes:

- **Risco:** possibilidade de algo acontecer e ter um impacto nos objetivos de organizações, programas ou atividades governamentais, sendo medido em termos de consequências e probabilidades (BRASIL, 2012a).

O evento de risco, portanto, materializa o risco, consequência negativa para o alcance dos objetivos institucionais. Na prática, os termos "evento de risco" e "risco" podem ser tratados como sinônimos.

- **Objetivo:** 'algo' que se estabeleceu para ser alcançado, de caráter quantitativo ou qualitativo (BRASIL, 2012b).

- **Controle Interno:** 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 e os objetivos gerais de controle serão atendidos (BRASIL, 2012a). Em síntese, os controles internos representam uma forma de tratamento (resposta) aos riscos, os quais são adotados para assegurar, de forma razoável, que os objetivos organizacionais sejam alcançados.

Os controles internos representam, portanto, instrumentos de governança à disposição dos gestores, pois convergem para a consecução dos objetivos das instituições e seus programas.

- **Fonte de risco:** é o elemento que, individualmente ou combinado, tem potencial intrínseco para dar origem ao risco, podendo ser tangível ou intangível (ABNT, 2009).

Em outras palavras, as fontes de risco são todos os sujeitos, objetos ou situações que podem originar um evento negativo. São classificadas em seis categorias: pessoas, processos, sistemas, infraestrutura (física ou organizacional), tecnologia ou ainda eventos externos à organização.

Os riscos são avaliados em duas dimensões, uma antes e outra após a aplicação de controles, conforme a seguir (BRASIL, 2009):

- **Risco inerente:** é o risco do negócio, do processo ou da atividade, independente dos controles internos administrativos adotados.

- **Risco residual:** é o risco que remanesce após a mitigação por controles internos.

Portanto, o risco residual é a parcela do risco inerente que permanece após a implementação de atividades administrativas que permitam reduzir a probabilidade e/ou impacto do evento, de modo a evitar, reduzir, compartilhar ou, ainda, aceitar o risco.

3. PROCEDIMENTOS

Entendido o arcabouço conceitual básico, passa-se à exposição dos procedimentos e técnicas utilizados na construção do cenário sobre a gestão de risco das organizações ou suas subáreas. A parte operacional está dividida em quatro etapas para melhor entendimento.

3.1 IDENTIFICAÇÃO E REGISTRO DE OBJETIVOS E PROCESSOS DE TRABALHO (VISÃO GERAL)

Nesta fase, é preciso levantar e entender a legislação aplicável ao objeto, o regimento interno da organização, trabalhos anteriores de órgãos de controle interno e externo sobre o assunto, artigos acadêmicos ou técnicos, bem como outras informações disponíveis.

Deve-se, então, identificar os objetivos de cada atividade e/ou política pública a ser auditada, bem como compreender e registrar as etapas do processo de trabalho que compõem a atividade administrativa, desenvolvidas para alcançar os objetivos estabelecidos. Como exemplo, no caso do processo de descentralização de recursos da União para outros entes públicos ou privados por meio de transferências voluntárias de recursos, poder-se-ia dividir o processo nas seguintes etapas: a) motivação da transferência; b) seleção do recebedor da descentralização; a) celebração do ajuste; b) acompanhamento da execução; e c) análise de prestação de contas.

Em seguida, para se construir visão detalhada do objeto e da gestão de riscos, devem ser requeridos da instituição (i) informações sobre planejamento estratégico (ou assemelhado) e/ou sobre a inserção do objeto de auditoria no planejamento estratégico do órgão ou unidade; (ii) fluxogramas e narrativas do processo de trabalho (descrição textual das atividades realizadas); (iii) normativos internos aplicáveis e relação de áreas responsáveis pela gestão do objeto.

Superada a fase inicial de entendimento do objeto da auditoria, passa-se à realização de entrevistas com gestores e operadores dos processos ou atividades, com o objetivo de aprofundar o conhecimento acerca dos objetivos e da operacionalização das atividades desenvolvidas em cada etapa do processo de trabalho.

