FGV EBAPE

RAP
REVISTA DE ADMINISTRAÇÃO PÚBLICA

Incorporação de modelos internacionais de gerenciamento de riscos na normativa federal

Flávio Sergio Rezende Nunes de Souza[1]
Marcus Vinícius de Azevedo Braga[2]
Armando Santos Moreira da Cunha[1]
Patrick Del Bosco de Sales[1]

[1] Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro / RJ – Brasil
[2] Universidade Federal do Rio de Janeiro / Instituto de Economia, Rio de Janeiro / RJ – Brasil

O interesse no gerenciamento de riscos tem crescido continuamente, fortalecido pela disseminação de modelos internacionais. Na administração pública federal brasileira, o uso da gestão de riscos é recente e encontra-se em expansão. Esta pesquisa analisou como modelos internacionais de gerenciamento de riscos corporativos são adotados pelas normas e orientações do Governo Federal. Aplicam-se os conceitos de forças coercitivas, normativas e miméticas da teoria neoinstitucional e observa-se a presença de conceitos das normas internacionais na normativa brasileira. Aplicou-se a análise de conteúdo em documentos, entrevistas, normas e palestras, a fim de identificar traços do modelo do Comitê das Organizações Patrocinadoras de Treadway (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO]) para Gerenciamento de Riscos Corporativos (*Enterprise Risk Management* [ERM]), conhecido como modelo "COSO ERM", e do modelo da Organização Internacional de Normalização (*International Organization for Standardization* [ISO]), conhecido como Norma ISO 31000:2009, adotados por sua relevância. Os resultados identificam que importantes atores exercem pressões para adoção dos modelos internacionais, como os próprios organismos internacionais, associações profissionais e órgãos públicos, em especial aqueles ligados à auditoria governamental. Apesar da forte influência verificada, a estruturação das normas permite a manutenção da autonomia nacional e sua customização no contexto das organizações.

Palavras-chave: gerenciamento de riscos corporativos; administração pública; COSO ERM; ISO 31000:2009; Brasil.

Incorporación de modelos internacionales de gestión de riesgos en las reglamentaciones federales

El interés en la gestión de riesgos ha crecido de manera constante, fortalecido por la difusión de modelos internacionales. En la administración pública federal de Brasil, el uso de la gestión de riesgos es reciente y se está expandiendo. Esta investigación analiza cómo las normas y directrices del gobierno federal adoptan los modelos internacionales de gestión de riesgos corporativos. Siguiendo la teoría neoinstitucional, se investigó la exposición a fuerzas coercitivas, normativas y miméticas, y la presencia de conceptos de normas internacionales en la reglamentación brasileña. Se utilizó el análisis de contenido en documentos, normas, entrevistas y seminarios para identificar los rasgos de los modelos COSO ERM e ISO 31000/2009, adoptados por su relevancia. Los resultados identifican actores importantes que ejercen presión para la adopción de modelos internacionales, como organizaciones internacionales, asociaciones profesionales y agencias públicas, especialmente las vinculadas a la auditoría gubernamental. A pesar de la fuerte influencia, la estructuración de estándares permite el mantenimiento de la autonomía nacional y su personalización en el contexto de las organizaciones.

Palabras clave: gestión de riesgos corporativos; administración pública; COSO ERM; ISO 31000-2009; Brasil.

Incorporation of international risk management standards into federal regulations

The issue of risk management has gained attention in the field of administration due to the dissemination of international frameworks. In Brazilian federal public administration, risk management is a recent and expanding practice. This research analyzes how international corporate risk management frameworks have been adopted by the federal government through regulations and guidelines. The study adopts the concepts of coercive, normative, and mimetic forces from the neo-institutional theory, and examines the presence of international norms in the Brazilian regulations. Through a qualitative approach, content analysis in documents, norms, interviews, and seminars was used to identify traits of the COSO ERM and ISO 31000/2009 frameworks, which were chosen based on relevance. Results identify important actors pushing for the use of international frameworks, such as international organizations, professional associations, and public agencies, especially those related to government audits. Despite the strong international influence, the Brazilian norms are adapted to the organizations' context and allowing the maintenance of national autonomy.

Keywords: enterprise risk management; public administration; COSO ERM; ISO 31000; Brazil.

DOI: http://dx.doi.org/10.1590/0034-761220180117
ISSN: 1982-3134
Artigo recebido em 04 abril 2018 e aceito em 09 nov. 2019.
[Versao traduzida]

1. INTRODUÇÃO

O gerenciamento de riscos corporativos é considerado um importante instrumento no arcabouço da governança corporativa. Também conhecido como "nova gestão de riscos" (Palermo, 2014), o gerenciamento de riscos corporativos é o uso da gestão de riscos de modo integral, formal e sistemático e tem sido adotado por diversos tipos de organização, inclusive do setor público (Oulasvirta & Anttiroiko, 2017).

A difusão, a adoção e o uso de gerenciamento de riscos corporativos, como uma inovação gerencial, tem sido foco de pesquisas nas últimas décadas. Sua difusão tem ocorrido de modo crescente e atinge diversas organizações pelo mundo. Porém, as pesquisas relacionadas à difusão desse instrumento no setor público ainda se restringem a países que realizaram sua adoção de modo antecipado, em geral àqueles considerados desenvolvidos (Collier & Woods, 2011; Crawford & Stein, 2005; Oulasvirta & Anttiroiko, 2017; Palermo, 2014; Woods, 2009).

Tal influência cruza países e, internacionalmente, as normas e práticas desenvolvidas em e para um contexto passam a ser aplicadas em países com diferentes contextos. Esta pesquisa analisou a influência dos modelos internacionais de gerenciamento de riscos corporativos, de origem anglo-saxã, nas normas e orientações do Governo Federal brasileiro sobre a questão. Enfocam-se os 2 modelos internacionais considerados mais relevantes: a) o modelo do Comitê das Organizações Patrocinadoras de Treadway (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO]) para Gestão de Riscos Corporativos (*Enterprise Risk Management* [ERM]), conhecido como modelo "COSO ERM"; e b) o modelo da Organização Internacional de Normalização (*International Organization for Standardization* [ISO]), conhecido como Norma ISO 31000:2009. Para tal, avaliaram-se normas, documentos e acórdãos, bem como entrevistas e palestras, utilizando uma abordagem qualitativa, por meio de análise de conteúdo (Bardin, 2011).

O COSO é formado pelas principais associações de classe de profissionais da área financeira e contábil dos Estados Unidos da América (EUA). O modelo COSO ERM foi elaborado pela empresa de origem inglesa PricewaterhouseCoopers (PwC), com a colaboração de um conselho consultivo de profissionais americanos (Hayne & Free, 2014). Já a Norma ISO 31000:2009 é derivada do modelo criado pelo Comitê de Normas da Austrália/Nova Zelândia (Standards Australia/Standards New Zealand Committee [AS/NZS]), conhecido como norma AS/NZS 4360:2004 (Leitch, 2010). Tais modelos de origem anglo-saxã têm sua gênese na busca por fraudes nos relatórios financeiros/contábeis (Delmas, 2002; Delmas & Montes-Sancho, 2011; Delmas & Montiel, 2008; Guler, Guillén, & Macpherson, 2002; Hayne & Free, 2014).

A incorporação de modelos estrangeiros não garante que a implementação da gestão de riscos será bem-sucedida. Diferentes ambientes e culturas necessitam adaptar o conteúdo de tais modelos para um ajuste ao objeto em foco, sob o risco de desvio da finalidade buscada pela norma (Dobija, 2015; Oulasvirta & Anttiroiko, 2017).

Além de contribuir com a literatura tratando de um caso na América Latina, de adoção tardia, este artigo subsidia o entendimento do processo de normalização do gerenciamento de riscos corporativos no Governo Federal brasileiro, com destaque para as forças e os atores envolvidos nesse processo.