As reuniões devem ser executadas mediante a aplicação de técnicas de entrevista. Em alguns casos, a equipe pode aprofundar sua visão do objeto ou confirmar informações por meio de exame documental de processos e atos administrativos relacionados. Os dados obtidos devem ser utilizados na preparação dos seguintes documentos, que formam a visão geral do objeto:

a. **Fluxograma:** documento que fornece uma representação gráfica do processo de trabalho, evidenciando a sequência das atividades, os prazos e o fluxo de documentos entre as áreas envolvidas.

Destaca-se que os fluxogramas devem, na medida do possível, ser desenvolvidos e, em conjunto com os gestores responsáveis, ajustados e validados, mediante aposição de data e assinatura, para evitar questionamentos futuros.

b. **Narrativa do processo de trabalho:** documento que descreve, de forma textual e com maior riqueza de detalhes, a sequência das atividades de gestão, a legislação relacionada a cada etapa, os sistemas informatizados envolvidos e os mecanismos de controle administrativo adotados – sejam esses normatizados ou apenas práticas de trabalho executadas pelos setores –, unidades responsáveis, quantitativo e estrutura do quadro de pessoal, entre outros detalhes pertinentes.

Quando analisados em conjunto, esses documentos proporcionam amplo entendimento acerca da operacionalização do objeto de auditoria, em especial seus objetivos, etapas do processo de trabalho e atividades nelas desenvolvidas, o que permite avançar à fase de identificação e avaliação de riscos.

3.2 IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A terceira etapa compreende a identificação de eventos que possam afetar os objetivos organizacionais estabelecidos, e está associada ao senso crítico e ao julgamento profissional dos auditores, gestores e corpo operacional responsável pela execução da atividade examinada. Essa etapa deve ser uma construção coletiva da equipe de auditoria a partir das contribuições dos gestores e operadores dos processos e, se possível, corroborada por outras instâncias de auditoria interna ou externa. Para identificação e registro dos eventos de risco, deve-se fazer uso de Matriz da Riscos por Processos (MRP), cuja estrutura será exposta adiante.

Na matriz, que já deve conter os objetivos e as etapas do processo de trabalho, cada integrante da equipe de fiscalização deve identificar, individualmente, rol de possíveis eventos que possam impactar negativamente na consecução dos objetivos do objeto da auditoria, tomando por base, em especial, os dados obtidos nas etapas anteriores. A realização dessa etapa de forma individual, no primeiro momento, objetiva potencializar a intelecção particular de cada membro sobre todas as possibilidades de riscos sem a interferência ou viés que pode ser gerado por outros integrantes da equipe.

Após levantamento individual, a equipe deve reunir-se, discutir os riscos inventariados e principalmente outros possíveis, consolidando o resultado em matriz única, passando-se em seguida para a avaliação do impacto (magnitude de um efeito negativo) e probabilidade (estimativa) de ocorrência de cada risco segundo as variáveis da matriz de riscos a seguir. Sempre que possível, deve haver consenso na equipe quanto à existência e classificação dos riscos.

Como suporte à avaliação do impacto e da probabilidade do risco e visando a redução da subjetividade inerente ao processo de avaliação, devem ser desenvolvidas tabelas de apoio contendo critérios qualitativos – e, sempre que possível, quantitativos – para avaliação das variáveis impacto e probabilidade (exemplo: muito alto, alto, médio, baixo e muito baixo).

3.3 ASSOCIAÇÃO DOS CONTROLES INTERNOS AOS RISCOS E AVALIAÇÃO DO CONTROLE

Nesta etapa, o auditor deve identificar os mecanismos de controle existentes, correlacionando-os aos eventos de risco já catalogados. Para cada risco deverão ser associados, caso existentes, os controles formais e informais de que dispõe a unidade, os quais, direta

Quadro 1: Mapa de Riscos (probabilidade vs. impacto):

Tabela Risco						
		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Muito Alto	Médio 20	Elevado 40	Extremamente elevado 60	Extremamente elevado 80	Extremamente elevado 100
	Alto	Médio 16	Elevado 32	Elevado 48	Extremamente elevado 64	Extremamente elevado 80
	Médio	Médio 12	Médio 24	Elevado 36	Elevado 48	Extremamente elevado 60
	Baixo	Baixo 8	Médio 16	Médio 24	Elevado 32	Elevado 40
	Muito Baixo	Baixo 4	Baixo 8	Médio 16	Médio 16	Médio 20