2. A ADOÇÃO DE INOVAÇÕES GERENCIAIS NO CONTEXTO TRANSNACIONAL

Pesquisas recentes abordam a disseminação de modelos de adoção voluntária, que definem e regulam atividades (Hayne & Free, 2014), a exemplo de diversas normas da ISO (Delmas, 2002; Delmas & Montes-Sancho, 2011; Delmas & Montiel, 2008; Guler et al., 2002) e do modelo COSO ERM (Hayne & Free, 2014), entre outros modelos (Durand & McGuire, 2005; Perez-Aleman, 2010). Segundo Rogers (1995, p. 5), a difusão consiste no "processo pelo qual uma inovação é comunicada por determinados canais através do tempo por meio de membros de um sistema social".

A abordagem neoinstitucional predomina na explicação da difusão de modelos internacionais (Guler et al., 2002; Perez-Aleman, 2010). Ela enfatiza a difusão por meio do isomorfismo, que é produto de forças coercitivas, miméticas e normativas, e conduz à compatibilização das características das organizações com o ambiente (DiMaggio & Powell, 1983).

O tipo coercitivo é derivado de pressões exógenas, exercidas por outras organizações e por expectativas culturais da sociedade. Elas podem manifestar-se por meio de persuasão, convite para agir em conjunto, além de requisitos técnicos e legais. Desse modo, determinados países, bem como organismos internacionais e agências de desenvolvimento, podem impor suas expectativas aos governos, que muitas vezes são pressionados a atender a padrões considerados legitimados (DiMaggio & Powell, 1983; Dobbin, Simmons, & Garrett, 2007; Weyland, 2005). Já o isomorfismo mimético ocorre quando a organização toma o que outras organizações estão fazendo, suas soluções para problemas similares, como modelo. Normalmente ocorre quando as tecnologias são insuficientemente compreendidas ou quando há incerteza no ambiente. A reprodução das características dessas organizações pode ser involuntária ou explícita, viabilizada por meio de firmas de consultoria ou associações profissionais. As empresas adotam as práticas dessas organizações buscando aumentar sua legitimidade, para demonstrar que estão melhorando seus processos. Por fim, o isomorfismo normativo se relaciona à profissionalização, dado que membros de determinadas profissões tendem a definir métodos de trabalho. Cabe notar que essas próprias categorias profissionais sofrem pressões miméticas e coercitivas. As fontes desse isomorfismo se relacionam à educação e a uma base cognitiva. Assim, são constituídas redes de profissionais que difundem modelos organizacionais, vistos como legitimados por seus adotantes, por terem a chancela dessas redes.

Aplicando tais conceitos ao campo organizacional do setor público, governos buscam legitimidade por meio da adoção de características de soluções globais já aceitas e legitimadas (Meyer, Boli, Thomas, & Ramirez, 1997) ou procuram assemelhar-se a governos ou instituições de países que gozam de maior legitimidade (DiMaggio & Powell, 1983; Dobbin et al., 2007; Weyland, 2005). Assim, eles emulam seus pares ou utilizam modelos que se encontram disponíveis, ressaltando-se aqueles mais notáveis e acessíveis (DiMaggio & Powell, 1983; Miller & Banaszak-Holl, 2005; Soule & Earl, 2001; Strang & Soule, 1998). Os próprios indivíduos em posições políticas acabam dependendo dessa legitimidade para defender a viabilidade das soluções propostas (Amenta & Ramsey, 2010). Por fim, os governos podem adotar procedimentos padronizados pela pressão de associações profissionais e acadêmicas, assim como de organizações privadas produtoras de metodologias (DiMaggio & Powell, 1983; Hall, 1993; Strang & Soule, 1998).

Apesar de pressões similares, a resposta pode não ocorrer ao mesmo tempo. Em economias em desenvolvimento, a adoção de modelos internacionais tende a ser tardia. O que seria explicado, em parte, pela aprendizagem da inovação em outros contextos, pela necessidade de adequação da inovação

ao contexto local, o que levaria a maiores dificuldades para sua implementação, dadas as diferenças de recursos materiais e de conhecimento ou devido a diferenças culturais específicas (Perez-Aleman, 2010). Tais aspectos se aplicariam a inovações gerenciais, como gestão de riscos, cuja adoção tem sido intensificada nos últimos 20 anos, sobretudo em relação aos modelos COSO ERM e ISO 31000:2009 (Huber & Scheytt, 2013; Scheytt, Soin, Sahlin-Andersson, & Power, 2006).

3. MODELOS DE GERENCIAMENTO DE RISCOS CORPORATIVOS

O modelo conhecido como COSO II, "Gerenciamento de Riscos Corporativos – Estrutura Integrada", foi lançado em 2004. O primeiro modelo COSO[1], conhecido como COSO I surgiu em 1992, com a publicação de "Controles Internos – Estrutura Integrada", porém, não é considerado um gerenciamento de riscos corporativos, pois tem foco no controle interno.

O COSO II não substituiu o anterior, mas incorporou as questões de controle interno e introduziu a gestão de riscos pelos novos componentes e elementos incorporados. Na etapa de concepção, o COSO II contou com o auxílio da PwC e de um conselho consultivo, formado por consultores, acadêmicos e executivos. À época desse lançamento, o COSO já gozava de elevado reconhecimento por seu histórico de sucesso no estabelecimento de orientações e boas práticas (Hayne & Free, 2014). A atualização do COSO II em 2017 preservou os principais aspectos da versão anterior e tornou seu texto mais claro e abrangente. Além disso, essa versão inclui aspectos da cultura gerencial e da estratégia, com uma visão ampliada dos objetivos e dos níveis organizacionais, de modo que as organizações possam obter mais valor na realização do gerenciamento de riscos corporativos (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO], 2017).

Já o modelo da Norma ISO[2] 31000:2009 (*International Organization for Standardization* [ISO], 2009) foi desenvolvido por um comitê especial, composto por delegações de 28 países. Foram aprimorados os conceitos, as diretrizes e as práticas de normas técnicas que a precederam, como a AS/NZS 4360:2004, estabelecida pelo comitê conjunto da Austrália e da Nova Zelândia, que levou à propositura da referida norma internacional (Leitch, 2010). Diferente do COSO II, essa norma não tem abordagem prescritiva, trazendo em seu texto princípios e diretrizes gerais sobre gerenciamento de riscos corporativos.

Esses modelos têm finalidades bem similares e não apresentam conflitos entre si, devendo ocorrer um alinhamento ainda maior nos próximos anos (Moeller, 2011). Existem mais similaridades do que diferenças entre os modelos. No entanto, a ISO 31000:2009 traz uma abordagem mais simplificada (Gjerdrum & Peter, 2011). O Quadro 1 apresenta as semelhanças identificadas entre os modelos e o Quadro 2 traz algumas diferenças.

[1] O COSO é um comitê, sem fins lucrativos, dedicado à melhoria dos relatórios financeiros por meio da ética, efetividade dos controles internos e governança corporativa e surgiu com a finalidade de criar estruturas sistemáticas que dessem conta do novo cenário apresentado pelas corporações. É formado por algumas das principais associações de classe de profissionais da área financeira e contábil nos EUA.
[2] A ISO é o fórum mundial onde se busca o consenso na elaboração de normas internacionais, por meio da conciliação dos interesses de diversos segmentos da sociedade. Suas normas são desenvolvidas por meio de diversos organismos nacionais de normalização, atualmente presentes em mais de 150 países.

QUADRO 1 SEMELHANÇAS ENTRE OS MODELOS COSO ERM E ISO 31000:2009

Aspecto	Descrição
Escopo	Pode ser aplicado à organização inteira ou em níveis organizacionais inferiores. Pode ser utilizado em qualquer tipo de organização.
Conceito de risco	Considera o risco como positivo ou negativo (oportunidades ou ameaças).
Documentação	Preveem o estabelecimento de uma política de gestão de riscos. Preveem o estabelecimento de critérios para avaliação dos riscos. Estabelecem que todas as atividades de gestão de riscos devem ser documentadas.
Características	A implementação da gestão de riscos leva em consideração as necessidades específicas da organização. Processo dinâmico, iterativo, que contribui para a melhoria contínua. Integração dos riscos com os objetivos. Gestão de riscos é incorporada aos processos organizacionais. Necessidade de considerar o custo-benefício no tratamento dos riscos. O processo de gestão de riscos não garante o alcance dos objetivos.
Processo	Seguem etapas similares: estabelecimento do contexto/objetivos, identificação, análise e avaliação, tratamento, comunicação e monitoramento.

Fonte: Elaborado pelos autores.

No tocante às diferenças, ressalta-se que, em termos de responsabilização, enquanto o COSO define especificamente quem seriam os envolvidos, a ISO deixa a critério da organização definir os papéis centrais. Ainda, em relação aos papéis, verifica-se que o elevado envolvimento dos profissionais da auditoria no uso de modelos os leva a transcender as suas funções, passando a exercer atividades de consultoria nas organizações (Zwaan, Stewart, & Subramaniam, 2011).

QUADRO 2 DIFERENÇAS ENTRE OS MODELOS COSO ERM E ISO 31000:2009

Aspecto	COSO ERM	ISO 31000:2009
Orientação	Diretrizes mais detalhadas e prescritivas.	Princípios e diretrizes genéricas.
Desenvolvimento	Por entidades relacionadas a profissionais da área contábil e de auditoria.	Procedimento para criação de padrões ISO (consenso).
Responsabilidades	Estabelece responsabilidades mais específicas. Define papéis do CEO, diretoria, auditores internos e gerentes de alto nível. Afirma que os proprietários de riscos devem ser os gerentes mais próximos das potenciais questões.	A critério da organização. Definição por meio da política, do estabelecimento do contexto e de proprietários de riscos.

Fonte: Elaborado pelos autores.

4. A ADOÇÃO DO GERENCIAMENTO DE RISCOS CORPORATIVOS PELO SETOR PÚBLICO

Diversos estudos abordam a difusão e adoção de ferramentas e sistemas, que inicialmente foram desenhados para empresas privadas, mas posteriormente foram adotados pelo setor público (Jackson & Lapsley, 2003; Oulasvirta & Anttiroiko, 2017; Spano, Carta, & Mascia, 2009; Troshani, Jerram, & Hill, 2011).

Em particular, a adoção do gerenciamento de riscos corporativos pelo setor público tem sido discutida por alguns autores, a exemplo de organizações públicas do Reino Unido, e dos governos locais da Finlândia (Oulasvirta & Anttiroiko, 2017), do Reino Unido e da Austrália (Collier & Woods, 2011; Crawford & Stein, 2005; Woods, 2009).

No caso dos governos locais da Finlândia, observou-se, na maior parte, a aplicação da gestão de riscos em áreas específicas, como saúde, segurança e finanças, em vez do uso integral por meio do gerenciamento de riscos corporativos, demonstrando-se a existência de "silos". Além disso, Oulasvirta e Anttiroiko (2017) relatam a falta de percepção de benefício por parte dos gestores quando considerados os custos de implementação de gerenciamento de riscos corporativos. Verifica-se que as pressões para a adoção voluntária de modelos de gerenciamento de riscos corporativos não surtem o efeito desejado quando os gerentes seniores não aderem ao projeto. Assim, segundo os autores, as organizações do setor público seriam mais racionais e seletivas na adoção de ferramentas de gestão do que normalmente se presume (Oulasvirta & Anttiroiko, 2017).

Já no Reino Unido, a introdução do gerenciamento de riscos corporativos nos governos locais foi influenciada por auditorias de desempenho realizadas pelo governo central, que apresentavam expectativas de que os sistemas de gerenciamento de riscos corporativos fossem desenvolvidos com base em práticas e modelos profissionais já disponíveis (Palermo, 2014; Woods, 2009).

5. METODOLOGIA

Os dados foram coletados por meio do exame de normas e documentos, de entrevistas semiestruturadas e de palestras do seminário realizado pela Escola Nacional de Administração Pública (ENAP), sobre desafios para a implementação da Instrução Normativa Conjunta do Ministério do Planejamento, Desenvolvimento e Gestão (MPDG) e do Ministério da Transparência e Controladoria-Geral da União (CGU) n. 01/2016 (Escola Nacional de Administração Pública [ENAP], 2017). Os dados foram submetidos a análise de conteúdo (Bardin, 2011).

Primeiro, selecionaram-se as normas que estruturam a temática no país, entre elas: a) Referencial básico de governança (Tribunal de Contas da União [TCU], 2014); b) Lei n. 13.303 (2016); c) Instrução Normativa Conjunta MP/CGU n. 1 (2016); d) referencial de combate à fraude e à corrupção (TCU, 2017a); e e) Instrução Normativa CGU n. 03 ([CGU], 2017). Na codificação e análise comparativa (Gibbs, 2008) foram utilizadas as características apresentadas nos quadros 1 e 2.

Em seguida, observaram-se os conceitos e as recomendações dos modelos internacionais refletidos na normativa e nas decisões do Tribunal de Contas da União (TCU). Realizou-se busca na base de dados do TCU (TCU, 2017b), que identificou às vezes e as condições em que os modelos internacionais aparecem citados ou referenciados nos documentos e acórdãos desse órgão. A busca ocorreu em setembro de 2017, utilizando as palavras "COSO" e "riscos", em combinação, e o termo "31000", isoladamente. A coleta resultou em 185 acórdãos e 4 atos normativos, com as primeiras ocorrências no ano de 2006, cuja maioria se referia ao COSO I. Os modelos COSO II e ISO apareceram citados

a partir de 2010. Em relação aos atos normativos, 2 tratavam de ambos os modelos e 2 se referiam exclusivamente ao COSO ERM. Em relação aos acórdãos, 43 não mencionavam nenhum desses modelos e a maior parte deles estava relacionada ao COSO I. Dos demais acórdãos, 25 eram comuns aos 2 modelos, 99 tratavam somente do COSO II e 18 abordavam exclusivamente a ISO 31000:2009.

Por fim, foram realizadas entrevistas de caráter complementar à análise documental, com 6 especialistas em gestão de riscos, como ilustra o Quadro 3. Ressalta-se que os 2 primeiros entrevistados participaram diretamente da elaboração da Instrução Normativa Conjunta MP/CGU n. 1 (2016).

QUADRO 3 ENTREVISTAS REALIZADAS

Entrevistado	Descrição	Experiência no serviço público/privado (anos)
E1	Servidor público federal	31
E2	Servidor público federal	10
E3	Consultor privado	38
E4	Servidor público federal	20
E5	Servidor público federal	31
E6	Servidor público federal	20

Fonte: Elaborado pelos autores.

As diversas fontes de dados e métodos de tratamento tiveram a finalidade de obter a triangulação metodológica (Flick, 2007).

6. INICIATIVAS PARA A ADOÇÃO DO GERENCIAMENTO DE RISCOS CORPORATIVOS NO GOVERNO FEDERAL

O processo de adoção do gerenciamento de riscos corporativos no Governo Federal, apesar de iniciado na década de 1990, foi largamente difundido apenas em 2016. Na primeira fase, poucos órgãos se envolveram com o modelo. Após a questão ser normalizada pela Instrução Normativa Conjunta MP/CGU n. 1 (2016), a implementação dessa ferramenta passou a ter vigência no Poder Executivo federal.

As primeiras iniciativas se deram de modo fragmentado em algumas organizações do Governo Federal. O Banco Central, na década de 1990, após o advento do Plano Real, iniciou o gerenciamento de riscos financeiros. Em 2011, segundo alguns dos entrevistados (E1 e E2) e uma palestra (ENAP, 2017), o Banco Central passou a utilizar o gerenciamento de riscos corporativos de modo mais amplo.