Fonte: MRP - SecexDesenvolvimento

Quadro 2:
Efeitos da mitigação do risco inerente pelos controles internos

Avaliação do Controle	Mitigação	Obtenção do valor numérico do risco residual estimado
Inexistente	Estimada redução 4,5% do risco	Multiplicar risco inerente por 0,95
Fraco	Estimada redução 23% do risco	Multiplicar risco inerente por 0,77
Mediano	Estimada redução 50% do risco	Multiplicar risco inerente por 0,50
Satisfatório	Estimada redução 77% do risco	Multiplicar risco inerente por 0,23
Forte	Estimada redução 95% do risco	Multiplicar risco inerente por 0,05

Fonte: MRP - SecexDesenvolvimento

ou indiretamente, possam contribuir para mitigar os riscos identificados.

Uma atividade importante nessa etapa é a realização de *workshops* e/ou entrevistas adicionais com gestores e operadores dos processos, com o objetivo de validar os riscos inventariados e indagar a respeito dos controles internos existentes associados a cada risco. É preciso ainda considerar as informações sobre controles internos obtidas na fase inicial de construção da visão geral do objeto. Essas reuniões são também uma oportunidade aos responsáveis pelos processos para que informem à equipe sobre a existência de riscos até então não identificados.

Após identificação e associação dos controles aos riscos na MRP, deve ser avaliada, tanto pela equipe de auditoria como pelos responsáveis pelo processo, a qualidade dos controles internos segundo as categorias de avaliação estabelecidas para o trabalho (e.g. forte, satisfatório, mediano, fraco ou inexistente). Nesse caso, podem ser desenvolvidos e aplicados questionários para coletar a percepção do corpo operacional e gerencial responsável pelo processo no que toca à qualidade e/ou eficácia do controle na mitigação dos riscos.

Na avaliação dos controles internos, também devem ser estabelecidas escalas qualitativas e, se possível, quantitativas, que contribuam para a redução da subjetividade inerente ao processo de avaliação. Além disso, para cada categoria de avaliação, devem ser definidos os efeitos que os mecanismos de controle produzirão sobre os riscos inerentes (cuja valoração já considerou probabilidades e impactos), conforme tabela exemplificativa a seguir.

Desse modo, o risco residual retratará o resultado da avaliação dos controles formais ou informais associados a cada evento de risco inerente. A MRP, portanto, exibirá informação acerca do risco residual, tomando por base as cores e os valores definidos na tabela utilizada para avaliação do risco inerente (Quadro 1). O diagrama abaixo ilustra, de forma exemplificativa, um caso prático do efeito do controle para mitigação do risco inerente:

Portanto, a partir da aplicação dos coeficientes previstos na terceira coluna do Quadro 2 sobre os valores associados aos riscos do Quadro 1, é possível obter um parâmetro numérico de risco residual estimado associado a cada risco inerente, conforme tabela adiante.

O risco residual estimado representa o resíduo de risco inerente que permanece após aplicação dos controles, ou ainda a parcela do risco carente de controles internos para que seja mitigado pro completo. É considerado estimado porque os efeitos dos controles ainda não foram aferidos nessa etapa do trabalho, tratando-se de estimativa com base em critérios predominantemente qualitativos (Quadro 2).