Segundo um dos entrevistados (E2), no início da década de 2000, surgiram iniciativas no Ministério da Previdência, na Secretaria do Tesouro Nacional e na Receita Federal e, em 2013, o gerenciamento de riscos corporativos foi apresentado na esfera federal por meio do Programa Nacional de Gestão Pública e Desburocratização (Gespública) (Decreto n. 5.378, 2005), que foi descontinuado em 2017. Esse programa publicou um manual (Ministério do Planejamento, Desenvolvimento e Gestão

[MPDG], 2013), baseado em *The orange book*, do Tesouro Britânico (*Her Majesty's Treasury [HM Treasury*], 2004). No entanto, segundo alguns dos entrevistados (E1, E2), o uso da metodologia era voluntário, não ocorrendo disseminação relevante nessa ocasião.

Iniciativas mais estruturadas, que permitiram uma expansão do gerenciamento de riscos corporativos na gestão pública, ocorreram no âmbito do TCU, da CGU e, em seguida, no MPDG. Por exemplo, em 2009, visando a subsidiar um anteprojeto de lei, o TCU realizou estudo sobre controles internos, explorando modelos e verificando que outros países ampliaram seu papel, passando a tratá-los como instrumentos de gerenciamento de riscos. Em 2011, o TCU estabeleceu a melhoria do gerenciamento de riscos corporativos como objetivo estratégico. Segundo um dos entrevistados (E3), o tema continuou em destaque no planejamento estratégico de 2015.

Um importante marco no TCU foi à aplicação de questionário em 2013, para avaliar a maturidade em gestão de riscos em 65 organizações da administração indireta. A resposta por parte dos órgãos favoreceu a reflexão sobre o assunto. Ao mesmo tempo, segundo um dos entrevistados (E1), a realização do levantamento demonstrou que o TCU apoiava a temática naquele momento. Assim tal estabelecimento de requisitos técnicos e as expectativas desse órgão sobre a temática levaria a uma pressão coercitiva e, ao mesmo tempo, a uma pressão normativa por parte dos profissionais da área de auditoria governamental.

Na CGU, um marco foi um convite à Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em 2009. Realizou-se visita e produziu-se um relatório sobre o sistema de integridade da administração pública federal brasileira (ENAP, 2017; *Organisation for Economic Cooperation and Development* [OECD], 2012). Dentre as recomendações do relatório, ressalta-se: "integrar a gestão de riscos como elemento-chave da responsabilidade gerencial, de modo a promover a integridade e prevenir a improbidade, os desvios e a corrupção" (OECD, 2012, p. 19). O relatório apontou lacunas na gestão de riscos e destacou o papel de orientação da CGU. Com isso, o assunto passou a ser estudado de maneira mais intensa na CGU. Tais esforços foram contemplados por financiamento do Banco Interamericano de Desenvolvimento (BID), no programa de Fortalecimento da Prevenção e Combate à Corrupção na Gestão Pública Brasileira (Proprevine), que, entre outras temáticas, abrangia a gestão de riscos. Em 2012 se formou um grupo de trabalho que buscava estabelecer um referencial metodológico de gestão de riscos para a administração pública (E1).

Em 2016, o Ministro Valdir Simão, ex-ministro da CGU e nomeado Ministro do Planejamento, que acompanhava o trabalho da OCDE, propôs a instrumentalização dos gestores públicos para a implementação da gestão de riscos (E1). Dessa forma, conjuntamente com a CGU, liderada, à época, pelo Ministro Luiz Navarro, que também havia acompanhado os trabalhos da OCDE, decidiu-se pela elaboração e publicação da Instrução Normativa Conjunta MP/CGU n. 1 (2016), normalizando a aplicação dessa metodologia no Poder Executivo federal (E1, E2). Essa agenda levou a outros eventos importantes sobre o tema, com reflexos na governança da administração pública federal, culminando na publicação do Decreto n. 9.203 (2017) e no encaminhamento de um projeto de lei, nos quais a gestão de riscos é explicitamente tratada (E1).

7. ANÁLISE DAS NORMAS, ORIENTAÇÕES E ACÓRDÃOS

Esta pesquisa revelou maior presença do modelo do COSO nos documentos analisados. O modelo do COSO surgiu antes do modelo da ISO e logo conquistou reconhecimento, inicialmente como uma discussão de controles internos. Tal modelo é patrocinado por cinco importantes organizações

americanas, dentre elas o *Institute of Internal Auditors* (IIA) o que demonstra a sua popularidade entre os profissionais de auditoria. Ele também é apoiado pela *International Organization of Supreme Audit Institutions* (INTOSAI), pelo BID, pelo Banco Mundial e pelo *Government Accountability Office* (GAO) dos EUA (TCU, 2009).

Já a ISO 31000:2009 surgiu somente em 2009. Segundo um dos entrevistados (E1), a ISO trouxe um ponto de vista mais prático, enquanto o COSO era mais doutrinário. Outro ponto favorável a esse modelo é que a ISO, como organização normalizadora internacional era mais conhecida do que o COSO, já estava presente em diversos países com vistas à definição de normas das mais variadas naturezas, como metrologia, segurança alimentar, sistemas de qualidade e proteção ambiental, entre outras.

A aceitação de tais modelos, segundo alguns dos entrevistados (E1, E4), era facilitada pelas organizações de elevado prestígio concebendo e apoiando os modelos, o que lhes confere legitimação, fornecendo segurança para a sedimentação do gerenciamento de riscos corporativos no setor público. Outro entrevistado (E4) destaca que o uso de modelos facilita a padronização dos conceitos e da linguagem.

As menções aos modelos nas normas e nos acórdãos evidenciam a influência que eles possuem. Ao avaliar o significado dos trechos presentes nesses documentos, verificam-se, principalmente, recomendações de aplicação dos modelos e o reconhecimento de que são importantes referências para o gerenciamento de riscos corporativos, em função de sua legitimidade, credibilidade e aceitação. O Quadro 4 demonstra exemplos desses trechos.

QUADRO 4 INFLUÊNCIAS DOS MODELOS NA GESTÃO DE RISCOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Documento	Trecho do documento
Portaria n. 189/2009 (TCU, 2009a)	[...] **a utilização do modelo COSO como referência** de análise, enfatizando a gestão dos riscos corporativos, com base em princípios de boa governança [...] (p. 2).
Acórdão n. 1.233/2012, Ata 19/2012 – Plenário (TCU, 2012)	[...] esses países adotam modelos de controle interno convergentes, calcados em gerenciamento de riscos e em estruturas de governança e que esses modelos têm por base os principais documentos relacionados à gestão de risco e controles internos **reconhecidos internacionalmente, como o COSO I/II**, o padrão AS/NZS 4360 e as diretrizes para as Normas de controle Interno do Setor Público, da INTOSAI. [...] foi concluído com sugestão de anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal, incluindo uma seção tratando "Da Gestão de Riscos, do Controle Interno e da Governança Corporativa", o que contribui para que sejam positivadas no ordenamento jurídico brasileiro boas práticas para a adequada governança corporativa **contidas em marcos de referência, como Coso I e II**, **reconhecidos mundialmente**.
Acórdão n. 7.128/2013, Ata 43 – Segunda Câmara (TCU, 2013)	[...] a promoção de trabalhos de avaliação de riscos, utilizando como referência **modelos consagrados, a exemplo do Coso** II [...].

Continua

Documento	Trecho do documento
Acórdão n. 242/2015, Ata 5/2015 – Plenário (TCU, 2015a)	Como critérios de auditoria, de modo a possibilitar análise abrangente do tema, foram utilizados **como referência modelos de avaliação de riscos e controles bem estabelecidos, em especial o framework Coso ERM e a norma ABNT NBR-ISO 31000:2009**. O Coso ERM [...] [com o] intuito de disseminar uma consciência sobre riscos e controles por toda a entidade e tornar-se um modelo comum para a discussão e a avaliação de riscos organizacionais [...] o cumprimento e a observância das suas recomendações, relativas aos controles internos, são amplamente praticados e **tidos como modelo de referência no Brasil e na maioria dos países do mundo**. [...] A ABNT NBR-ISO 31000:2009 [...] **costuma ser adotada como referência para a realização de benchmark** de processos relativos à gestão de riscos.
Acórdão n. 1.294/2015, Ata 19/2015 – Plenário (TCU, 2015b)	[...] elaborados com base em **modelos internacionais (em especial, o Coso ERM e a ISO 31000:2009)** [...].
Acórdão n. 729/2017, Ata 12/2017 – Plenário (TCU, 2017c)	[...] considerando as recomendações das **melhores práticas internacionais que tratam da gestão de riscos corporativos**, como **o COSO/ERM** e as normas INTOSAI GOV 9130/2007 e **ABNT NBR ISO 31000:2009**. [...] incorporando ao seu texto as melhores práticas internacionais estabelecidas nesta área [...] dos **principais frameworks de gestão de riscos**, como [a norma] **ISO 31000:2009** e modelos do Committee of Sponsoring Organizations of the Treadway Commission – **COSO I e II** [...].

Fonte: Elaborado pelos autores.

Nos trechos mencionados, o modelo é associado a: a) "melhores práticas internacionais"; b) "referência para a realização de *benchmark*"; c) "modelos consagrados"; d) "[modelos] reconhecidos internacionalmente"; e e) "marcos de referência", o que, ao mesmo tempo, confere legitimidade aos modelos e às normas e aos entendimentos construídos, por estarem baseados em algo legítimo e aceito internacionalmente.

Na pesquisa, surgiram menções a outros modelos, mas em frequência menor do que aos aqui estudados, como apresentado no Quadro 5. Tais modelos têm forte relação com os dois modelos abordados neste estudo, com exceção do modelo do Reino Unido, que reconhece os outros modelos, mas não afirma basear-se neles.

QUADRO 5 OUTROS MODELOS IDENTIFICADOS NOS ACÓRDÃOS

Modelo	Descrição
INTOSAI GOV 9130	Possui foco direcionado ao setor público e, em seu prefácio, afirma ser baseado no COSO II (**International Organization of Supreme Audit Institutions** [INTOSAI], 2007, p. 5). Acórdãos analisados na pesquisa denominam o modelo COSO-INTOSAI.
AS/NZS 4360:2004	Criada pelo comitê conjunto da Austrália e da Nova Zelândia, constitui um precursor da ISO 31000:2009 (Leitch, 2010).

Continua

Modelo	Descrição
Canadense	Específico para o setor público, serve como guia para implementação e operação do gerenciamento de riscos corporativos no governo canadense. O próprio documento apresenta seu alinhamento com a ISO 31000, em seu item 2.2: "o modelo [...] reflete, quando apropriado, padrões internacionais e nacionais relacionados ao gerenciamento de riscos, incluindo a norma de gerenciamento de riscos da ISO 31000" (Government of Canada, 2012).
GAO	Específico para o setor público, mas voltado para controles internos. Verifica-se a forte influência do COSO I. É citado em seu texto que esse modelo adapta os princípios do COSO para o ambiente governamental (Government Accountability Office [GAO], 2014).
Secretaria do Tesouro do Reino Unido	Específico para o setor público, traz orientações gerais sobre gerenciamento de riscos corporativos. Declara não haver um padrão em gerenciamento de riscos corporativos em organizações governamentais e afirma que as organizações podem optar por padrões específicos, como: AS/NZS 4360:2004, COSO ERM e o canadense (HM Treasury, 2004).

Fonte: Elaborado pelos autores.

Utilizando os fatores apresentados nos quadros 1 e 2 foram encontrados diversos aspectos dos modelos estudados nas principais normas selecionadas que orientam o gerenciamento de riscos corporativos na administração federal brasileira. O Quadro 6 descreve a análise realizada com publicações que abordam o gerenciamento de riscos corporativos como um de seus assuntos, isto é, elas não são específicas.

QUADRO 6 PUBLICAÇÕES DO GOVERNO FEDERAL QUE ABORDAM A GESTÃO DE RISCOS

Publicação	Descrição
Referencial básico de governança (TCU, 2014)	Menciona diversos aspectos da gestão de riscos, por ser assunto relacionado à governança. Cita ambos os modelos e afirma que o COSO II "ainda hoje **é tido como referência** no tema gestão de riscos" (TCU, 2014, p. 4). Possui como componente: "gestão de riscos e controle interno". Para conceituar risco, cita a ISO 31000. São citados também o COSO II e a INTOSAI GOV 9130 (TCU, 2014, p. 26). As práticas apresentadas no componente estão alinhadas com os modelos, a exemplo da necessidade de estabelecer uma política de gerenciamento de riscos e de assegurar sua integração aos processos organizacionais.
Lei n. 13.303 (2016)	Estabelece práticas de governança para empresas públicas, sociedades de economia mista e suas subsidiárias, incluindo responsabilidades sobre gerenciamento de riscos corporativos.
Instrução Normativa CGU n. 03 (CGU, 2017)	Estabelece princípios e diretrizes para a prática profissional da auditoria interna, incluindo a avaliação de gerenciamento de riscos corporativos. Dedica um tópico ao gerenciamento de riscos, no qual aborda as etapas do processo de gerenciamento, as responsabilidades e as questões que devem ser consideradas na avaliação.

Fonte: Elaborado pelos autores.

Duas normas analisadas têm a gestão de riscos como seu principal assunto: a) o referencial de combate à fraude e corrupção (TCU, 2017a), que é específico para riscos relacionados a essa temática; e b) a Instrução Normativa Conjunta MP/CGU/PR n. 1 (2016), que traz orientações gerais e determina, a implementação da gestão de riscos no âmbito de todos os órgãos e entidades do Poder Executivo federal.

O referencial de combate à fraude e corrupção cita diretamente os modelos estudados, recomendando seu uso. Além disso, aponta que o COSO é o modelo de gestão de riscos predominante no cenário corporativo internacional, em especial no norte-americano, e dedica um tópico específico para a norma técnica brasileira (NBR) ISO 31000:2009. Além disso, cita que adaptações desses modelos deram origem a modelos aplicados ao setor público, a exemplo do modelo do GAO (TCU, 2017a).

Alguns trechos da Instrução Normativa Conjunta MP/CGU/PR n. 1 (2016) são praticamente idênticos aos modelos analisados aqui, a exemplo do princípio que trata da gestão de riscos ser "sistemática, estruturada e oportuna" (ISO, 2009, p. 7). Ademais, adotam a estrutura do modelo por componentes, os quais são idênticos aos componentes do COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO], 2004, p. 7). Tal percepção é confirmada pelo TCU (2017a, p. 25): "a parte de gestão de risco desta [Instrução Normativa] IN é baseada no Coso II".

A percepção de entrevistados (E1, E2, E3), em especial daqueles que participaram da elaboração da Instrução Normativa Conjunta MP/CGU/PR n. 1 (2016), é de que as principais referências utilizadas na elaboração da instrução são o COSO e a ISO 31000:2009. Um desses entrevistados (E2) acrescentou, ainda, que *The orange book* (HM Treasury, 2004) foi usado como uma das principais referências.

O Quadro 7 ilustra características dessas normas relacionadas aos modelos estudados.

QUADRO 7 CARACTERÍSTICAS DE PUBLICAÇÕES ORIENTADORAS EM GERENCIAMENTO DE RISCOS CORPORATIVOS NO GOVERNO FEDERAL

Norma	Instrução Normativa Conjunta MP/CGU n. 1 (2016)	Referencial de combate à fraude e corrupção (TCU, 2017a)
Escopo	Órgãos e entidades como um todo. "Art. 1º Os órgãos e entidades do poder executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança." "Art. 3º [...] § 3º Os componentes dos controles internos da gestão e do gerenciamento de riscos aplicam-se a todos os níveis, unidades e dependências do órgão ou da entidade pública."	Integra a sistemática de risco da organização e abrange todos os níveis organizacionais. "[...] deve estar integrada à atividade de gestão de riscos da organização, que é uma atividade mais ampla, pois inclui uma visão sistêmica dos riscos mais relevantes a que a organização está submetida" (TCU, 2017a, p. 23). "[...] o referencial foi concebido para ajudar qualquer organização pública" (TCU, 2017a, p. 12).
Conceito de risco	"Art. 2º [...] XIII – risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos."	Aceita riscos positivos ou negativos, alinhando-se aos modelos: "[...] para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos ou maximizar o aproveitamento de oportunidades" (TCU, 2017a, p. 24).