Ao final dessa etapa, é possível definir a extensão e a profundidade da auditoria, com base no entendimento acerca dos objetivos e da operacionalização da atividade a ser fiscalizada. Os riscos inerentes e controles são conhecidos e o desenho e a qualidade dos controles internos já foram avaliados, obtendo-se como resultado os riscos residuais do processo sob

Figura 1:
Exemplo de cálculo do efeito estimado da mitigação do risco inerente por controles internos

Quadro 3: Quadro de Risco Residual (risco inerente vs. eficácia do controle)

Tabela Hiato de Controle						
		Eficácia do Controle				
		Forte	Satisfatório	Mediano	Fraco	Inexistente
Ranking do Risco	Extremamente elevado	Baixo 5	Médio 23	Elevado 50	Extremamente elevado 77	Extremamente elevado 96
	Extremamente elevado	Baixo 4	Médio 18	Elevado 40	Extremamente elevado 62	Extremamente elevado 76
	Extremamente elevado	Baixo 3	Médio 15	Elevado 32	Elevado 49	Extremamente elevado 64
	Extremamente elevado	Baixo 3	Médio 14	Elevado 30	Elevado 46	Extremamente elevado 60
	Elevado	Baixo 2	Médio 11	Médio 24	Elevado 37	Elevado 46
	Elevado	Baixo 2	Baixo 9	Médio 24	Elevado 31	Elevado 38

Fonte: MRP - SecexDesenvolvimento

auditoria. Essas referências podem ser utilizadas para direcionar os esforços de fiscalização na avaliação dos controles-chave estabelecidos para mitigar os riscos significantes (de maior probabilidade e impacto) aos quais está exposto o objetivo do processo auditado.

3.4 DEFINIÇÃO DE ESCOPO E EXECUÇÃO DE AUDITORIA COM FOCO EM RISCO

A partir da compreensão dos riscos, o escopo do trabalho deve ser definido com foco nas etapas do processo suscetíveis a eventos que possam interferir mais severamente na consecução dos objetivos estabelecidos. O escopo do trabalho pode ser limitado a determinada etapa do processo, nos casos em que o conjunto de riscos da etapa selecionada e os recursos de fiscalização justificarem.

Quando se tratar de auditoria operacional ou levantamento – casos em que os controles não são testados por procedimentos e técnicas de auditoria – recomenda-se, antes, estimar os riscos residuais por meio de *workshops* com operadores do processo. Esses encontros devem prever debates com os gestores e/ou com os operadores dos processos de trabalho (colaboradores lotados nas unidades e que lidam diariamente com os processos de gestão e são responsáveis por executá-los), como forma de colher subsídios para o aperfeiçoamento das avaliações dos eventos de risco contidas nas matrizes, notadamente em relação à probabilidade, ao impacto e aos procedimentos de controle interno.

As reuniões com os operadores dos processos, sempre que possível, devem ser realizadas sem a participação dos gestores e sem identificação pessoal dos presentes, de forma a conferir maior liberdade de expressão. Encerrada a etapa de validação/contribuição dos gestores/operadores dos processos, os ajustes e as revisões nas avaliações de riscos e de controles que se fizeram necessárias devem ser efetuadas e a MRP concluída, em versão final.

Os *workshops* são especialmente úteis para a confirmação dos eventos de riscos apontados na MRP, por meio da validação, pelo gestor, da possibilidade de materialização/ocorrência do evento negativo. Também servem para avaliar a existência e a conformação dos controles internos existentes como resposta aos eventos de risco, ou mesmo a inexistência desses e a identificação de novos riscos ainda não detectados pela equipe de fiscalização.

Por outro lado, quando a avaliação de riscos é etapa preliminar de auditoria de conformidade (realizada no planejamento), deverão ser modelados procedimentos de auditoria para, na fase de execução, avaliar a eficácia dos controles associados aos riscos incluídos no escopo, fazendo-se referência a esses procedimentos e respectivos papéis de trabalho em campo específico da MRP.

A definição do escopo da fiscalização deve considerar as situações de inexistência ou insuficiência de controles para riscos significantes, bem como os casos de controles desnecessários que acarretem prejuízo operacional (ineficiência) ao processo. Também podem ser propostas recomendações para adoção de providências de aprimoramento dos controles internos.

Aplicados os procedimentos e técnicas de auditoria para avaliação da eficácia dos controles internos

(testes de controles) e havendo distorções significativas quanto à avaliação dos riscos e/ou dos controles inicialmente registrados na MRP, devem ser realizadas revisões nesse documento.