Continua

Norma	Instrução Normativa Conjunta MP/CGU n. 1 (2016)	Referencial de combate à fraude e corrupção (TCU, 2017a)
Documentação	Dedica a seção IV à política de gestão de riscos, determinando que seja instituída pelos órgãos do Poder Executivo federal.	A política de gestão de riscos aplica-se em virtude de afirmar que deve estar integrada à gestão de riscos da organização, e menciona a Instrução Normativa Conjunta MP/CGU/PR n. 1 (2016).
	Dispõe que a política deverá estabelecer os critérios. "Art. 17 [...] II [...] b) como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos."	"Essa etapa também define os critérios de escopo e de risco para o resto do processo" (TCU, 2017a, p. 27).
	A determinação de instituição da política, contendo diversas diretrizes, e a posterior avaliação pela CGU, demonstra ser necessária a realização dos atos de maneira documentada.	"Documentar e atribuir responsabilidade pelos riscos e controles é importante" (TCU, 2017a, p. 28).
Características	"Art. 3º [...] § 5º Controles internos da gestão adequados [...] devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, complexidade, estrutura e missão do órgão ou da entidade pública."	"As medidas antifraude e anticorrupção não devem ser aplicadas uniforme e indistintamente em todas as organizações. Cada organização deve avaliar quais medidas são apropriadas para os seus riscos e benefícios esperados, considerando o seu tamanho, a sua natureza e a sua complexidade específica" (TCU, 2017a, p. 32).
	"Art. 14 [...] I – gestão de riscos de forma sistemática, estruturada e oportuna [...]. Art.14 [...] V – "[...] apoio à melhoria contínua dos processos organizacionais."	"[...] implementada e aplicada de forma sistemática, estruturada e oportuna" (TCU, 2017a, p. 24).
	"Art. 15 [...] II – aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis."	"[...] gerenciar riscos [...] de modo a criar as condições para o alcance dos objetivos e de seus propósitos" (TCU, 2017a, p. 24).
	"Art.14 [...] V – utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais."	"[...] deve ser considerado pela organização em suas atividades" (TCU, 2017a, p. 22).
	"Art.14 [...] III – estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização."	"O benefício decorrente da implementação de controles antifraude e anticorrupção deve ser maior que o seu custo" (TCU, 2017a, p. 33).
	Não garante o alcance de objetivos. "Art. 2º [...] VII – [...] fornecer razoável certeza quanto ao alcance dos objetivos da organização."	"[...] aumenta a eficácia no atingimento de objetivos" (TCU, 2017a, pp. 25-26).
Processo	Na seção III, segue exatamente os mesmos componentes do COSO ERM.	"[...] identificando-os, analisando-os e, em seguida, avaliando se devem ser modificados por algum critério" (TCU, 2017a, p. 24).

Continua

Norma	Instrução Normativa Conjunta MP/CGU n. 1 (2016)	Referencial de combate à fraude e corrupção (TCU, 2017a)
Orientação	Diretrizes gerais.	Específica para riscos relacionados à fraude e corrupção. Prescreve mecanismos e componentes.
Desenvolvimento	MP e CGU (administração e auditoria interna).	TCU (auditoria externa).
Responsabilidades	Discorre sobre responsabilidades em diversos momentos no texto e dedica a seção V exclusivamente a isso.	Recomenda a designação de responsabilidades de maneira coordenada.

Fonte: Elaborado pelos autores.

A Instrução Normativa Conjunta MP/CGU n. 1 (2016) traz diretrizes gerais, de modo que os órgãos possam ter certa autonomia para a customização de seus modelos de gestão de riscos. No entendimento de um dos entrevistados (E1), a norma é doutrinária, não estabelece um rito específico, havendo flexibilidade para uso em diversos tipos de organizações. Por outro lado, observa-se maior especificidade do que nos modelos estudados, havendo determinações quanto a responsabilidades, instituição de comitês e etapas a cumprir. Um exemplo disso é a determinação às entidades sobre a política de gestão de riscos a instituir. Apontam-se diversos aspectos que devem constar na política, além de determinar-se um prazo para que entrasse em vigor.

8. ANÁLISE DA DIFUSÃO

A análise de documentos e normas relacionados à gestão de riscos na administração pública federal mostra o protagonismo dos órgãos de controle no incentivo ao uso desse instrumento pelos gestores. A própria Instrução Normativa Conjunta MP/CGU n. 1 (2016) corrobora o papel da auditoria interna no fomento à aplicação do gerenciamento de riscos, em seu art. 2, III: "[...] auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos [...]". Tal resultado vai ao encontro das tendências observadas por Maijoor (2000), de crescimento dos sistemas de controle interno, que estão intimamente relacionados à gestão de riscos, fazendo parte das reformas empreendidas na governança corporativa de diversas nações, também trazendo o aumento da relevância dos auditores internos. Esse papel da auditoria também pode observado em outros países (Zwaan et al., 2011).

Verificou-se que, na administração pública federal, a normalização mais antiga que aborda o gerenciamento de riscos corporativos data de 2014 e que o primeiro acórdão a mencionar um modelo específico de gerenciamento de riscos corporativos é de 2010. Tal fato demonstra não só a atualidade do assunto no país, mas também, como ressaltado em uma das entrevistas (E1), a existência de determinado intervalo de tempo para a repercussão de modelos internacionais no contexto brasileiro, tendo em vista que o COSO ERM foi lançado em 2004. Outro motivo para essa demora pode associar-se à racionalidade e seletividade para a adoção de inovações gerenciais no setor público, como observado por Oulasvirta e Anttiroiko (2017). Ainda nessa mesma linha de análise, não foi possível observar influências da última atualização do COSO ERM, realizada em 2017, em virtude do curto horizonte de tempo entre seu lançamento e o desenvolvimento do estudo relatado neste artigo.

Essa cronologia permite concluir que antes que os próprios gestores atentassem para o gerenciamento de riscos corporativos, este já constituía uma preocupação no órgão de controle externo. Segundo alguns dos entrevistados (E1, E4), os auditores iniciaram a recomendação das práticas embasando seus argumentos nos modelos internacionais até o momento da efetiva institucionalização do gerenciamento de riscos corporativos. Além disso, a primeira normativa sobre o assunto foi publicada pelo órgão de controle externo (TCU, 2014). O Poder Executivo regulamentou a gestão de riscos apenas em 2016, em conjunto com o órgão de controle interno, por meio da Instrução Normativa Conjunta MP/CGU n. 1 (2016).

Alinhado a isso, um dos entrevistados (E4) reforçou a importância do TCU para a introdução do gerenciamento de riscos corporativos na administração pública federal. Em parte, o pioneirismo pode ser atribuído à influência internacional da INTOSAI: "o Tribunal de Contas da União, como membro da INTOSAI, também reconhece e utiliza o modelo [COSO I] como base para as suas avaliações [...]" (TCU, 2009b, p. 10)[3]. Alguns dos entrevistados (E1, E4, E5, E6) apontam, na mesma linha, o papel de associações profissionais como importantes difusoras desses modelos.

Assim, o isomorfismo normativo se mostra bem presente, tendo em vista a forte estruturação das categorias profissionais diante do gerenciamento de riscos corporativos. No setor público brasileiro, o gerenciamento de riscos corporativos surge principalmente nos órgãos relacionados à auditoria, ainda que o risco constitua uma preocupação do gestor. Nessa área, o COSO goza de grande reconhecimento, o que já vem de longa data, devido ao uso do COSO I. Este está presente nas universidades, fazendo parte, principalmente, do cabedal de profissionais da área contábil e de auditoria.

O gerenciamento de riscos corporativos é um instrumento muito recente, sobretudo no setor público. Desse modo, o insuficiente domínio dessa técnica também favorece o isomorfismo mimético, por meio da adoção de modelos disponíveis, de fácil acesso, como os estudados.

Os entrevistados mencionaram suas próprias experiências pessoais com os estudos sobre os modelos no meio acadêmico. Alguns deles (E2, E5) realizaram cursos acerca dos modelos específicos, como a AS/NZS 4360:2004. Outro estudou por conta própria (E1). Os entrevistados atuaram como docentes em cursos de especialização para a CGU, em 2008 e 2009 (p. ex., E1), e em cursos privados, que passaram a ter maior procura por parte de servidores (p. ex., E5). Observa-se, ainda, a disseminação do conhecimento por meio de processos de seleção de pessoal. Alguns deles obtiveram conhecimento sobre gerenciamento de riscos corporativos enquanto estavam em um órgão e depois foram utilizá-los em outro órgão (E2, E4).

Assim, de acordo com o isomorfismo mimético, verifica-se que a difusão desses modelos ocorre de maneira involuntária, por meio de servidores que tiveram acesso aos modelos em aulas, palestras e treinamentos. Ocorre, igualmente, de modo voluntário, tendo em vista que grandes firmas de consultoria promovem tais modelos, a exemplo da PwC, que participou da elaboração do COSO ERM. Além disso, organismos e agências internacionais, como a OCDE, têm recomendado o uso de instrumentos de gerenciamento de riscos corporativos no Brasil. Assim, evidenciam-se influências relacionadas ao isomorfismo coercitivo. Da mesma forma, pressões coercitivas são observadas nas expectativas dos próprios órgãos de controle.

[3] Em 2007, a INTOSAI atualizou as diretrizes para padrões de controles internos do setor público incorporando o COSO II (INTOSAI, 2007).

Cabe ressaltar que os esforços para a implementação de um modelo abrangente nas normas e orientações do Governo Federal, contemplando os riscos de forma integral em suas diversas unidades, evita a abordagem fragmentada da implementação da gestão de riscos por setores observados no caso finlandês (Oulasvirta & Anttiroiko, 2017).

9. CONCLUSÕES

Observou-se forte influência de modelos internacionais, como era de esperar. Modelos como o COSO ERM e a Norma ISO 31000:2009 foram usados como base para os esforços de implementação da gestão de riscos na administração pública federal, em busca de um legado aceito internacionalmente. Contudo, a presença dos modelos considerados referências internacionais nas normativas do TCU e de outros órgãos federais não garante sua aplicação. A efetiva adoção depende de diversos fatores, como liderança e promoção do instrumento (Oulasvirta & Anttiroiko, 2017). Como a gestão de riscos traz uma lógica diferente da ação no setor público, pode mostrar-se de difícil institucionalização. Um exemplo é oferecido por Azevedo, Aquino, Lino e Cavelmoretti (2019): a gestão de riscos e providências obrigatórias segundo a Lei Complementar n. 101 (Lei de Responsabilidade Fiscal, 2000) é realizada de modo cerimonial pelos governos analisados. Ou seja, sua adoção não é efetiva.

Apesar das forças coercitivas e normativas presentes que levaram o modelo de riscos a ser incluído na normativa do Governo Federal e de órgãos de controle externo, a real adoção da gestão de riscos de modo generalizado pelos órgãos executivos na gestão pública ainda parece ser um passo distante.

A influência do modelo de gestão de riscos de origem anglo-saxã analisada não é, necessariamente, de um país específico, mas de organismos internacionais que promovem e disseminam tais práticas. O modelo do COSO é patrocinado por associações norte-americanas e elaborado por uma das 4 maiores e mais reconhecidas empresas de auditoria do mundo (Big 4), a PwC, de origem londrina, enquanto o modelo da ISO tem suas raízes no modelo previamente elaborado pelo AS/NZS.

As organizações que legitimam a adoção de tais normas são internacionais e de natureza profissional. Entre elas se encontram: a) as organizações não governamentais (ONGs) com atuação supranacional, a exemplo da OCDE e do BID; b) os consultores e as firmas de consultoria; c) a academia; d) as associações profissionais, principalmente aquelas relacionadas à profissão contábil e à área de auditoria, como a INTOSAI e o IIA; e e) os órgãos e os especialistas do próprio governo, tidos como referências por sua capacidade técnica.

Destaca-se que, apesar das normas brasileiras estudadas apresentarem elevado vínculo com os modelos internacionais, a forma como são estruturadas, como diretrizes gerais, possibilita a manutenção da autonomia nacional e sua customização no contexto das organizações. Futuras pesquisas podem aprofundar a institucionalização (bem-sucedida ou não) do gerenciamento de riscos corporativos nas organizações do setor público e como têm alterado o comportamento dos gestores e a condução das políticas públicas, dos serviços e do tipo de controle exercido pelos órgãos internos dessas organizações.

REFERÊNCIAS

Amenta, E., & Ramsey, K. M. (2010). Institutional theory. In K. T. Leicht, & J. C. Jenkins (Eds.), *Handbook of politics: State and society in global perspective* (pp. 15-39). New York, NY: Springer.

Azevedo, R. R., Aquino, A. C. B., Lino, A. F., & Cavelmoretti, G. (2019). A precariedade do conteúdo informacional dos anexos de riscos fiscais de municípios brasileiros. *Advances in Scientific and Applied Accounting*, *12*(2), 4-22.

Bardin, L. (2011). *Análise de conteúdo*. Lisboa, Portugal: Ed. 70.

Collier, P. M., & Woods, M. (2011). A comparison of the local authority: adoption of risk management in England and Australia. *Australian Accounting Review*, *21*(2), 111-123.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk* management: integrated framework. Jersey City, NJ: Autor.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: integrating risk with strategy and performance*. Jersey City, NJ: Autor.

Crawford, M., & Stein, W. (2005). "Second order" change in UK local government: the case of risk management. *International Journal of Public Sector Management*, *18*(5), 414-423.

Decreto n. 5.378, de 23 de fevereiro de 2005. (2005). Institui o Programa Nacional de Gestão Pública e Desburocratização – GESPÚBLICA e o Comitê Gestor do Programa Nacional de Gestão Pública e Desburocratização, e dá outras providências. Brasília, DF.

Decreto n. 9.203, de 22 de novembro de 2017. (2017). Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF.

Delmas, M. (2002). The diffusion of environmental management standards in Europe and in the United States: an institutional perspective. *Policy Sciences*, *35*, 91-119.

Delmas, M., & Montes-Sancho, M. J. (2011). An institutional perspective on the diffusion of international management system standards: the case of the environmental management standard ISO 14001. *Business Ethics Quarterly*, *21*(1), 103-132.

Delmas, M., & Montiel, I. (2008). The diffusion of voluntary international management standards: responsible care, ISO 9000, and ISO 14001 in the chemical industry. *Policy Studies Journal*, *36*(1), 65-93.

DiMaggio, P., & Powell, W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*, 147-160.

Dobbin, F., Simmons, B., & Garrett, G. (2007). The global diffusion of public policies: social construction, coercion, competition, or learning? *Annual Review of Sociology*, *33*(1), 449-472.

Dobija, D. (2015). Exploring audit committee practices: oversight of financial reporting and external auditors in Poland. *Journal of Management & Governance*, *19*(1), 113-143.

Durand, R., & McGuire, J. (2005). Legitimating agencies in the face of selection: the case of AACSB. *Organization Studies*, *26*(2), 165-196.

Escola Nacional de Administração Pública. (2017). *Seminário Gestão de Riscos: desafios para implementação da Instrução Normativa Conjunta MP/CGU* (arquivo de vídeo). Recuperado de https://www.youtube.com/watch?v=Qvc-PoPxNyQ&t=3740s

Flick, U. (2007). *Managing quality in qualitative research*. London, England: SAGE.

Gibbs, G. (2008). *Analyzing qualitative data*. London, England: SAGE.

Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management: a comparison of ISO 31000:2009 and the COSO ERM framework. *Risk Management*, *31*(2), 8-13.