3.5 SISTEMATIZAÇÃO DAS ANÁLISES EM MATRIZ DE RISCOS POR PROCESSOS (MRP)

O registro das avaliações qualitativas e quantitativas deve ocorrer de forma sequenciada e associada a cada evento de risco. Ao longo de cada etapa do processo de identificação e avaliação dos eventos de risco, bem como da avaliação do desenho dos controles, novas informações devem ser incorporadas às MRPs, documento organizado para permitir a visualização integrada e resumida dos elementos de gestão de riscos catalogados ao longo do trabalho, com base na estrutura sugerida a seguir:

Cada coluna deve apresentar as seguintes informações:

a. objetivo do órgão/entidade/programa/atividade auditado;

b. etapas do processo auditado: subdivisão didática das fases de um processo administrativo;

c. riscos: riscos inerentes por etapa do processo, caracterizados por: evento de risco, categoria (exemplos: operacional, conformidade, financeiro, de informação, de imagem, etc.), classificação da probabilidade, classificação do impacto, avaliação da probabilidade e avaliação do impacto;

d. resultado do risco inerente: resultado numérico do risco inerente (multiplicação da probabilidade pelo impacto, em uma escala de 1 a 100, conforme critério apresentado no Quadro 2 a título de exemplo);

e. controles: descrição e classificação (Forte, Satisfatório, Mediano, Fraco ou Inexistente) dos controles internos associados a cada risco;

f. avaliação do controle interno;

g. resultado do risco residual: resultado numérico do risco residual estimado, ou seja, do risco mitigado após a aplicação dos controles internos (ref. Quadro 3, estimativa);

h. referência aos testes de controle interno: referência aos procedimentos de auditoria para avaliação da eficácia dos controles internos.

4. RESULTADO

Ao final dos procedimentos, obtém-se visão estruturada da qualidade da gestão de riscos e controles internos do objeto auditado – um dos componentes da governança pública –, com informações sobre objetivos, etapas do processo de trabalho e atividades nelas desenvolvidas para atingir os objetivos, riscos inerentes associados a cada etapa, controles internos adotados e sua qualidade, bem como risco residual estimado, de modo a permitir o direcionamento e a otimização dos esforços de auditoria.

Além disso, o trabalho colaborativo de debate com os gestores sobre os objetivos do processo sob auditoria, riscos e controles possui elevado caráter pedagógico, pois permite uma reflexão profunda sobre o *modus operandi* das unidades e das atividades desenvolvidas, especialmente em relação a formas de aprimoramento dos controles internos administrativos.

Quadro 4: Estrutura de Matriz de Riscos por Processos (MRP)

		Riscos	Avaliação RI	Controles	Avaliação CI	Risco Residual	Referência Teste de CI
Objetivo	Etapa 1						PA - 1
							PA - 2
	Etapa 2						PA - N
							PA - N
							PA - N
	Etapa 3						PA - N
							PA - N
							PA - N

Fonte: MRP - SecexDesenvolvimento

5. APLICAÇÃO EM TRABALHOS DO TCU

No âmbito das modalidades de fiscalização do Tribunal de Contas da União, a metodologia pode ser empregada em levantamentos e auditorias. No primeiro caso, é possível abranger objeto maior, executando a primeira etapa na fase de planejamento e as três subsequentes na fase de execução. O resultado obtido converge perfeitamente para a finalidade do instrumento, conforme Padrões de Levantamento do TCU (BRASIL, 2011), pois permite a construção da visão geral do objeto e da avaliação de risco. Nesse caso, a avaliação de risco se estende até a avaliação do risco residual estimado.

Já em auditorias de conformidade, é possível aplicar a mesma técnica integralmente na fase de planejamento da fiscalização, desde que o escopo seja menor. Nesse caso, o resultado da avaliação geral de riscos permitirá eleger os pontos de auditoria prioritários e a viabilidade de empreender esforço fiscalizatório sobre o tema. Uma vez escolhido o escopo e delimitado o objeto, devem ser aplicados testes de controle (procedimentos e técnicas de auditoria) para aferição do risco residual efetivo.

6. CONCLUSÃO

Realizar avaliações de riscos e controles internos pode não atingir o máximo de sua efetividade caso não sejam adotadas técnicas objetivas e organizadas para esse fim. De modo a atender essa necessidade é que foi desenvolvida a presente metodologia de auditoria com foco em processo e risco.