Government Accountability Office. (2014). *Standards for Internal Control in the Federal Government* (GAO-14-704G). Washington, DC: Autor.

Government of Canada. (2012). *Guide to integrated risk management: a recommended approach for developing a corporate risk profile*. Recuperado de: https://www.canada.ca/en/treasury-board-

secretariat/corporate/risk-management/guide-integrated-risk-management.html#toc1_1

Guler, I., Guillén, M., & Macpherson, J. M. (2002). Global competition, institutions, and the diffusion of organizational practices: the international spread of ISO 9000 quality certificates. *Administrative Science Quarterly*, *47*(2), 207-232.

Hall, P. A. (1993). Policy paradigms, social learning, and the state: the case of economic policymaking in Britain. *Comparative Politics*, *25*(3), 275-296.

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*, *39*(5), 309-330.

Her Majesty's Treasury. (2014). *The orange book: management of risk – principles and concepts*. Recuperado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Huber, C., & Scheytt, T. (2013). The dispositif of risk management: reconstructing risk management after the financial crisis. *Management Accounting Research*, *24*(2), 88-99.

Instrução Normativa CGU n. 03, de 9 de junho de 2017. (2017). Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Recuperado de https://www.cgu.gov.br/sobre/legislacao/instrucoes-normativas

Instrução Normativa Conjunta MP/CGU n. 1, de 10 de maio de 2016. (2016). Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Recuperado de *https://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf*

International Organization for Standardization. (2009). *Risk management: principles and guidelines* (31000:2009). Geneva: Autor.

International Organization of Supreme Audit Institutions. (2007). *Guidelines for internal control standards for the public sector: further information on entity risk management* (INTOSAI GOV 9130). Brussels, Belgium: Autor.

Jackson, A., & Lapsley, I. (2003). The diffusion of accounting practices in the new "managerial" public sector. *International Journal of Public Sector Management*, *16*(5), 359-372.

Lei n. 13.303, de 30 de junho de 2016. (2016). Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Brasília, DF.

Lei Complementar n. 101, de 4 de maio de 2000. (2000). Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Brasília, DF.

Leitch, M. (2010). ISO 31000:2009 – the new international standard on risk management. *Risk Analysis*, *30*(6), 887-892.

Maijoor, S. (2000). The internal control explosion. *International Journal of Auditing*, *4*(1), 101-109.

Meyer, J. W., Boli, J., Thomas, G. M., & Ramirez, F. O. (1997). World society and the nation-State. *American Journal of Sociology*, *103*(1), 144-181.

Miller, E. A., & Banaszak-Holl, J. (2005). Cognitive and normative determinants of State policymaking behavior: lessons from the sociological institutionalism. *Publius*, *35*(2), 191-216.

Ministério do Planejamento, Desenvolvimento e Gestão. (2013). *Guia de orientação para o gerenciamento de riscos: versão final*. Recuperado de http://www.gespublica.gov.br/sites/default/files/documentos/p_vii_risco_oportunidade.pdf

Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Organisation for Economic Cooperation and Development. (2012). *OECD integrity review of Brazil: managing risks for a cleaner public service* (OECD Public Governance Reviews). Paris, France: OECD Publishing.

Oulasvirta, L., & Anttiroiko, A. V. (2017). Adoption of comprehensive risk management in local government. *Local Government Studies*, *43*(3), 1-26.

Palermo, T. (2014). Accountability and expertise in public sector risk management: a case study. *Financial Accountability & Management*, *30*(3), 322-341.

Perez-Aleman, P. (2010). Collective learning in global diffusion: spreading quality standards in a developing country cluster. *Organization Science*, *22*(1), 173-189.

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York, NY: The Free Press.

Scheytt, T., Soin, K., Sahlin-Andersson, K., & Power, M. (2006). Introduction: organizations, risk and regulation. *Journal of Management Studies*, *43*(6), 1331-1337.

Soule, S., & Earl, J. (2001). The enactment of State-level hate crime law in the United States: intrastate and interstate factors. *Sociological Perspectives*, *44*(3), 281-305.

Spano, A., Carta, D., & Mascia, P. (2009). The impact of introducing an ERP system on organizational processes and individual employees of an Italian regional government organization. *Public Management Review*, *11*(6), 791-809.

Standards Australia/Standards New Zealand (2004) Australian/New Zealand Standard AS/NZS 4360:2004: *Risk Management*. Homebush, NSW: Standards Australia / Wellington: Standards New Zealand.

Strang, D., & Soule, S. A. (1998). Diffusion in organizations and social movements: from hybrid corn to poison pills. *Annual Review of Sociology*, *24*(1), 265-290.

Tribunal de Contas da União. (2009b). *Critérios gerais de controle interno na administração pública: um estudo dos modelos e das normas disciplinadoras em diversos países*. Brasília, DF: Autor.

Tribunal de Contas da União. (2009a). *Portaria 189/2009.* Aprova a realização do projeto contas. Recuperado de https://pesquisa.apps.tcu.gov.br/#/redireciona/ato-normativo/%22ATO-NORMATIVO-77379%22

Tribunal de Contas da União. (2012). *Acórdão 1.233/2012, Ata 19/2012 – Plenário*. Recuperado de https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1233850%22

Tribunal de Contas da União. (2013). *Acórdão n. 7.128/2013, Ata 43 – Segunda Câmara*. Recuperado de https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1295060%22

Tribunal de Contas da União. (2014). *Referencial básico de governança aplicável a órgãos e entidades da administração pública*. Brasília, DF: Autor.

Tribunal de Contas da União. (2015a). *Acórdão n. 242/2015, Ata 5/2015 – Plenário.* Recuperado de https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1371785%22

Tribunal de Contas da União. (2015b). *Acórdão n. 1.294/2015, Ata 19/2015 – Plenário.* Recuperado de https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1420727%22

Tribunal de Contas da União. (2017a). *Referencial de combate à fraude e corrupção: aplicável a órgãos e entidades da Administração Pública*. Brasília, DF: Autor.

Tribunal de Contas da União. (2017b). *Pesquisa integrada do TCU*. Recuperado de http://portal.tcu.gov.br/inicio/index.htm

Tribunal de Contas da União. (2017c). *Acórdão n. 729/2017, Ata 12/2017 – Plenário.* Recuperado de https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2251050%22

Troshani, I., Jerram, C., & Hill, S. R. (2011). Exploring the public sector adoption of HRIS. *Industrial Management and Data Systems*, *111*(3), 470-488.

Weyland, K. (2005). Theories of policy diffusion: lessons from Latin American pension reform. *World Politics*, *57*(2), 262-295.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, *20*(1), 69-81.

Zwaan, L., Stewart, J., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, *26*(7), 586-604.

Flávio Sergio Rezende Nunes de Souza

https://orcid.org/0000-0001-6024-5200
Mestre em Administração pela Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas (FGV EBAPE); Gabinete de Segurança Institucional da Presidência da República (GSI-PR).
E-mail: flavio.nunes@marinha.mil.br

Marcus Vinícius de Azevedo Braga

https://orcid.org/0000-0002-7399-0952
Doutor em Políticas Públicas, Estratégias e Desenvolvimento pela Universidade Federal do Rio de Janeiro (UFRJ); Mestre em Educação pela Universidade de Brasília (UnB); Controladoria-Geral da União (CGU).
E-mail: marcusbragaprofessor@gmail.com

Armando Santos Moreira da Cunha

https://orcid.org/0000-0002-3412-4031
Doutor em Gestão pelo Instituto Superior de Ciências do Trabalho e da Empresa (Portugal); Mestrado em Administração Pública pela University of Southern California (USA); Professor da Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas (FGV EBAPE). E-mail: armando.cunha@fgv.br

Patrick Del Bosco de Sales

https://orcid.org/0000-0001-9204-8770
Mestre em Administração pela Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas (FGV EBAPE); Instrutor do Centro de Instrução Almirante Newton Braga (CIANB).
E-mail: del.bosco@marinha.mil.br