Alinhada a conceitos modernos de governança no setor público, e atendendo às normas internacionais de auditoria interna, bem assim às normas de auditoria do Tribunal de Contas da União, a metodologia consiste em aplicar procedimentos de forma sistemática e disciplinada com vistas a mapear processos de trabalho, por meio da associação de riscos a mecanismos de controle.

Em linhas gerais, a construção do cenário sobre a gestão de risco das organizações divide-se em quatro etapas principais: (i) Identificação e registro de objetivos do processo a ser auditado (visão geral): envolve o conhecimento detalhado do objeto a ser fiscalizado e são produzidas peças como fluxograma e narrativas das etapas do processo fiscalizado; (ii) Identificação e avaliação de riscos: aborda a identificação, o reconhecimento e/ou a intelecção sobre os possíveis eventos que possam afetar os objetivos do objeto da fiscalização, e está associada ao senso crítico e ao julgamento profissional dos auditores, gestores e operadores do processo sob exame; (iii) Associação dos controles internos aos riscos e avaliação dos controles internos: correlaciona os mecanismos de controle aos eventos de risco; e (iv) Definição do escopo de auditoria com foco em risco: etapa na qual, a partir do conhecimento construído nas etapas anteriores, é possível definir o escopo da auditoria com foco nos riscos significantes, ou seja, aqueles cuja materialização possa causar maior impacto em desfavor da consecução dos objetivos estabelecidos para o objeto da auditoria.

As diretrizes apresentadas neste artigo servem de guia para que o auditor, conforme a sua necessidade, se aprofunde no assunto e passe a aplicar os conceitos aqui expostos em trabalhos de fiscalização, de modo a contribuir para a melhoria da governança e, consequentemente, para o alcance dos objetivos organizacionais ou de políticas públicas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISSO 31000: Gestão de riscos – princípios e diretrizes, 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=57311>. Acesso em: 25 de junho de 2014.

BRASIL. Tribunal de Contas da União. Governança Pública: Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública e Ações Indutoras de Melhoria. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014.

_____. Tribunal de Contas da União. Portaria nº 175/2013. Dispõe sobre orientações às unidades jurisdicionadas ao Tribunal quanto à elaboração de conteúdos dos relatórios de gestão referentes ao exercício de 2013. Brasília, 9 de julho de 2013.

_____. Tribunal de Contas da União. Glossário de Termos do Controle Externo - Segecex/Adsup/Adplan. Brasília: TCU, setembro de 2012a.

_____. Tribunal de Contas da União. Curso de avaliação de controles internos / Tribunal de Contas da União; Conteudistas: Antonio Alves de Carvalho Neto, Bruno Medeiros Papariello. 2ª ed. – Brasília: TCU, Instituto Serzedello Corrêa, 2012b.

_____. Tribunal de Contas da União. Portaria-Segecex-TCU nº 15/2011. Disciplina a realização de levantamentos e aprova, em caráter preliminar, o documento Padrões de Levantamento. Brasília, 9 de maio de 2011.

_____. Tribunal de Contas da União. Anexo à Portaria-TCU nº 280/2010. Normas de Auditoria do Tribunal de Contas da União. Brasília, 8 de dezembro de 2010.

_____. Tribunal de Contas da União. Critérios gerais de controle interno na Administração Pública: um estudo dos modelos e das normas disciplinadoras em diversos países. Brasília, 2009. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2056688.PDF>. Acesso em: 25 de junho de 2014.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de Riscos Corporativos – Sumário Executivo, Estrutura e Gerenciamento de Riscos na Empresa – Integrated Framework: Application Techniques, 2004. Versão em português disponível em: <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em: 25 de junho de 2014.

IIA, The Institute of Internal Auditor. Normas Internacionais para a Prática Profissional de Auditoria Interna. São Paulo, 2012. Versão em português disponível em: < http://www.iiabrasil.org.br/new/2013/downs/IPPF/standards2013_portuguese.pdf>. Acesso em: 25 de junho de 2014.